城市轨道交通装备认证实施规则

编号：XXXXXXXX

特定要求－基于通信的列车运行控制系统（CBTC）

（V1.0）

2018-XX-XX发布　　2018-XX-XX实施

中国国家认证认可监督管理委员会发布

目　录

城市轨道交通装备认证实施规则

特定要求－基于通信的列车运行控制系统（CBTC）

1　适用范围

本实施规则适用于城市轨道交通基于通信的列车运行控制系统（CBTC）的产品认证。本规则应与《城市轨道交通装备认证实施规则通用要求》结合使用。

2　认证模式

1）安全认证；

2）初始工厂检查+产品抽样检测+获证后监督；

3）新设计、制造或变更、扩展的城市轨道交通CBTC系统/子系统/设备应采用1）+ 2）规定的认证模式，其它设备采用2）规定的认证模式。

3　认证申请单元划分及产品标准

1）按产品型式、用途等划分认证单元，具体认证单元划分和认证依据的产品标准详见附件1。

2）同一认证申请人，同一规格型号、不同地域生产场地生产的产品为不同的认证单元。

4　认证程序

认证模式的基本过程包括：认证的申请；安全认证（适用时）；初始工厂检查；产品抽样检测；认证结果评价；获证后的监督。

5　认证申请必须具备的条件

1）中华人民共和国境内申请人/制造商/生产厂（简称申请人，下同）应持有具有法人资格或其它类似资格的《营业执照》，境外申请人应持有所在国家/地区法律法规规定的登记注册证明，经营范围覆盖申请认证的产品（简称申证产品，下同）。

2）应按照ISO9000系列标准及城市轨道交通装备认证实施规则建立质量管理体系。

3）申证产品应具有合法技术来源。

4）符合法律法规要求，近三年内无产品质量导致的较大及以上事故。

6　申请文件

——同属一个认证规则的申请认证产品应提交产品认证申请书一份，其中：

1）产品类别：规则名称中的产品名称；

2）产品名称：认证单元名称；

3）型号规格：企业实际产品型号+应提供的参数+版本（系统版本、软件版本、子系统软件版本）；

4）认证适用标准编号及名称：按附件1中的标准填写，可只写编号；

5）产品单元：按附件1中的单元填写，可只写编号。

——并随附以下文件各一份：

1）《营业执照》（含统一社会信用代码）或登记注册证明文件的复印件。

2）企业情况调查表（至少包含详细生产场所、必备的生产设备、工艺装备、计量器具和检测手段、技术人员、工作时间、使用语言等）。

3）质量手册或等效文件（受控文本）及程序文件清单。

4）质量体系认证证书复印件（如有）。

5）相关安全评估证书和报告复印件（若已获得）。

6）有关技术资料[认证产品的企业标准、引用标准、产品说明书、MTBF报告、产品软/硬件配置清单、配置（含变更）管理办法（含软硬件）、产品设计开发文件清单（含软硬件）、软件开发流程图、按规定程序批准涉及产品一致性的硬件图纸、技术转让或授权证明（适用时）硬件配置图、生产工艺文件清单、安全证明文件、必要的工艺路线（流程）图、总装图、电气原理图、外购、外协及外委加工产品的供方名单等]。

7）申请同一认证单元内各规格型号之间差异的技术说明。

8）申请人符合相关法律法规及近三年内无产品质量导致的较大及以上事故的声明。

9）申证产品技术来源合法性证明文件或申证产品无知识产权侵权行为声明。

10）法律法规要求的其它资料。

7 安全认证

安全认证根据附件 7《城市轨道交通 CBTC 系统安全认证要求》实施。

8 工厂质量保证能力补充要求

工厂质量保证能力检查按照《城市轨道交通装备认证实施规则 通用要求》审核模式中的 B 开展。

8.1 一般性补充要求

1）申证企业具有申证产品的风险承担能力，注册资本（实缴资本）满足附件 2 的要求。

2）申证企业可持续保持申证产品质量安全的专业能力。对申请认证的产品具备研发、

设计能力，具备相关技术开发人员。应配备足够软件和系统集成相关专业技术开发人员，且相关人员应具备相应的研发、设计能力；还应配备足够的硬件设计相关专业技术人员，且相关人员应具备相应的硬件研发、设计和工艺设计能力。技术人员满足附件 3 的要求。

3）申证产品应持续符合认证标准或技术规范的要求，关键零部件和材料控制符合附件 4 的要求。

4）具备保证申证产品质量的过程能力，设计/生产设备、工艺装备、计量器具和检测手段满足附件 5 的要求。

5）申请CBTC系统认证时，申请企业应至少具备下述两种条件之一：ATP/ATO合格产品研发和生产能力及整体ATC系统的集成能力；ATS和CI合格产品研发和生产能力及整体ATC系统的集成能力。

6）申证产品的设计开发与实现应在实际运用中确认其符合性，企业初次申请时应满足下列条件之一：

① 已在城市轨道交通行业成功运用（或试用），能够提供城市轨道交通行业主管部门（或有关部门）出具的近三年内的试用（或运用）报告，内容至少包括使用项目或场所、合同数量、产品的名称、规格型号、使用起止时间（一年及以上）、里程（10万公里以上）、产品使用情况及履约情况等，以及相应的供货合同（或试用协议）；

② 具有城市轨道交通行业主管机构（或有关部门）的产品合格评审意见

8.2 初始工厂检查补充要求

8.2.1 文件审查

受理企业的初次申请后，认证机构需组织技术人员进行文件审查，除通用要求明确文件以外，还应对产品说明书、MTBF 报告、产品软/硬件配置清单、配置（含变更）管理办法（含软硬件）、产品设计开发文件清单（含软硬件）、软件开发流程图、按规定程序批准涉及产品一致性的硬件图纸、技术转让或授权证明（适用时）硬件配置图、生产工艺文件清单、必要的工艺路线（流程）图、总装图、电气原理图以及安全证明文件（安全评估报告和证书以及必要的产品技术文档）等进行文件审查，如需企业提供详细的技术文档，应书面通知企业提供，文件审查后出具文件审查报告。文件审查需要约 50-100 人日。

当系统的安全认证由受理产品认证的认证机构完成时，文件审查可以不做安全证明文件的审核，此时文件审查需要约 10-15 人日。

8.2.2 系统配置一致性检查

对企业提出申请认证的产品的系统版本、系统软件版本和子系统软件版本进行一致性检

查，核实现场检查内容、功能测试报告和安全评估报告确认版本保持一致。系统安全平台变更、软件架构变更、安全核心部分的算法逻辑变更、较复杂的安全功能变更和重大安全功能缺陷克服等相关系统变更，需要进行变更的安全评估，并由认证机构进行功能测试；系统应用控制功能变更、接口功能变更、一般安全功能变更和缺陷克服等变更应由企业执行内部安全评估流程和变更控制流程并报认证机构备案；其它数据变更、非安全功能变更及上述以外的其它非安全相关的变更等由企业执行内部变更控制流程并报认证机构备案。

9 产品抽样检测要求

9.1 检测依据

CURC/J 0009 城市轨道交通 CBTC 信号系统-ATP 子系统规范

CURC/J 0010 城市轨道交通 CBTC 信号系统-ATO 子系统规范

CURC/J 0011 城市轨道交通 CBTC 信号系统-ATS 子系统规范

CURC/J 0012 城市轨道交通 CBTC 信号系统-CI 子系统规范

CJ/T 407 城市轨道交通基于通信的列车自动控制系统技术要求

GB/T 12758 城市轨道交通信号系统通用技术条件

GB 50490 城市轨道交通技术规范

9.2 抽样方案

按下表采取一次抽样方案，具体抽样基数及抽样数量见表1。

表1 城市轨道交通CBTC系统认证产品质量检测抽样表

项目 单元	检测类别	抽样基数（套）	抽样数量（套）	备注
CBTC	功能测试		1	
ATP	型式试验	≥2	1	
ATO	型式试验	≥2	1	
ATS	型式试验	≥2	1	
CI	型式试验	≥2	1	

抽样说明：

1. 型式试验需要做完整的功能性测试，功能性测试需要企业提供必备的图样（如图纸、表图等）；
2. 每个规格的产品抽取 1 套硬件产品；
3. 企业需提供系统设备结构图、接口防护器件清单、产品合格证、系统完整软硬件配置清单；
4. 电磁兼容性试验、雷电电磁脉冲防护试验需提供的技术文档：系统硬件配置图、受试设备正常工作状态说明、电磁兼容和雷电电磁脉冲防护关键配置说明；
5. 所抽取的样品还应包括出厂合格证明书或质量保证书；
6. 用户抽样时，不要求抽样基数；
7. CBTC 系统只做功能性测试，功能测试是在各子系统型式试验基础上完成。

9.3 抽样要求

9.3.1 抽样工作由认证机构或检测单位派人进行，须至少 2 名抽样人员。

9.3.2 抽样地点在生产企业成品库或用户处随机抽样。

9.3.3 样本应是近期内生产的检测合格且未经使用的产品。

8.3.4 样品应按要求包装后由生产企业/用户在规定的时间内寄、送至抽样人员指定的检测地点。

9.4 检测项目

CBTC系统检测项目及检测类别划分，见附件6。

9.5 检测结果的判定

CBTC信号系统认证单元的检测项目均为A类检测项点，所检测项点均合格判定单元产品检测合格，否则判定为不合格。

附件 1：城市轨道交通 CBTC 系统认证单元划分及产品标准

单元	单元名称/规格型号		应提供参数	标准编号及名称	风险类别
1	CBTC系统	各厂家型号	系统版本、子系统版本及其软硬件完整配置	GB/T 12758城市轨道交通信号系统通用技术条件 CJ/T 407城市轨道交通基于通信的列车自动控制系统技术要求 GB 50490城市轨道交通技术规范	1
2	ATP	各厂家型号	系统版本及软硬件完整配置	CURC/J 0009城市轨道交通CBTC信号系统－ATP子系统规范 CJ/T 407城市轨道交通基于通信的列车自动控制系统技术要求 GB/T 12758城市轨道交通信号系统通用技术条件	1

3	ATO	各厂家型号	系统版本及软硬件完整配置	CURC/J 0010城市轨道交通CBTC信号系统－ATO子系统规范 CJ/T 407城市轨道交通基于通信的列车自动控制系统技术要求 GB/T 12758城市轨道交通信号系统通用技术条件	1
4	ATS	各厂家型号	系统版本及软硬件完整配置	CURC/J 0011城市轨道交通CBTC信号系统－ATS子系统规范 CJ/T 407城市轨道交通基于通信的列车自动控制系统技术要求 GB/T 12758城市轨道交通信号系统通用技术条件	1
5	CI	各厂家型号	系统版本及软硬件完整配置	CURC/J 0012城市轨道交通CBTC信号系统－CI子系统规范 CJ/T 407城市轨道交通基于通信的列车自动控制系统技术要求 GB/T 12758城市轨道交通信号系统通用技术条件	1

附件 2　城市轨道交通 CBTC 系统申请人注册资本（实缴资本）要求

序号	产品名称	注册资本的要求
1	CBTC	不少于 5000 万元
2	ATP	
3	ATO	
4	ATS	
5	CI	

附件 3：城市轨道交通 CBTC 系统技术人员要求

人员岗位	专业要求	工作经历和学历要求	数量	备注
项目负责人	电气、信号、自动控制、自动化、计算机专业	承担过轨道交通信号系统设备研发的项目负责人，从事信号系统研发 10 年以上，本科及以上学历。	1	
软件研发负责人		承担过轨道交通信号系统软件研发的项目负责人，从事信号系统软件研发 10 年（本科）、8 年（硕士）或 6 年（博士）以上。	1	
硬件研发负责人		承担过轨道交通信号系统硬件研发的项目负责人，从事信号系统硬件研发 10 年（本科）、8 年（硕士）或 6 年（博士）以上。	1	
软件开发人员		参加过轨道交通信号系统软件研发项目，从事信号系统软件研发 5 年（本科）、4 年（硕士）或 3 年（博士）以上。	10	ATO 不少于 5 人
硬件开发人员		参加过轨道交通信号系统硬件研发项目，从事信号系统硬件研发 5 年（本科）、4 年（硕士）或 3 年（博士）以上。	5	ATS 硬件如不是自研设备时，可不配备。
注： 1. 各认证单元均需要配备足够相关人员，人员可以复用；当单元中不牵涉到硬件研发生产时，硬件开发人员可以不配备。 2. 现场审核时，检查员对 CBTC 系统设备的设计人员进行现场考核。				

附件 4：城市轨道交通 CBTC 系统关键零部件和材料清单

产品名称/单元		零部件名称		控制项目	变更时需检测项目
CBTC系统		ATP		ATP子系统型号、版本、详细配置、制造商、城轨认证	系统安全平台变更、软件架构变更、安全核心部分的算法逻辑变更、较复杂的安全功能变更和重大安全功能缺陷克服，需要进行变更安全评估，并由认证机构进行功能测试，当发生硬件变更时，需要进行EMC和防雷等测试（适用时）。
		ATO		ATO子系统型号、版本、详细配置、制造商、城轨认证	
		ATS		ATS子系统型号、版本、详细配置、制造商、城轨认证	
		CI		CI子系统型号、版本、详细配置、制造商、城轨认证	
ATP	软件	ATP车载设备软件		版本、详细配置	系统安全平台变更、软件架构变更、安全核心部分的算法逻辑变更、较复杂的安全功能变更和重大安全功能缺陷克服，需要进行变更安全评估，并由认证机构进行功能测试。
		ATP地面设备软件		版本、详细配置	
	硬件	车载	车载人机交互界面	型号、制造商	
			系统平台	型号、制造商、详细配置、城轨认证（适用时）	系统安全平台变更、软件架构变更、安全核心部分的算法逻辑变更、较复杂的安全功能变更和重大安全功能缺陷克服，需要进行变更安全评估，并由认证机构进行功能测试，当发生硬件变更时，需要进行EMC和防雷等测试（适用时）。
			接口滤波器（适用时）	型号、制造商	EMC
			应答器/信标信息接收单元	型号、制造商、城轨认证（适用时）	
			连接器（适用时）	型号、制造商	EMC、振动
		地面	系统平台	型号、制造商、详细配置、城轨认证（适用时）	系统安全平台变更、软件架构变更、安全核心部分的算法逻辑变更、较复杂的安全功能变更和重大安全功能缺陷克服，需要进行变更安全评估，并由认证机构进行功能测试，当发生硬件变更时，需要进行EMC和防雷等测试（适用时）。
			主机电源（适用时）		
			机柜	型号、制造商	EMC
			断路器（适用时）	型号、制造商	
			滤波器（适用时）	型号、制造商	EMC、防雷
			浪涌保护器（适用时）	型号、制造商、城轨认证	EMC、防雷

ATO	软件	ATO车载设备软件	版本、详细配置	系统安全平台变更、软件架构变更、安全核心部分的算法逻辑变更、较复杂的安全功能变更和重大安全功能缺陷克服，需要进行变更安全评估，并由认证机构进行功能测试。
	硬件	车在人机交互界面	型号、制造商	
		车载主机	型号、制造商、城轨认证（适用时）	系统安全平台变更、软件架构变更、安全核心部分的算法逻辑变更、较复杂的安全功能变更和重大安全功能缺陷克服，需要进行变更安全评估，并由认证机构进行功能测试，当发生硬件变更时，需要进行EMC和防雷等测试（适用时）。
		接口滤波器（适用时）	型号、制造商	EMC
		应答器/信标信息接收单元	型号、制造商、城轨认证（适用时）	
		连接器（适用时）	型号、制造商	EMC、振动
ATS	软件	应用软件	型号、版本、详细配置	系统安全平台变更、软件架构变更、安全核心部分的算法逻辑变更、较复杂的安全功能变更和重大安全功能缺陷克服，需要进行变更安全评估，并由认证机构进行功能测试。
CI	软件	应用软件	根据联锁系统结构明确适合企业自身系统及其各子系统的版本和详细信息（如：联锁系统型号，联锁机、通信机、驱采机版本和详细配置）	系统安全平台变更、软件架构变更、安全核心部分的算法逻辑变更、较复杂的安全功能变更和重大安全功能缺陷克服，需要进行变更安全评估，并由认证机构进行功能测试。
		平台软件	型号、版本、详细配置	
	硬件	系统平台	型号、版本、详细配置	系统安全平台变更、软件架构变更、安全核心部分的算法逻辑变更、较复杂的安全功能变更和重大安全功能缺陷克服，需要进行变更安全评估，并由认证机构进行功能测试，当发生硬件变更时，需要进行EMC和防雷等测试（适用时）。
		机柜	型号、防护等级、制造商	EMC
		电源	型号、制造商	EMC、防雷
		浪涌保护器（适用时）	型号、制造商、城轨认证（适用时）	EMC、防雷

附件 5：城市轨道交通 CBTC 系统必备设计生产设备、工艺装备、计量器具和检测检测手段

序号	工艺类别	设备名称	特殊要求	备注
1	系统及软件检测过程	高精度万用表	精度：0.3%	
2		多通道示波器	频率范围：0~500MHz	
3		模拟仿真系统/模拟测试系统	出厂测试	
4		信号发生器	0~50MHz	
5		频率计	0~100MHz	
6	生产过程	三防处理线		
7		清洗机		
8		静电防护设施		
9		ICT在线测试仪		
10		电子装联线	防静电、环境控制	
11		电子高温运行室	控制点温度偏差±2℃	
12		元器件筛选设备	分立元件	
13		老化设备		
14		元器件测试设备		适应产品标准要求
15		元器件成型设备		贴片元件除外
16	硬件测试过程	整机测试台及相关测试设备	满足出厂检验要求并能模拟现场运用环境	
17	硬件检测过程	单板测试台		
18		自动光学监测仪		
19		X射线检测仪		
20		静电测试仪		
21		数字存储示波器		
22		耐压测试仪		
23		绝缘测试仪		

附件 6：城市轨道交通 CBTC 系统检测项目

序号	检测/检验项目	检测类别	初次和复评检测	监督检测	适用单元	备注
1	系统功能测试	A	√	√	全部	
2	常温性能	A	√		ATP（ATO）车载、ATP地面、ATS	
3	工作环境温度范围试验	A	√		ATP地面、CI	
4	低温试验	A	√		ATP（ATO）车载、ATS	
5	高温试验	A	√		ATP（ATO）车载、ATS	
6	恒定湿热试验	A	√		ATP地面、ATS、CI	
7	交变湿热试验	A	√		ATP（ATO）车载	
8	电磁兼容试验	A	√		ATP（ATO）车载、ATP地面、ATS、CI	
9	雷电电磁脉冲防护试验	A	√		ATP地面、ATS、CI	
10	振动冲击试验	A	√		ATP（ATO）车载	
11	防护等级试验	A	√		ATP（ATO）车载	

12	低气压试验	A	√		ATP（ATO）车载、ATP地面、CI	
13	一致性检验	A	√	√	全部	

注：
1. “√”表示应进行的检测/检验项目；
2. 初评时需对系统进行功能测试，并需对每个认证单元每种产品均进行硬件抽样检测；
3. 监督时从企业1年内开通的所有设备中随机抽取软件进行功能性测试，对涉及安全相关指标的检测项目进行抽样检测；
4. 第2次监督时每个认证单元进行抽样检测；
5. 每次监督时均进行一致性检验，随机抽取即将发往现场的硬件设备的关键零部件是否与备案确认表一致，软件的一致性检验是对抽取的设备软件版本和证书确认的软件版本进行一致性检查；
6. 复评时，系统功能测试从企业3年内开通的设备中随机抽取软件版本进行系统全项功能测试；并需对每个认证单元每种产品均进行硬件抽样检测；
7. 产品行业主管部门组织产品监督抽查出现不合格或产品在使用过程中出现质量问题时，随时增加抽检产品的频次、数量、项目；
8. 当产品关键原材料发生变更、生产地址发生变更、关键生产设备、生产工艺发生变更时，根据实际情况增加产品抽查检测，检测产品数量、检测项目可更具实际情况确定；
9. 每年结合年度监督审核或不定期的监督审核确认认证产品的一致性；
10. 如果企业已在认证机构申请ATP、ATO、ATS和联锁产品装备认证，则CBTC产品检测/检验不需重复2-12项。

附件 7：城市轨道交通 CBTC 系统安全认证要求

1 概述

本文件规定了城市轨道交通 CBTC 系统实施安全认证的基本原则和要求，基于城市轨道交通 CBTC 系统的安全风险和认证风险制定，其目的是保证认证产品的功能安全持续符合法律法规及标准要求。

2 术语和定义

2.1 安全相关系统

必需要能实现要求的安全功能已达到或保持受控设备的安全状态；并且自身或与其它 E/E/PE 安全相关系统、其它技术安全相关系统或外部风险降低设施一道，能够达到要求的安全功能所需的安全完整性。

2.2 功能安全

与受控设备及其控制系统有关的整体安全的组成部分，取决于 E/E/PE 安全相关系统、其它技术安全相关系统和外部风险降低设施功能的正确行使。

2.3 安全功能

针对特定的危险事件，为达到或保持受控设备的安全状态，由 E/E/PE 安全相关系统、其它技术安全相关系统或外部风险降低设施实现的功能。

2.4 安全完整性

在规定条件下和规定时间内，安全相关系统成功实现所要求的安全功能的概率。

2.5 安全完整性等级

许多已规定的断续的数值之一，这些数值规定了分配给安全相关系统的安全功能的安全完整性要求。数值越大，安全完整性等级越高。

系统/子系统/部件的安全完整性等级及每功能每小时容许危害率需求对应关系见下表。

每功能每小时容许危害率	安全完整性等级
$10^{-9} \leqslant THR < 10^{-8}$	4
$10^{-8} \leqslant THR < 10^{-7}$	3
$10^{-7} \leqslant THR < 10^{-6}$	2
$10^{-6} \leqslant THR < 10^{-5}$	1
$10^{-5} < THR$	0

3 安全认证依据标准

3.1 安全标准

GB/T 21562-2008 轨道交通 可靠性、可用性、可维修性和安全性规范及示例

GB/T 28808-2012 轨道交通 通信信号及处理系统 控制和防护系统软件

GB/T 28809-2012 轨道交通 通信信号及处理系统安全电子信号系统

3.2 参考标准

GB/T 21562-2 轨道交通 可靠性、可用性、可维修性和安全性规范及示例第2部分：安全性的应用指南

GB/T 24339.1-2009 轨道交通 通信、信号和处理系统第1部分：封闭式传输系统中的安全相关通信

GB/T 24339.2-2009 轨道交通 通信、信号和处理系统第2部分：开放式传输系统中的安全相关通信

GB/T 19001-2016 质量管理体系 要求（ISO 9001:2015，IDT）

4 认证模式

城市轨道交通装备功能安全认证模式为：安全评估。

5 申请与受理

5.1 安全认证申请条件

1)中华人民共和国境内企业应持有工商行政主管部门颁发的企业法人《营业执照》，境外企业应持有有关机构的登记注册证明，经营范围包括认证产品，注册资金5000万元及以上；

2)企业应按照 GB/T19001 标准和城市轨道交通装备认证实施规则建立质量管理体系，或者外国申请人所在国或地区等同采用 ISO9001 标准和城市轨道交通装备认证实施规则的要求；

3）企业应根据第3章所依据的相关标准建立安全管理组织，并配备相应安全管理人员；

4）申请认证产品符合国家、行业颁布的产品标准或相关部门发布的技术条件要求；

5）企业对申请认证的产品具备研发、设计能力和相关技术开发人员。应配备足够软件和系统集成相关专业技术开发人员，且相关人员应具备相应的研发、设计能力；还应配备足够的硬件设计相关专业技术人员，且相关人员应具备相应

的硬件研发、设计和工艺设计能力；

6）符合法律法规要求，近三年内无因产品质量导致的较大及以上事故（国务院令 2007 第 493 号《生产安全事故报告和调查处理条例》）。

5.2 申请资料

——申请认证产品应提交正式的认证申请书一式二份，其中：

1)产品类别：本规则中的产品名称；

2)产品名称：企业标称的产品名称；

3)认证适用标准编号及名称：标准可只写编号。

——并随附以下文件

1)组织机构代码、《营业执照》副本或工商行政主管部门登记注册证明文件的复印件；

2) 企业情况调查表；

3) 质量手册（受控文本）及程序文件清单；

4)质量体系认证证书复印件；

5）相关安全评估证书和报告复印件（若已获得）；

6)拟提交评估用文件清单；

7）企业关于符合相关法律法规及近三年内无因产品质量导致的较大及以上事故的声明。

6 认证实施的基本要求

6.1 安全认证方法和流程

安全认证应根据附录要求对申请认证的系统/子系统/部件在申请范围内开展。其所覆盖的安全生命周期阶段以及每个生命周期阶段的活动应符合附录中第 2 章的要求。

6.2 评估时间

一般情况下,申请方申请认证的要求经认证机构评审并签订认证合同后，开展安全评估工作,评估时间包括文件审核和现场审核两部分,一般以人日数计算。

文件审核和现场检查时间根据所申请认证产品的认证模式、产品复杂程度、单元数量以及系统/子系统/设备的安全完整性等级等确定。

6.3 评估结果

安全评估完成后，认证机构出具安全评估证书和报告，给出安全评估结论和

意见。

7 安全认证证书及安全评估报告

7.1 证书有效期

安全认证证书不设有效期，其有效性与证书明示的设备配置相一致。

7.2 安全认证证书的内容

安全认证证书至少应包括：产品名称、企业名称、企业地址、依据标准、产品配置以及认证结论。认证结论应明示产品的设计和开发过程及文档是否符合依据标准，相关安全功能所能达到的 SIL 等级，并应明确是否有安全限制条件。

7.3 安全评估报告的内容

安全评估报告至少应包括：文件名称、客户标识、预定安全评估工作描述、识别或简述所使用安全评估方法和程序、被评估产品标识、按评估地点相关信息、安全评估结果只针对预定工作、评估产品的声明、安全评估结论和限制条件以及安全评估人员的姓名、签字或签章。安全评估报告中还至少应涵盖附录中第 2 章所描述生命周期及其相关活动。

7.4 安全认证后的变更

当发生系统安全平台变更、软件架构变更、安全核心部分的算法逻辑变更、较复杂的安全功能变更和重大安全功能缺陷克服等相关系统变更，需要由认证机构进行变更安全认证。

7.5 安全认证证书的暂停和撤销

7.5.1 凡有下列情况之一者，认证机构将暂停持证人使用认证机构认证证书和报告。

1）由于已认证产品的质量原因，导致城市轨道交通较大以下事故，或者有关单位、部门或个人反映并经查实，已认证的产品存在质量安全问题但不需要立即撤销认证证书；

2）其他应当暂停认证证书的情形。

证书暂停期间，获证企业生产的该产品不得使用认证证书和报告，不得就其认证资格做出误导性的声明；属产品质量缺陷或安全事故被暂停认证的，企业不得将确认的缺陷产品和事故产品预期交付使用或投入市场，已交付使用的应主动召回，并向现有的和潜在的所有相关采购方告知其认证状态。如企业申请注销正在暂停中的认证证书，认证机构应评价其是否完成相关不合格产品的处置后予以

注销。

7.5.2 凡有下列情况之一，认证机构将撤销持证人持有的认证证书及报告：

1）已认证的产品出现因质量问题导致较大及以上事故或一年内发生三起及以上一般事故；

2）转让认证证书或违反有关规定、严重损害相关认证信誉；

3）弄虚作假，采用欺骗、贿赂等不正当手段获取认证证书；

4）其他违反国家法律法规的情形。

认证机构将采取适当方式对外公告被撤销的安全认证证书。

证书持有者应及时向认证机构通报由已认证的产品质量问题导致的一般及以上事故。

7.6 安全认证证书的使用

持证人应确保安全认证证书的使用符合《城市轨道交通装备认证证书和认证标志使用管理办法》的规定。

8 安全认证标志

获得安全认证证书的设备不使用城轨装备认证标志。

9 收费

由认证机构按有关规定，根据评估合同向申请方收取。

附录　安全评估方法、流程及内容

1　安全评估工作方法及流程

认证机构根据安全评估流程对被评估系统/子系统/部件的全生命周期的质量管理、技术管理和安全管理活动进行审核，主要是对系统保障是否满足标准的相关要求进行评估，评估活动包括但不限于：

- 项目文件审核；
- 见证设计和测试过程；
- 与设计、验证和确认人员面谈；
- 质量、技术和安全审核，含现场审核项目过程和体系。

安全评估的标准主要为本要求第 2 章依据标准及相关标准。认证机构应根据项目计划起草相应的安全评估计划，确定安全评估活动和安全评估项目的时间节点。认证机构将审核中发现的观察项和不符合项及时反馈给被评估产品的企业（以下简称“企业”），企业应针对观察项和不符合项进行纠正或澄清。认证机构记录其收集的所有审核证据，并在完成安全评估后，针对评估内容发布最终安全评估报告和安全评估证书。

评估过程主要覆盖三方面内容：安全管理、质量管理和技术安全。认证机构依据本要求第 2 章依据标准相关条款针对项目进行评估。

认证机构根据客观证据提出公正性评估意见。如果企业采用了等效于标准或高于标准的方法或技术而导致系统/子系统/部件未完全符合本要求第 2 章依据标准相关要求，在企业提供充分证据的情况下，认证机构应对此类不符合项作为技术例外接收。

2　生命周期内安全评估工作内容

安全评估工作中的具体评估工作是在特定项目所确定的生命周期内开展的。本章详细说明了生命周期内每个阶段的目标、要求、交付物及所需验证和确认工作。这些要求的应用和阶段范围应根据特定系统/子系统及部件的情况调整到满足系统评估的目的。

2.1 第 1 阶段: 概念

本阶段目的是使对系统的理解达到使后续的 RAMS 生命周期任务能圆满完成的层次。

本阶段企业应在 RAMS 性能范畴内明确系统范围、背景和目标和系统环境；进行系统财务分析的 RAMS 蕴涵、系统可行性研究的 RAMS 蕴涵方面的回顾；在该阶段企业还应确定影响系统 RAMS 性能的危害源，包括：与其他系统的相互作用；与人的相互作用；获取类似和/或相关系统中先前的 RAMS 要求和过去的 RAMS 性能、已确定的 RAMS 性能危害源、当前的行业主管部门（或有关部门）安全规章与目标和安全立法等方面信息；还应为后续的

生命周期 RAMS 任务定义管理要求的范围。

本阶段的结果、设定的所有假设及理由应形成文档。并且文档应包括在生命周期第 2、3 和 4 阶段能充分实现 RAMS 要求的管理结构。本阶段的交付物是后续生命周期阶段的关键输入。

本阶段应进行如下验证任务：

a) 评估本阶段内作为 RAMS 任务输入的信息、(合适的)数据与其他统计数字的充分性；

b) 评估所定义的系统环境的充分性；

c) 评估所列出的危害源的完整性；

d) 评估本阶段内使用的方法、工具和技术的合适性；

e) 评估本阶段内所有执行任务的人员的能力。

2.2 第 2 阶段：系统定义和应用条件

本阶段的目的是定义系统任务概要、定义系统范围、确定影响系统特性的应用条件、定义系统危害分析的范围、确定系统 RAMS 方针、建立系统的安全计划；

本阶段规定系统任务概要、系统范围、影响系统的应用条件范围、系统危害分析的范围；应完成支持目标的初步 RAM 分析、初步危害识别；为系统建立通用 RAMS 方针；为系统建立安全计划。

本阶段的结果、设定的所有假设及理由应形成文档。并且文档应包括系统 RAMS 方针及安全计划。本阶段的交付物构成后续生命周期阶段的一个关键输入。

本阶段应进行如下验证任务：

a) 评估本阶段内作为任务输入的信息、（合适的）数据及其他统计数字的充分性。

b) 在第 1 阶段可交付性的基础上，应该验证第 2 阶段的可交付性的各个方面，特别是评审 RAMS 方针与在第 1 阶段中规定的系统要求相一致。

c) 应对 RAM 分析的完整性和危害识别过程进行评估。

d) 安全计划充分性的评审，包括核查安全计划内所有数据源的充分性。

e) 评估该阶段内所使用的方法、工具和技术的适用性。

f) 评估本阶段执行任务的全体人员的能力。

任何一个错误或不足都需要重复先前一个或多个生命周期阶段中的部分或全部工作。

2.3 第 3 阶段：风险分析

风险分析在生命周期的几个阶段需要重复。风险分析工作应有设计、运营、维护、安全技术、电气等方面专家参与完成。

本阶段的目标是识别与系统有关的危害、识别导致危害的事件、确定与危害有关的风险、建立用于计划内的风险管理的流程。

本阶段应在系统应用环境中，系统地确定并区分所有有理由预见的系统危害的优先次序，包括由以下条件所产生的危害、确定导致危害的事件的顺序、估计每个危害发生的频度、估计每个危害后果可能的严重性、估计每个危害产生的系统风险。在考虑了可用性与系统生命周期费用要求的冲突后，本阶段应确定与每个已识别危害有关的风险的可接受性并对其进行分类。建立一个危害日志作为管理风险的基础。在生命周期中，只要已识别的危害发生改变或确定有新的危害，危害日志就应更新。

本阶段的结果、设定的所有假设及理由应形成文档。风险分析的结果应记录在危害日志中。

本阶段应进行如下验证任务：

a）评估作为本阶段内任务输入的信息、（合适时）数据和其他统计数字的充分性；

b）第 3 阶段的可交付性应比照第 2 阶段的交付物来进行检查；

c）评估风险评估的完整性；

d）评估风险可接受的类别；

e）评估具体系统危害日志流程的合适性；

f）评估本阶段内使用的方法、工具和技术的合适性；

g）评估本阶段执行任务的全体人员的能力。

任何一个错误或不足需要重复先前一个或多个生命周期阶段中的部分或全部工作。

2.4 第 4 阶段：系统需求

本阶段的目标是指明系统全面的 RAMS 要求，对系统 RAMS 规定全面的论证与验收准则，为控制后续生命周期阶段的 RAM 任务建立 RAM 规划。

本阶段应规定整个系统的所有 RAMS 要求、所考核系统的 RAMS 要求。规定与系统 RAMS 相一致的所有要求。并为余下的生命周期任务建立详细的 RAM 规划。对于具体系统，RAM 规划应包括判定能最有效地达到 RAM 要求的任务。具体系统的 RAM 规划应经过行业主管部门（或有关部门）及其支撑工业的同意，并在整个系统生命周期内进行实施。RAM 规划中，应考虑管理、可靠性、可维护性和可用性。修订安全计划以保证所有今后计划任务与系统的应急 RAMS 要求相一致。

本阶段的结果、设定的所有假设及理由应形成文件。本阶段应该产生一个更新的安全计划和验收计划。本阶段的交付物是后续生命周期阶段的输入。

本阶段应进行如下验证任务：

a）评估本阶段内作为任务输入的信息、（合适时）数据和其他的统计数字的充分性；

b）系统要求应在比照第 2、3 阶段产生的可交付性（包括生命周期费用）后验证；

c）安全性要求应在比照行业主管部门（或有关部门）的安全目标和安全方针后验证；

d）RAM 要求应对照行业主管部门（或有关部门）的 RAM 目标和 RAM 方针进行验证；

e）评估验收计划和确认计划的充分性与完整性；

f）评估 RAM 规划的充分性（包括复核所有使用的数据源的充分性）；

g）评估本阶段内采用的方法、工具和技术；

h）评估本阶段执行任务的全体人员的能力。

任何一个错误或不足都需要重复先前一个或多个生命周期阶段中的部分或全部工作。

2.5 第 5 阶段：系统需求的分配

本阶段的目标是把系统的所有 RAMS 要求分配给所设计的子系统/部件和外部设施，为所设计的子系统/部件和外部设施规定 RAMS 验收准则。

本阶段要给所设计的子系统、部件和外部设施分配功能要求，给所设计的子系统、部件和外部风险减小设施分配安全要求，并规定所设计的子系统、部件与外部设施达到全部的系统 RAM 要求，包括共因失效与多路失效的影响，以及复核 RAM 规划；还应规定符合子系统、部件和外部设施要求的一些需求，包括：子系统/部件和外部设施要求的验收准则、子系统/部件和外部设施要求的论证、验收过程与步骤；复核并更新安全计划和确认计划，确保计划的任务与分配后的系统要求相一致。应关注计划中安全功能容易被忽略的关键部分，如人员独立性要求部分和系统接口控制部分。

本阶段的结果、作出的所有假设及理由应形成文件。本阶段应产生更新的安全计划。本阶段产生的文件应包括给所设计的子系统、部件和外部设施分配系统要求。本阶段的交付物是后续生命周期阶段的一个关键输入。

本阶段要进行如下的验证任务：

a）评估本阶段内作为任务输入的信息、（合适时）数据和其他的统计数字的充分性；

b）对照第 4 阶段产生的可交付性，验证系统、子系统、部件和外部设施要求，包括对系统生命周期费用要求的复核；

c）应验证所设计的子系统、部件和外部设备总的组成结构，确保与整个系统 RAMS 要求相一致；

d）应验证子系统、部件和外部设施的 RAMS 要求，确保这些要求可追溯至系统的 RAMS

要求；

e）应验证子系统、部件和外部设施的 RAMS 要求，确保功能之间的完整性和一致性；

f）修订后的安全计划和确认计划应经过验证以确保持续可用性；

g）评估本阶段内使用的方法、工具和技术的适宜性；

h）评估本阶段执行任务的全体人员的能力。

任何一个错误或不足都需要重复先前的一个或多个生命周期阶段中的部分或全部工作。

2.6 第 6 阶段：设计和实现

本阶段的目标是创建符合 RAMS 要求的子系统和部件、证明子系统和部件符合 RAMS 要求以及为后续的生命周期任务（包括 RAMS）建立计划。

本阶段应设计满足 RAMS 要求的子系统和部件的方案，完成满足 RAMS 要求的子系统和部件的施工设计，在 RAMS 范围内为今后的生命周期任务建立包括安装、试运行、运营和维护及运营中数据获取和评估的计划，定义、验证和建立能够生产已确认的 RAMS 的子系统和部件的制造工序，并考虑使用环境应力筛选、RAMS 改进测试、对 RAMS 有关失效模式进行检查和测试、实施安全计划的中规定的生命周期内从事工作的团体之间关系、责任、能力及所担任角色的措施。

为已设计的并独立使用的系统准备一个通用安全例证，证明系统能满足安全性要求。该安全例证应通过行业主管部门（或有关部门）的正式批准，如果在这个阶段适合，则为系统准备应用安全例证。该应用安全例证建立在通用安全例证的基础之上，用于证明对于特定类别的应用，系统设计及其物理实现（包括安装和试验阶段）满足安全性要求。该应用安全例证需经行业主管部门（或有关部门）的正式批准，且应包括对所有考核应用的级别，证明系统安全性所必须的全部附加信息以及系统应用有关的所有约束与限制。

本阶段的结果、作出的所有假设及理由应形成文件。应继续记录本阶段内进行的 RAMS 确认任务。应提出 RAMS 后续生命周期任务的详细计划。运营与维护规程，包括所有提供备用部件的相关信息，特别是安全相关项目，应在本阶段内提出。本阶段必须形成通用安全例证。本阶段可形成应用安全例证。本阶段的交付物成为后续生命周期阶段的一个关键输入。

本阶段应进行如下验证任务：

a）评估作为本阶段任务输入的信息、（合适时）数据与其他统计数字的充分性；

b）通过分析和测试，验证子系统和部件的设计符合 RAMS 要求；

c）通过分析和测试，验证子系统和部件的施工设计与设计方案一致；

d）确认子系统和部件的实现，以保证与 RAMS 验收准则（包括生命周期要求）相一致；

e）通过分析和测试，验证制造布局可生产出已经确认了 RAMS 的子系统和部件；

f）验证所有后续生命周期活动计划与系统 RAMS 要求（包括生命周期费用要求）相一致；

g）评估通用安全例证与相应的应用安全例证的充分性和完整性；

h）评估本阶段内使用的方法、工具和技术的合适性；

i）评估本阶段内执行任务的全体人员的能力；

j）保证 RAMS 确认计划的持续适用性。

任何一个错误或不足可以要求重复先前的一个或多个生命周期阶段中的部分或全部工作。

2.7 第 7 阶段：制造

本阶段的目标是实施能生产出已确认 RAMS 的子系统和部件的制造工序、建立以 RAMS 为中心的工序保障安排以及建立子系统和部件 RAMS 的支持计划。

本阶段应验证和实现制造工序，建立子系统和部件支持计划，并安排满足要求的制造、实施满足要求的制造、实现 RAMS 流程保证，以避免潜在的 RAMS 相关失效模式。

本阶段的结果、设定的所有假设及理由应形成文挡。应继续记录本阶段内进行的 RAMS 确认任务。本阶段的交付物构成后续生命周期阶段的一个关键输入。

本阶段应该执行如下的验证任务：

a）评估本阶段作为任务输入的信息、（合适时）数据及其他统计数字的充分性；

b）验证 RAMS 支持文件是正确的、充分的，并与生命周期费用要求和系统规定的目标 RAMS 要求相一致；

c）评估以确保正在生产的产品按系统要求制造；

d）评估本阶段内使用的方法、工具和技术的合适性；

e）评估本阶段内执行任务的全体人员的能力。

任何一个错误或者不足可以要求重复先前的一个或多个生命周期阶段的部分或全部工作。

2.8 第 8 阶段：安装

本阶段的目标是对形成完整系统所需要的子系统和部件进行组装与安装并启动系统支持计划。

本阶段应按照安装计划对形成完整系统所需要的子系统、部件和外部设施进行组装和安装，写出安装流程，并在安装完成后复核和修改安全计划，确保记录了系统或工序发生的变化，并在后续的生命周期任务中实施有效管理。开始人员培训，制订可用的支持步骤，建立备件供应，建立工具供应。

本阶段的结果、设定的所有假设及理由应形成文档。应继续记录本阶段内所执行的所有 RAMS 确认任务，包括安装工作。更新安全计划。本阶段的交付物构成后续生命周期阶段的一个关键输入。

本阶段应进行如下验证任务：

a）评估本阶段内作为任务输入的信息、（适当时）数据和其他统计数字的充分性；

b）验证安装工作是按安装计划进行的；

c）通过分析和测试，验证已安装的系统满足 RAMS 要求；

d）评估安全计划以确保其持续适用性；

e）评估系统支持计划的有效性和充分性；

f）评估本阶段使用的方法、工具和技术的合适性；

g）评估本阶段内执行任务的全体人员的能力。

任何一个错误或不足可以要求重复先前的一个或多个生命周期阶段的部分或全部工作。

2.9 第 9 阶段：系统确认(包括安全验收和试运行)

本阶段的目标是确认子系统、部件和外部风险降低设施的总成与系统的 RAMS 要求一致；对子系统、部件和外部风险降低设施的总成进行调试和试运行；准备和（合适时）验收系统的安全例证；提供获得的数据并评估。

本阶段应按照确认计划来确认子系统、部件和外部风险降低设施的总成并记录确认流程；按照调试计划对子系统、部件和外部风险降低设施的总成进行调试并记录其过程；如果需要，采用试运营周期以解决正式运营时的系统问题。当采用作为系统验收一个部分的试运营周期时，在系统投入商业运营之前，应考虑证明系统的安全性；若在第 6 阶段还没有准备好，则应为系统准备一个应用安全例证，用它来证明该系统在应用中符合系统安全性要求。

本阶段的结果、设定的所有假设及理由应形成文档。应继续记录本阶段内执行的所有 RAMS 确认任务，包括调试工作。在本阶段内应为系统提供一个应用安全例证。应继续记录本阶段内进行的所有验收任务。本阶段的交付物构成后续生命周期阶段的一个关键输入。

本阶段应执行如下验证任务：

a）评估本阶段作为任务输入的信息、（合适时）数据和其他统计数字的充分性；

b）通过分析和测试，验证并确认所安装系统满足 RAMS 要求；

c）验证调试活动是按调试计划实施的；

d）评估运营数据采集系统的有效性和充分性；

e）评估在本阶段内所使用的方法、工具和技术的合适性；

f）评估本阶段执行任务的全体人员的能力。

任何一个错误或者不足可要求重复先前的一个或多个生命周期阶段的部分或全部工作。

确认后的系统应在城市轨道交通行业内开展试运用。试运用结束后，由城市轨道交通主管部门或相关部门（试用单位）出具试运用报告（内容包括使用项目或场所、合同数量、产品的名称规格型号、使用起止时间、产品使用情况及履约情况等）。

2.10 第 10 阶段：系统验收

本阶段的目标是评估子系统、部件和外部风险降低设施的总成符合整个系统的所有 RAMS 要求并验收投入运营的系统。

本阶段应根据系统验收计划评估系统的所有验证和确认任务，特别是在第 4 阶段准备的系统要求、验证与确认计划以及在第 9 阶段中准备的验证和确认任务的记录。如果合适，应正式验收系统以便投入运营；复核和更新危害日志，记录系统确认或验收过程中确定的残留危害，并确保这些危害所造成的风险得以有效管理。

本阶段的结果、设定的所有假设及理由应形成文档。应继续记录本阶段所执行的所有验收任务。更新本阶段的危害日志。本阶段的可交付性构成后续生命周期阶段的一个关键输入。

本阶段应执行以下验证任务：

a）评估本阶段内作为任务输入的信息、（合适时）数据与其他统计数字的充分性；

b）通过分析和测试验收系统满足 RAMS 要求（包括生命周期费用要求）；

c）验证验收工作是按验收计划执行的；

d）评估修改过的安全计划的延续适用性；

e）评估以确保任何残留的危害已得到有效地管理；

f）评估特殊应用安全例证的充分性和完整性；

g）评估在本阶段内使用的方法、工具和技术的合适性；

h）评估在本阶段内执行任务的全体人员的能力。

任何一个错误或者不足可要求重复先前的一个或多个生命周期阶段的部分或全部工作。

3　评估交付物

认证机构评估交付物见下表。

评估交付物	备注
阶段审核报告	根据需要提供
评估通知	中间提供
评估报告	最终提供
评估证书	最终提供

附表 企业主要交付物

下表所列为不同安全完整性等级和评估层次的企业主要交付物，表中所列企业各阶段所提交文档应在安全生命周期过程中适时更新。实际评估中所提交文档应与下表中所列文档实质性内容相一致。

序号	企业应提交文件	安全完整性等级		
		SIL 0	SIL 1/ SIL 2	SIL 3/ SIL 4
1.	系统质量保障计划	√	√	√
2.	系统安全计划		√	√
3.	系统验证计划	√	√	√
4.	配置管理计划	√	√	√
5.	系统确认计划	√	√	√
6.	软件质量保障计划	√	√	√
7.	软件配置管理计划	√	√	√
8.	初步危害分析（PHA）		√	√
9.	系统危害分析（SHA）			√
10.	接口危害分析（IHA）			√
11.	子系统危害分析（SSHA）			√
12.	危害及可操作性分析报告（HAZOP）		√	√
13.	系统风险分析报告	√	√	√
14.	系统风险分析验证报告	√	√	√
15.	危害日志		√	√
16.	系统需求规范	√	√	√
17.	系统安全需求规范		√	√
18.	系统需求测试规范	√	√	√
19.	系统结构规范	√	√	√
20.	故障树分析（FTA）			√
21.	失效模式与影响分析报告（FMECA）		√	√
22.	可靠性预计报告	√	√	√
23.	软/硬件接口规范		√	√
24.	子系统需求规范	√	√	√
25.	系统集成测试规范	√	√	√
26.	硬件确认计划		√	√

序号	企业应提交文件	安全完整性等级		
		SIL 0	SIL 1/ SIL 2	SIL 3/ SIL 4
27.	硬件需求规范		√	√
28.	硬件测试规范		√	√
29.	硬件结构规范	√	√	√
30.	硬件设计规范（或硬件详细设计说明）	√	√	√
31.	硬件设计图（电气连接图等图纸）	√	√	√
32.	硬件电路图（PCB 图及电路原理图）	√	√	√
33.	硬件内部接口规范		√	√
34.	硬件外部接口规范		√	√
35.	硬件集成测试规范	√	√	√
36.	硬件设计测试规范		√	√
37.	硬件制造需求规范		√	√
38.	硬件维护需求规范		√	√
39.	硬件制造可接受性测试规范		√	√
40.	硬件安装和调试需求规范		√	√
41.	硬件报废需求规范		√	√
42.	硬件处理需求规范		√	√
43.	软件验证计划		√	√
44.	软件确认计划		√	√
45.	软件需求规范	√	√	√
46.	全面软件测试规范	√	√	√
47.	软件结构规范	√	√	√
48.	软件接口规范	√	√	√
49.	软件集成测试规范	√	√	√
50.	软件设计规范（软件概要设计说明）	√	√	√
51.	软件组件设计规范（软件详细设计说明）		√	√
52.	软件组件测试规范		√	√
53.	系统需求验证报告	√	√	√
54.	硬件需求验证报告		√	√
55.	系统结构和设计验证报告		√	√
56.	软件需求验证报告	√	√	√
57.	软件结构和设计验证报告	√	√	√
58.	软件组件设计验证报告		√	√
59.	硬件结构验证报告		√	√
60.	硬件设计验证报告		√	√
61.	子系统结构规范	√	√	√
62.	硬件制造数据		√	√
63.	硬件实施验证报告		√	√
64.	硬件设计测试报告		√	√
65.	硬件集成测试报告	√	√	√
66.	硬件制造可接受性测试报告		√	√
67.	软件源代码	√	√	√
68.	软件组件测试报告		√	√
69.	软件源代码验证报告	√	√	√
70.	软件确认报告	√	√	√
71.	质量保障验证报告	√	√	√
72.	软件质量保障验证报告	√	√	√
73.	系统集成测试案例	√	√	√
74.	硬件制造计划		√	√

序号	企业应提交文件	安全完整性等级		
		SIL 0	**SIL 1/ SIL 2**	**SIL 3/ SIL 4**
75.	硬件制造验证报告		√	√
76.	硬件测试案例		√	√
77.	硬件测试报告		√	√
78.	硬件确认报告		√	√
79.	工具确认报告		√	√
80.	硬件确认验证报告		√	√
81.	软件静态测试报告		√	√
82.	软件动态测试报告		√	√
83.	软件测试案例	√	√	√
84.	软件编码规范		√	√
85.	硬件安装规范	√	√	√
86.	调试测试规范	√	√	√
87.	安装计划	√	√	√
88.	调试计划	√	√	√
89.	安装测试规范	√	√	√
90.	安装测试报告	√	√	√
91.	安装、测试和调试验证报告	√	√	√
92.	软件应用需求规范		√	√
93.	软件应用准备计划		√	√
94.	软件应用测试规范		√	√
95.	软件应用结构和设计		√	√
96.	软件应用准备验证报告		√	√
97.	软件应用测试报告		√	√
98.	软件应用数据/算法源代码		√	√
99.	软件应用数据/算法验证报告		√	√
100.	软件集成验证报告		√	√
101.	硬件集成验证报告		√	√
102.	软件集成测试报告	√	√	√
103.	软/硬件集成测试规范		√	√
104.	软/硬件集成测试报告		√	√
105.	全面软件测试报告	√	√	√
106.	系统集成测试报告	√	√	√
107.	系统集成验证报告	√	√	√
108.	系统需求测试报告	√	√	√
109.	系统确认报告	√	√	√
110.	最终验证报告		√	√
111.	发布清单	√	√	√
112.	系统安全案例		√	√
	END			