

自动控制系统软件 STL

- 产品认证实施规则

(家用电器和类似用途自检软件产品)

(版本号：第 3 版)

前 言

本文件由广电计量检测集团股份有限公司发布,版权归,广电计量检测集团股份有限公司所有,任何组织及个人未经广电计量检测集团股份有限公司许可,不得以任何形式全部或部分使用。

本文件代替 GRGT-WI-AT-TE-026-A.0(版本号:第 2 版),与第 2 版相比,本版本主要变化如下:

——删除 3 认证依据标准 IEC 61508-3、ISO 26262-6;

本文件及其所代替文件历次版本发布情况为:

——2025 年 6 月 24 日首次发布 GRGT-WIAT-TE-026-A.0(版本号:第 1 版);

——2025 年 7 月 20 日第一次修订,发布为 GRGT-WI-AT-TE-026-A.0(版本号:第 2 版)

——本次为第三次修订,版本号:第 3 版,修订日期 2025 年 12 月 18 日。

目 录

1. 目的 - 1 -

2. 认证范围 - 1 -

3. 认证依据标准 - 1 -

4. 认证模式 - 1 -

5. 认证程序 - 2 -

 5.1. 认证单元划分 - 2 -

 5.2. 认证申请和申请评审 - 2 -

 5.3. 功能安全评估 - 4 -

 5.4. 质量管理能力检查 - 5 -

 5.5. 认证复核及决定 - 5 -

 5.6. 获证后监督 - 6 -

6. 认证证书 - 7 -

 6.1. 证书内容 - 7 -

 6.2. 证书的有效性 - 8 -

 6.3. 认证的变更 - 8 -

 6.4. 获证单元覆盖产品的扩展 - 8 -

 6.5. 证书的暂停、恢复、注销和撤销 - 9 -

7. 认证标志 - 9 -

8. 收费 - 9 -

9. 认证责任 - 10 -

10. 技术争议及申诉 - 10 -

11. 信息公开 - 10 -

附录 A: 术语和缩略语 - 11 -

附录 B: 认证申请材料 - 12 -

附录 C: 软件安全生命周期建议的工作产品清单 - 13 -

附录 D: IEC 60730 CLASS B/C 获证产品年度自查表 - 15 -

1. 目的

根据 CNAS-CC02《产品、过程和服务认证机构要求》对认证机构的通用要求，结合 IEC 60730-1（自动电气控制-第 1 部分：一般要求）和 IEC 60335-1（家用和类似电器-安全-第一部分：通用要求）的对家用电器和类似用途自检软件的技术要求和测试要求，特制定适用于广电计量检测集团股份有限公司（以下简称广电计量）实施家用电器和类似用途自动控制系统软件 STL 产品认证的规则和程序要求，以指导广电计量审核管理部门执行相关的认证活动。

2. 认证范围

本规则适用于广电计量对家用电器和类似用途自检软件产品开展的认证活动。

本规则所指的认证产品为应用于白色家电（如洗衣机、电冰箱/冰柜、洗碗机、烘干机等）、厨房电器（如智能炊具、电饭煲、电磁炉、烤箱等）、环境控制设备（如空调控制器、吊扇等）和智能家居（等智能插座/开关、门锁控制器等）等家用电器或类似用途的自检软件。

备注：在无特殊说明的情况下，这些自检软件通常是指用于控制器芯片（如 MCU、SoC 等）中的嵌入式软件（英文全称：Self-diagnostic Test Library，以下简称 STL）。

3. 认证依据标准

- 1) IEC 60730-1 Automatic electrical controls - Part 1: General requirements
- 2) IEC 60335-1 Household and similar electrical appliances - Safety - Part 1: General requirements

注：本实施规则所涉及的标准均为最新标准。申请认证产品可能适用以上一个或多个执行标准。

4. 认证模式

软件 STL 的认证模式为：功能安全评估+现场检查+获证后监督，基本环节包括：

- 1) 认证申请和受理；

- 2) 功能安全评估;
- 3) 现场检查;
- 4) 认证结果评价与批准;
- 5) 获证后监督。

5. 认证程序

5.1. 认证单元划分

软件 STL 认证单元的划分原则如下:

- 硬件平台相同 (如同一 MCU 系列的不同型号), 可划分为同一认证单元。
- 使用不同内核的架构, 如 ARM 架构和 RISC - V 架构, 需划分为不同单元。
- 软件 STL 安全等级不一样时 (即同时存在 Class B, Class C 的软件要求时), 不可划分为同一认证单元。

5.2. 认证申请和申请评审

5.2.1 认证委托方需要按照认证机构出具的认证申请文件要求填写必要的认证委托方信息、认证单元信息、以及适用标准条款的声明等内容。

5.2.2 认证委托方在申请软件 STL 认证时, 应按照本规则附录 B (认证申请材料) 要求向认证机构提供相关资料。

5.2.3 认证委托方应对提供资料的真实性负责, 认证机构对认证委托方提供的认证申请资料进行管理、保存, 并负有保密的义务。

5.2.4 认证机构对申请材料进行评审, 在 10 个工作日内向认证委托方发出受理或不受理的通知, 或要求认证委托方整改后重新提出认证申请。

5.2.5 认证申请评审通过后, 认证机构与申请组织签订具有法律效力的书面认证合同或等效文

件。

5.2.6 认证机构应对整个认证周期制定审核方案，确定适宜的审核人日，以使检查组能够对受审核方相应等级的软件 STL 分类的进行充分的审核，包括所需审核的活动、文档、部门/人员以及软件工具链使用情况等。

表 1 现场检查人日数

检查项目	基础人日	备注
功能安全评估	1 人日/每产品	1. 视具体产品，评估项目数量适当增减人日； 2. 每增加一款产品功能评估，增加 0.5 人日。
5.4 质量管理能力检查	0.5 人日	如企业质量管理体系过期或未获得质量管理体系认证证书的，需补充相关条款检查，视企业规模、认证单元数适当增加人日数。增加的人日一般不超 2 人日。

5.2.7 若认证委托方提交的软件 STL 认证申请文件中,同时申请了 IEC 61058 和(或)ISO 26262 产品认证，审核方案策划时应考虑所有适用要求，以及结合审核所需的额外审核人日。

5.2.8 审核方案应根据认证单元适用的标准范围、产品复杂度、涉及场所、客户特殊要求等因素策划所需的功能安全评估和现场检查的安排等。

5.2.9 审核方案的确定和任何后续调整，应考虑认证单元的适用标准范围和认证单元的划分。

5.2.10 若认证合同有要求，则审核方案中应策划证书有效期结束前续证所需的审核活动，以保持证书下一个认证周期有效。

5.2.11 检查组长应根据审核方案、以及前期与认证委托方的沟通信息，编制适用于认证单元的检查计划。

5.2.12 检查计划中至少应包括以下内容：审核目的、审核准则、审核范围、审核日期、时间安排和场所、检查组成员及审核任务安排。

5.2.13 检查组长应在现场审核活动开始前将检查计划提交给受审核方进行确认，并留出足够的时间，以使受审核方能够对某一检查组成员的任命表示反对，并在反对有效时使认证机构能够重组检查组。

5.3. 功能安全评估

5.3.1 检查组在执行功能安全评估时，应按照认证产品依据标准适用条款对受审核方提供的验证报告或证据进行逐条评估。

5.3.2 认证单元的诊断测试能力应能覆盖相应硬件平台（如 MCU）内的硬件组件（如 CPU），如 IEC 60730-1 表 H.2 和（或）IEC 60335-1 表 R.1 所列。当硬件平台不包括某些 IEC 60730-1 表 H.2 和（或）IEC 60335-1 表 R.1 中所列硬件组件，或某些诊断测试项由集成商完成时，则需要在评价结果中明确记录裁剪的理由。

5.3.3 软件验证（包括软件模块验证、软件集成验证和软件需求确认）规范应考虑适当的验证方法和用例设计方法，可参考 IEC 61508-3 或 ISO 26262-6 实施。

5.3.4 软件验证报告的结果应能显示软件安全需求、软件架构和软件模块已达到设计要求，否则将记录为不符合。

5.3.5 检查员在评估验证结果时，应重点关注以下信息：

- 1) 使用的验证方法和测试用例设计方法的充分性；
- 2) 适用时，验证所抽取的型号合理性；
- 3) 验证环境的合理性；
- 4) 预期结果和实际结果的一致性。

5.3.6 认证产品验证报告及验证机构要求

- 1) 受审核方应自行安排具备验证能力的实验室执行验证并出具验证报告, 可以是受审核方控制之下的组织, 也可以是独立于受审核方的外部机构。
- 2) 实施验证活动的人员或组织, 应确保所有验证活动严格按照认证单元验证规范要求实施, 并根据过程中产生的验证记录、数据和日志文件等, 最终被整理为验证报告。
- 3) 验证结果应符合验证规范中定义的所有通过准则或与预期结果一致, 否则将记录为不符合。

5.3.7 检查员应对上述验证报告进行功能安全评估, 并对认证单元满足安全需求和标准要求 (IEC 60730-1 和 (或) IEC 60335-1) 作出评价 (通过或不通过)。

5.4. 质量管理能力检查

5.4.1 本规则所述的现场检查主要针对受审核方研发管理现场实施, 检查员应重点关注以下内容:

- 1) 认证产品的一致性检查;
- 2) 已建立的质量管理体系及证明其有效运行的证据;
- 3) 必要时, 对认证单元的测试项进行现场抽测。

5.4.5 根据质量管理能力检查, 检查组出具现场检查报告。现场检查结论为不通过的, 检查组直接向认证机构报告。现场检查存在不符合项时, 受审核方应在规定期限内完成整改, 认证机构采取适当方式对整改结果进行验证。未能按期完成整改的或整改不通过的, 按现场检查不通过处理。

5.5. 认证复核及决定

5.5.1 检查组将风险评估报告、现场检查报告提交给认证机构复核人员。复核人员将按照认证机构复核相关要求对认证审核材料进行评价和复核, 并作出认证决定。

5.5.2 若认证决定的结果是拒绝的,则广电计量将通知认证委托方和受审核方不通过的结果及原因,本次认证结束。

5.5.3 若认证决定的结果是通过的,则广电计量将启动发证流程,为受审核方颁发功能安全产品认证证书。

5.6. 获证后监督

5.6.1 初次认证决定后,认证机构应在每 12 个月内安排对获证组织实施年度监督审核。审核组应对获证组织以下方面进行确认:

- 1) 初次认证或上一次监督的不符合项整改情况(适用时);
- 2) 获证产品的设计变更情况,软件校验码(如 SHA-256 校验码)与初次认证的校验码不一致时视为存在设计变更;
- 3) 认证证书和标志的使用情况;
- 4) 质量管理体系有效性情况。

5.6.2 获证组织应根据 5.6.1 要求提前 1 个月向认证机构提供获证产品的年度自查表,当获证产品存在设计变更时,认证机构应安排现场审核,这种情况现场监督的人日通常为 1 人日。当获证产品不存在任何变更,认证机构可视情况安排非现场审核(如文件审核),根据自查表向获证组织确认相关记录文件的真实性和完整性。

5.6.3 认证机构可根据获证产品实际使用情况,按年度调整监督检查的时间。若发生下述情况之一,可能增加现场监督频次:

- 1) 获证产品出现严重安全问题或用户提出安全方面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安全标准/技术要求规定的符合性提出质疑时;
- 3) 各类国抽、省抽中相关测试项目结果显示获证产品存在重大安全隐患时。

5.6.4 审核组负责报告监督检查结论。监督检查结论为不通过的,审核组直接向认证机构报告。

监督检查存在不符合项时,持证方应在规定期限内完成整改,认证机构采取适当方式对整改结果进行验证。未能按期完成整改的或整改不通过,按监督检查不通过处理。

5.6.5 认证机构组织对监督检查结论、监督抽样检测结果进行综合评价,评价合格的,认证证书持续有效。当监督检查不通过或监督抽样试验不合格时,则判定年度监督不合格,按照认证机构的证书暂停、恢复、注销和撤销相关程序处理证书。

6. 认证证书

6.1. 证书内容

6.1.1 功能安全产品认证证书的格式采用认证机构通用的自愿性产品认证证书格式,应至少包括(但不限于)以下基本信息:

- 1) 证书类型和证书编号;
- 2) 认证委托人、制造商和、生产企业名称及其场所地址;
- 3) 软件 STL 适用的硬件平台、软件 STL 名称和版本;
- 4) 认证依据,包括获证产品的标准和技术要求;
- 5) 认证的等级(如 Class B 或 Class C);
- 6) 认证模式;
- 7) 不适用条款(如有);
- 8) 证书使用约束和限制说明(如有);
- 9) 认证机构名称、地址;
- 10) 颁证日期、证书有效期;
- 11) 相关的认可标识及认可注册号(适用时);

12) 证书状态的查询方式。

6.2. 证书的有效性

6.2.1 本规则覆盖的产品认证证书的有效期为五年。

6.2.2 在证书有效期内，证书的有效性依靠认证机构的证后年度监督获得保持。认证证书有效期届满有保持证书需求的，认证委托人应在证书有效期届满前 90 天内提出委托。证书有效期内最后一次监督结果通过的，认证机构直接换发新证书，有效期五年。

6.3. 认证的变更

6.3.1 对于获证后发生的以下变更，获证组织应向认证机构发起认证变更申请：

- 1) 证书上的内容发生变化的（如认证委托方、制造商或生产企业的名称、地址变更等）；
- 2) 获证产品发生技术变更（如硬件平台更换、软件安全需求变更、软件版本更新、技术标准更新等）影响依据标准的符合性的；
- 3) 认证依据变更，且有要求需要符合最新认证依据的；
- 4) 除上述以外可能影响获证产品的一致性、符合性的其他类型变更。

6.3.2 认证机构根据获证组织提交的变更申请进行评价，确认变更所需执行或补充的认证活动。

6.3.3 经认证机构评价后（包括已执行所需的功能安全评估和（或）现场检查）符合要求的变更，需要换发证书的，新证书的编号和有效期保持不变，注明变更批准日期。

6.4. 获证单元覆盖产品的扩展

6.4.1 证书持有者需要增加与已获证产品为同一认证单元的认证时应提交申请（如扩充软件 STL 适用的硬件平台）。

6.4.2 证书持有者应针对扩展产品进行差异分析，变更相关设计文档和补充所需的验证活动，必要时认证机构安排功能安全评估和（或）现场检查。

6.4.3 认证机构核查扩展产品与获证产品的一致性，确认认证结果对扩展产品的有效性，评价合格后，根据需要颁发新证书或换发证书。

6.5. 证书的暂停、恢复、注销和撤销

6.5.1 当证书持有者违反认证机构认证有关规定或获证产品不能持续满足认证要求时，认证机构按有关规定对认证证书做出相应的暂停、撤销和注销的处理，并将处理结果进行公告。

6.5.2 证书持有者可以向认证机构申请暂停、注销其持有的认证证书。

6.5.3 证书暂停期间，证书持有者如果需要恢复认证证书，应在规定的暂停期限内向认证机构提出恢复申请，认证机构按有关规定进行恢复处理。否则，认证机构将撤销或注销被暂停的认证证书。

6.5.4 如果恢复认证的条件是做出缩小认证范围的决定，认证机构将对正式的认证文件、公开信息、标志使用的授权等作出所有必要的更改，以确保缩小的认证范围被清楚地传达到客户，并在认证文件和公布的信息中清晰地描述。

7. 认证标志

7.1. 获得广电计量自愿性产品认证证书允许使用如下认证标志：



7.2. 证书持有者使用认证标志应符合认证机构产品认证证书和标志管理的相关要求。

7.3. 标志（印刷/模压等形式）可由获证组织自行印刷/模压，可按照基本式样比例放大或者缩小，但不得变形，不允许施加文字说明，且确保认证标志图案的清晰可识。

8. 收费

认证费用按广电计量自愿性产品认证相关规定执行，由广电计量和认证委托方通过签订认

证合同收取。

9. 认证责任

9.1 广电计量对做出的认证决定负责。

9.2 广电计量对现场审核结果、认证相关报告负责。

9.3 认证委托方应对其所提交的认证申请资料的真实性、合法性负责。

10. 技术争议及申诉

有关申诉、投诉和争议按照广电计量的认证申诉、投诉相关规定处理。

11. 信息公开

见广电计量网站 <https://www.grgtest.com>。

附录 A：术语和缩略语

认证单元：是指产品认证的基本单位。同一认证委托人、同一生产企业、同一类别、同一型号的产品为一个认证单元。对于 IEC 60730-1 或 IEC 60335-1 而言，认证单元即软件 STL 自诊断测试库。

Class B 控制功能：用于防止设备进入不安全状态的控制功能。该控制功能的失效不会直接导致危险情况。示例包括：温度限制器、压力限制器。

Class C 控制功能：指用于防止爆炸等特殊危险的控制功能，或当其失效时可能直接导致设备发生危险的控制功能。示例包括：燃烧器控制系统、密闭式水系统（无泄压保护）的热熔断器。

STL：Self-diagnostic Test Library，STL 是 IEC 60730-1 或 IEC 60335-1 标准中针对 Class B 和 Class C 安全等级的控制器所要求的嵌入式软件自检模块，用于在运行时检测关键硬件（如 CPU、内存、时钟等）的故障，确保控制器安全功能可靠执行。

附录 B：认证申请材料

表 B.1 认证申请材料

序号	资料名称
B.1	产品认证申请书
B.2	质量管理体系资质证明文件
B.3	认证委托方工商注册证明、组织机构代码证或其他证明性文件
B.4	软件安全生命周期要求的所有相关工作产品（如附录 C 所建议）
B.5	认证机构所需其他材料（例如产品适用的其他法律法规标准的声明、适用性声明、承诺书等）

附录 C：软件安全生命周期建议的工作产品清单

表 B.1 软件 STL 安全生命周期建议的工作产品清单

序号	文件	备注
1	软件需求	
2	软件需求确认规范（包括测试用例）	
3	软件需求确认报告	
4	软件架构设计	
5	软件安全分析报告	
6	软件架构设计评审报告	
7	软件架构设计验证报告	Class B 认证时可选
8	软件集成测试规范（包括测试用例）	
9	软件集成测试报告	
10	软件模块设计	
11	软件模块设计评审报告	
12	软件源代码工程	
13	源代码发布说明（Release Note）	
14	静态分析报告	
15	代码评审报告	
16	软件单元测试规范（包括测试用例）	
17	单元测试报告	
18	软件开发环境描述（开发模型、工具、语言、规则、配置参考	

	等方面的描述)	
19	配置管理记录 (版本管理、分支合并管理.....)	
20	变更管理记录 (需求变更、设计变更.....)	
21	STL 用户指南	

备注：上述文件可以依据实际情况进行合理裁剪，包括对上述文件的增加、合并和减少等。

附录 D：IEC 60730 Class B/C 获证产品年度自查表

企业名称：_____

证书编号：_____

自查年度：_____年_____月

D.1 上一次审核不符合项整改确认

检查项	是/否	证据文件（编号/日期）
上次认证或监督的不符合项是否已全部关闭？	<input type="checkbox"/> 是 <input type="checkbox"/> 否	整改报告：_____
整改措施是否有效验证？	<input type="checkbox"/> 是 <input type="checkbox"/> 否	验证记录：_____

D.2 软件变更核查

初次软件版本：_____，

校验码（如 SHA-256）：_____

检查项	是/否	版本信息	校验码（如 SHA-256）
软件是否发生变更？	<input type="checkbox"/> 是 <input type="checkbox"/> 否	当前版本：_____	当前校验码：_____

注：若校验码不一致，必须提交《软件变更说明表》并安排现场监督。

D.3 认证标志的使用

检查项	是/否	证据文件
获证产品是否加施认证标志？	<input type="checkbox"/> 是 <input type="checkbox"/> 否	如是，需提供标志使用图示、认证标志使用记录。
标志图案是否完整、无变形？	<input type="checkbox"/> 是 <input type="checkbox"/> 否	标志使用照片（产品/包装） 编号：IMG_2023XX
是否超范围使用认证标志？	<input type="checkbox"/> 是 <input type="checkbox"/> 否	软件 STL 适用的硬件平台规格书、 用户手册、宣传手册等

D.4 自查结论

- ☐ 无变更, 申请非现场审核 (需提交本表及证据文件)
- ☐ 存在变更, 申请现场监督 (需同步提交变更文档)

企业承诺:

本单位确认上述内容真实完整, 并承担因虚假申报导致的法律责任。

签字 (盖章): _____

日期: _____

文件提交要求:

提前 1 个月提交至认证机构, 附以下文件:

☒ 上次审核不符合报告和整改、验证记录

☒ 软件版本校验工具输出截图

☒ 变更部分的测试报告 (如有)

☒ 标志使用照片 (产品/包装)

☒ 最新证书扫描件

☒ 软件 STL 适用的硬件平台规格书、用户手册、宣传手册等