

家用电器软件评估要求

Requirements of Software Evaluation of Household Appliances

¹ 中国质量认证中心 ² 上海出入境检验检疫局

王会玲¹ 刘晓东² 徐胜² 黄华² 秦晓宇² 章稼新²

摘要

依据 IEC 60335-1:2006 Ed.4.2+IS1:2007 和 IEC 60730-1:2003 Ed.3.1 附录 H 相关软件评估条款的要求,系统介绍了家用电器软件评估技术,包括软件评估的目的和依据,需要进行软件评估的家用电器的方法、术语及所需要的资料;详细介绍了可编程电子电路安全相关的软硬件结构要求与软件检查方法。

关键词

家用电器;软件评估;B类软件;C类软件;结构;故障/错误;措施

Abstract

Based on the relevant clauses of software evaluation on IEC 60335-1:2006 Ed.4.2+IS1:2007 and IEC 60730-1:2003 Ed.3.1 Annex H, this paper introduces in whole the techniques of software evaluation for household appliances, including the purpose and references, those appliances required, the techniques, the definitions and the information for software evaluation; it explains in detail the relevant safety requirements for architecture of software and hardware in programmable circuit and the techniques of software inspection.

Keywords

household appliances; software evaluation; software class B; software class C; architecture; fault/error; measure

引言

家用电器软件评估是指检查嵌入器具的可编程保护电子电路是否使用了合格的软件。如果软件失效会导致危害发生,因此必须通过评估来判定软件是否合格。安全相关的软件结构及相关的硬件布局必须具有避免发生软件错误和控制硬件故障的安全措施,以便软件在器具工作时能够可靠及时地发现并处理会导致危害的故障/错误,保障家电的安全使用,这就是软件评估的目的。

在 IEC 60335-1:2001 Ed.4.1 结构要求 22.46 中首次提出了家用电器软件评估要求:在保护电子电路中使用的软件,应为 B 类或 C 类软件。软件是否合格,依据附录 R (软件评估) 确定。检查程序按照经附录 R 修改过的 IEC 60730-1 附录 H (电子控制器) 的 H.2、H.7、H.11.12 进行。软件评估的内容适用于 IEC 60335-1:2006 Ed.4.2 和 IEC 60730-1:2007 Ed.3.2。

1 软件评估的适用范围

软件评估适用于使用可编程电子电路作为嵌入式控制器的家用电器,控制器除了具有使用功能/性能调节外,同时还有控制安全相关的功能,例如控制非正常工作 and 危险的过热、漏电、爆炸等现象。这类家用电器还应有

根据家电的特点和功能需求开发的集成硬件、软件及相应的外围电路(如电源、驱动元件等),即专用的程序控制板,软件评估不适用于智能控制器的其他外围电路,例如电源部分、驱动部分,该部分按照“第 19 章 非正常工作”考核。如果家电使用了符合 IEC 60730-1 的智能控制器(如起保护作用的智能型继电器式控制器),这种控制器应按照 IEC 60730-1 附录 H 单独检测。

2 软件评估的方法

软件评估的方法有视检和试验两种。

2.1 视检

(1)通过视检生产商提供的资料和样品,检查可编程电子系统的硬件结构和软件结构;

(2)从冗余技术、编码检错、容错设计、故障检测等方面,分析安全相关的程序流程、指令流和数据流;

(3)依据检查数据,评价软件是否结构合适,即是否采取了合适的避免错误和控制故障/错误的措施,以防止不安全现象的发生。

视检涉及的硬件有 CPU、定时器、存储器、内部数据路径、外部通信、输入/输出外围器件、监测装置和比较器。涉及的软件有程序流程、中断服务(故障处理)、自检和/或检测子程序、指令冗余和软件陷阱。

2.2 试验

IEC 60335-1 Ed.4.1 对此没有要求(H.11.12.6 和 H.11.12.6.1),但 IEC 60335-1 Ed.5.0^[1](status:CCDV)提出了具体的要求。在硬件开发阶段,要求生产商进行必要的试验,试验结果作为软件评估的资料提供给认证测试机构。这些试验包括视检(观察)、预审(走查)、静态分析、动态分析、硬件分析、硬件模拟、故障率计算、故障模式与效果分析(FMEA)、操作试验。

3 软件评估的依据

IEC 60335-1 22.46 要求:在保护电子电路中使用的软件应为 B 类或 C 类软件。安全相关的软件失效会导致危害,IEC 60335-1 附录 R 要求控制因软硬件问题产生的错误数据而导致的危害,在研发阶段采取措施避免程序区段中存在的错误。

当器具存在其他故障的情况下,软件失灵应当使用 B 类软件;如果软件单独失灵应当使用 C 类软件。

危害指的是危险的功能失效、电击、火灾、机械或其他危害。

依据附录 R 的评估要求来判断器具是否使用了合格的软件类别。评估程序按照修改过的 IEC 60730-1 H.2、H.7、H.11.12。

IEC 60730-1 H.2-16~H.2.20 是与使用软件的控制器的定义;H.7 是软件评估所需要的资料要求(IEC 60335-1 对此作了修改);H.11.12 是控制器结构要求(IEC 60335-1 对此作了修改),规定了硬件和软件组件的具体配置。要求使用 B 类或 C 类软件的电子电路必须采取措施,控制和避免软件相关的故障/错误,并规定了软件避免错误和控制错误/故障的可接受的措施。这是软件检查的主要内容。

4 软件评估术语

IEC 60335-1 附录 R 采用了 IEC 60730-1 附录 H 的 H.2.16~H.2.20 的定义,但没有采用“H.2.21 软件类别相关的定义”。IEC 60335-1 只给出了 B 类软件(3.9.4)和 C 类软件(3.9.5)的定义,没有给出其他软件(如 A 类软件)的定义。根据 Mr. Derek Johns 关于软件评估的讲义^[2],IEC 60335-1 Ed.5.0 采用了 IEC 60730-1 关于软件类别的定义。本文采用了该讲义关于软件类别的定义。

全部定义共 6 类 76 条,规定了软件类别、硬件结构、避免错误的措施、控制故障/错误的措施、贮存测试方法和软件相关的通用术语。以下定义是进行软件评估的基础。

- H.2.16 与使用软件的控制器的结构相关的定义;
- H.2.17 与使用软件的控制器的避免错误相关的

定义;

- H.2.18 与使用软件的控制器的故障/错误控制技术相关的定义;

- H.2.19 与使用软件的控制器的贮存测试相关的定义;

- H.2.20 软件术语的定义—总则。

根据软件分类方式,为方便起见,控制功能可相应地分为 A/B/C 类功能;故障也可以分为 A/B/C 类故障。

5 软件评估需要的资料

软件评估需要生产商提供标准要求的完整的资料。IEC 60335-1 附录 R 要求按照 IEC 60730-1 表 H.7.2 中的脚注 12)~16)和 18)要求提供资料。

根据表 H.7.2 的要求,通常要求生产商提供下述文件:

- (1) 功能说明,包括掉电后重新启动的程序;
- (2) 产品描述,重点是安全相关软件处理程序部分;
- (3) 带有风险缓解方案的风险分析文件;
- (4) 详细的设计说明,重点是安全相关的寄存器、存储器、接口模式;
- (5) 安全相关的流程图和/或状态图;
- (6) 安全相关软件独立于其他软件的证明;
- (7) 代码表,包括编程语言识别、注释及子程序列表;
- (8) 验证确认试验的测试说明和测试报告;
- (9) 使用、安装和/或维护手册;
- (10) 实现表 H.11.12.7 所选解决方案的证明文件。

6 软件的结构要求

IEC 60730-1 H.11.12 是针对使用软件的控制器的结构提出的要求。下面逐条解释标准的要求和检查方法,即从生产商提供的资料中如何寻找符合标准要求的证据。

(1) H.11.12 使用软件的控制器的结构应使得软件不影响控制器符合本标准的要求

说明:1) 通过 H.11.12.2~H.11.12.13 的结构检查是否符合标准要求,适用于 B 类和 C 类软件。2) 结构检查是软件评估主要内容,检查硬件结构是否合理,努力找出软件中尽可能多的设计错误,是否采取了可接受的避免错误和控制故障/错误的措施。

(2) 是否符合要求通过本标准关于电子控制器的试验、通过按照本要求的观察和通过表 H.7.2 脚注 12)~18)所要求的文件来检查

说明:1) 硬件、软件的功能、结构及故障分析。2) 视检 IEC 60730-1 表 H.7.2 的所有文件和样品。

(3) H.11.12.2 中 C 类软件的控制器应有下述结构之一:

- 带有周期自检和监测的单通道(H2.16.7);
- 带有比较的双通道(H2.16.3);
- 带有比较的双通道 H2.16.2)。

H.11.12.2 中 B 类软件的控制器应有下述结构之一:

- 带有功能测试的单通道(H2.16.5);
- 带有周期自检的单通道(H2.16.6);
- 无比较的双通道(H2.16.1)

说明:1)实现 B 类或 C 类软件的控制功能的硬件结构要求。2)避免错误的措施。3)视检设计说明及样品,检查电路结构是否符合 B 类或 C 类功能的要求。

(4) H.11.12.2.1 允许使用其他结构,只要达到 H.11.12.2 要求等效的安全水平

说明:1)结构要求的扩展,避免错误的措施。2)视检设计说明及样品,检查电路结构是否符合 B 类或 C 类功能的要求。

(5) H.11.12.3 在相同组件的两区域上具有比较的冗余存储器:用不同方式储存

说明:1)软件多样性结构。2)避免错误的措施。3)视检风险分析文件、设计说明和代码表。

(6) H.11.12.4 C 类软件使用有比较的双通道结构:应有附加的故障/错误监测措施

说明:1)C 类功能的硬件要求。2)避免错误的措施。3)视检设计说明和样品:电路结构(电路图、电路板)。

(7) H.11.12.5 非 A 类软件:应提供用于确认并控制在传输到外部与安全有关的数据通道中误差的措施

说明:1)避免数据传输过程中的错误。2)避免错误的措施。3)视检产品描述、风险分析文件、设计说明、流程图和/或状态图、代码表及样品。

(8) H.11.12.6 及 H.11.12.6.1

说明:1)硬件开发过程中的测试要求。2)避免错误的措施。3)不适用 GB 4706.1 附录 R 要求。

(9) H.11.12.7 非 A 类软件功能的控制器:制造商应在控制器内部提供措施,用于寻找表 H.11.12.7 中指出的与安全有关的区段和数据中的故障/错误的地址

说明:1)表 H.11.12.7 列举可编程电子系统中各种组件出现的故障/错误情况及可接受的控制措施,检查软件是否采用适当的措施,及时发现发生故障/错误的部件的地址。部件包括 CPU、中断、时钟、存储器、内部总线、外部通信、I/O 接口、监测单元及常规集成块。B 类软件和 C 类软件采取的措施不同。2)控制故障/错误的措施。3)视检产品描述、风险分析文件、设计说明、流程图和/或状态图、代码表、验证确认试验的测试说明和测

试报告及样品。

(10) H.11.12.7.1 对于使用带有自检和检测功能的单通道 C 类软件的器具,制造商应提供措施,用于寻找表 H.11.12.7 中指出的与安全有关的区段和数据中的故障/错误的地址

说明:1)C 类软件的一个例子,检查方法如 H.11.12.7。2)控制故障/错误的措施。3)视检产品描述、风险分析文件、设计说明、流程图和/或状态图、代码表、验证确认试验的测试说明和测试报告及样品。

(11) H.11.12.8 故障/错误检测应在 GB 4706.1 的 19.13 的试验失败之前进行

说明:1)要求软件发现故障/错误地址前不应发生 GB 4706.1 19.13 规定的危险现象。2)控制故障/错误的措施。3)视检产品描述、风险分析文件、设计说明、流程图和/或状态图、代码表、验证确认试验的测试说明和测试报告、使用安装和/或维护手册及样品。

(12) H.11.12.8.1 故障/错误发现:

- 应在 GB 4706.1 的 19.13 的试验失败之前进行;
- 如 C 类,应提供独立措施。

说明:1)要求发现故障/错误时,控制器在 GB 4706.1 19.13 规定的危险现象发生前做出反应。2)控制故障/错误的措施。3)视检产品描述、风险分析文件、设计说明、流程图和/或状态图、代码表、验证确认试验的测试说明和测试报告、使用安装和/或维护手册及样品。4)C 类功能器具要求提供能执行故障/错误响应的独立措施。

(13) H.11.12.9 C 类,双通道结构,双通道能力的损失:被认为是一种错误

说明:1)C 类功能的硬件问题引起的错误。2)控制故障/错误的措施。3)视检设计说明、风险分析文件,检查是否具有措施应对这个错误。

(14) H.11.12.10 软件应和操作顺序及相关硬件功能的有关部件相关联

说明:1)软件的应用要合理,根据器具的用途和功能来要求软件与操作顺序及相关硬件功能关联。2)避免错误的措施。3)视检功能说明、产品描述、设计说明、流程图和/或状态图、代码表、使用安装和/或维护手册及样品。

(15) H.11.12.11 存储器的位置使用标签:标签是唯一的

说明:1)辨识存储器唯一性的方法。2)避免错误的措施。3)视检样品。

(16) H.11.12.12 软件应被保护以免使用者改变与安全的区段和数据

说明:1)软件安全保护措施。2)避免错误的措施。3)

视检风险分析文件、代码表及使用、安装和/或维护手册。

(17) H.11.12.13 控制所用软件及安全相关的硬件的初始化及终止应在 GB 4706.1 的 19.13 的试验失败之前进行

说明:1)要求安全相关的软件、硬件在启动和停止工作前不发生 GB 4706.1 的 19.13 规定的危险现象。2)避免错误的措施。3)视检功能说明、设计说明、风险分析文件、代码表及使用、安装和/或维护手册。

7 结语

IEC 60335-1 Ed.4.2 和 IEC 60730-1 Ed.3.2 规定了软件评估的程序、要求和方法。目前这两个标准正在修改中。计划于 2009 年 11 月发布的 IEC 60335-1 Ed.5.0 参考和引用了 IEC 60730-1 Ed.4.0^[3]和 IEC 61508 Ed.2.0^[4], 构成了完整的“附录 R 软件评估”程序。有关软件评估的基本要求及技术准备, 大家可参考《家用电器软件评估概要》^[5]。本文不当之处, 敬请读者指正。

参考文献

[1] International Electrotechnical Commission. IEC 60335-1 [5]

(上接第 36 页)

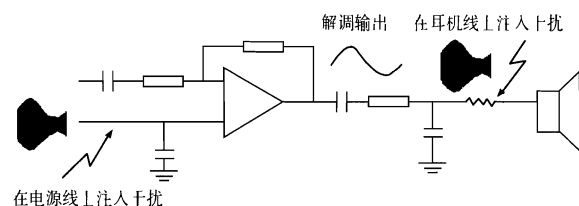


图 5 注入的 AM 干扰在音频下行链路通中被解调、放大

针对上述两种干扰形成的原因, 在研发设计中应采取以下措施:

(1) 对下行链路而言, 耳机左右声道在电路设计上应完全对称, 保持两个通道阻抗平衡, 以避免注入的共模电压转化为差模信号。

(2) 在耳机左右声道电路设计完全对称的情况下, 如果出现了注入干扰影响音频链路, 造成下行测试超标, 应首先考虑是否与音频放大器的抗干扰能力不足有关。在这种情况下, 可以在耳机通道上对地增加纳法级的电容, 构成低通滤波。电容值不宜过大, 一般应在 1~10 nF 之间选取, 否则会对音频信号造成衰减。

(3) 对上行链路而言, 由于测试以共模方式注入, 话筒的回流地上同样存在 AM 的干扰信号, 如果出现上行测试超标, 只对话筒的信号线作处理往往不能够解决问题, 在这种情况下, 需要把话筒的回流地也当作信号线来

Ed.5.0 [EB/OL]. (2008-08-31) [2009-03-10] <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=pro-det.p&proddb=db1&He=IEC&Pu=60335&Pa=1&Se=&Am=&Fr=5&TR=&Ed=5>.

- [2] Derek Johns. SOFTWARE TESTING ACCORDING TO IEC 60335-1 ANNEX R [R]. HANGZHOU: Derek Johns. 2008. 1-16.
- [3] International Electrotechnical Commission. IEC 60730-1 Ed. 4.0 [EB/OL]. (2009-05-30) [2009-07-10] <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=pro-det.p&proddb=db1&He=IEC&Pu=60730&Pa=1&Se=&Am=&Fr=&TR=&Ed=4>.
- [4] International Electrotechnical Commission. IEC 61508-1 Ed. 2.0 [EB/OL]. (2009-07-31) [2009-07-10] <http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=pro-det.p&proddb=db1&He=IEC&Pu=61508&Pa=1&Se=&Am=&Fr=&TR=&Ed=2>.
- [5] 刘晓东, 徐胜, 黄华, 等. 家用电器软件评估概要[J]. 安全与电磁兼容, 2009(1):29-31.

编辑:王颖

E-mail:wangy@cesi.ac.cn

处理。可以尝试在话筒信号线与回流地之间增加共模扼流圈, 以消除注入的共模干扰; 也可以调节话筒信号线与回流地上的共模阻抗, 让两者尽量接近, 以减少由于阻抗不平衡导致共模干扰转化为差模信号的机会。

参考文献

- [1] EN 61000-4-6:1996 Testing and measurement techniques - Immunity to conducted disturbances, induced by radio frequency fields[S]. 1996.
- [2] ETSI EN 301489 -1 -V1.7.1 -2007 Electromagnetic compatibility and Radio spectrum Matters (ERM): Electromagnetic Compatibility (EMC) standard for radio equipment and services: Part 1: Common technical requirements[S]. 2007
- [3] ETSI EN 301489 -7 V1.3.1 (2005 -11). Electromagnetic compatibility and Radio spectrum Matters (ERM): ElectroMagnetic Compatibility (EMC) standard for radio equipment and services: Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS)[S]. 2005.
- [4] Clayton R. Paul 著. 电磁兼容导论(第2版)[M]. 闻映红, 译. 北京: 人民邮电出版社, 2007.

编辑:王颖

E-mail:wangy@cesi.ac.cn