

清华大学 邵贝贝

嵌入式软件的安全可靠性控制

Embedded Software Safety and Reliability Control

嵌入式软件的安全可靠性

不同的嵌入式系统对其安全可靠性的要求是不一样的。一般说来,嵌入式系统对可靠性与安全性的要求要高于非嵌入式系统。对于PC机,偶然死机需要用户重新启动,损失有限。而对于嵌入式控制系统,死机是绝对不允许的。

系统的安全可靠性包含两重含义:一个是强调其安全性,特别是安全紧要系统(Safetycritical)即与人性命攸关的系统,保证安全是第一位的;另一重意思是计算方法要科学,结果要准确可靠,不得有误。表1给出不同安全可靠性要求的嵌入式产品的例子。

尽管不同应用的嵌入式系统对安全、可靠性要求不一样,但制造最好的产品,追求完美,是每个嵌入式开发工程师的愿望。而事实是,为了产品尽快上市,一些嵌入式软件的开发过程,往往是写个程序试一试,功能实现了,开发过程就完成了。程序并没有得到充分测试,隐患就在程序之中。

嵌入式软件的开发通常是由相关行业有经验的工程师完成的,他们对相关产品富有经验,但对于计算机的认识尚达不到计算机专家的水平,写出的程序代码可能存在隐患。

一些应用系统,往往是从功能

简单的系统发展而来的,例如早期的汽车黑盒子产品,仅仅记录一个时段的车速等状态,算不上安全紧要系统。开发者使用单循环加中断完成了基本功能的开发,这个产品就有了。后来,用户提出了更多的功能要求,于是一个个新功能被加了上去,程序变得越来越大,越来越难以维护。到软件安全性受到质疑时,测试和认证变得几乎不可能,只好全部推倒重来。

保证嵌入式软件的安全性,除了在整个软件开发过程中要边开发、边自我检查、测试之外,对于安全紧要系统,需要有专门的程序测试人员,甚至一支与开发队伍并列的测试队伍来保证代码的安全性。

对于航天类设备,既强调安全又强调算法科学可靠,还需要使用专门开发的软件管理、测试来保证其质量,这类商用软件的价格可能高达数万乃至数十万美元。

MISRA 与 MISRA 标准

车辆的安全性是人命关天的,

车辆用嵌入式软件,安全可靠是第一位的,随着汽车电子在车辆控制方面的高速发展,汽车电子用嵌入式软件的安全可靠性变得越来越重要。MISRA 是设在英国的汽车工业软件可靠性协会(Motor Industry SoftwareReliabilityAssociation)的简称。其官方网站为www.misra.org.uk。该协会由欧美的一些著名汽车公司和相关大学、研究机构组成,该机构对车用嵌入式软件的可靠性做了大量研究。1994年,MISRA 出版了其最早的出版物“Development Guidelines for VehicleBasedSoftware”,简称“The MISRA Guidelines”。由于嵌入式软件大都用C语言写成,很多写法在ANSI的C以及相应的C编译器看来并没有什么不可以,但在MISRA看来,在安全可靠性方面存在着隐患。

例如,以下写法在C语言中完全合法:

```
if (a = b && c = d && e = f) {
    满足条件要做的事;
}
```

MISRA 认为,下面的写法才满足可靠性要求:

```
if (a==b) {
    if (c==d) {
        if (e==f) {
            满足条件要做的事;
        }
    }
}
```

表1 不同的安全可靠性对比

	非安全紧要系统	安全紧要系统
算法并不关键	MP3 机顶盒 数码相机	汽车电子设备 心脏起搏器 交通信号系统
强调算法科学可靠	电子皮带秤 激光测距仪 电表	医疗监护设备 航海导航设备 航天器

```

    }
}

```

因为在判断 if (a = b && c = d && e = f) 中 3 个条件看起来是并列的,但在编译和执行中,存在着随意性和不确定性。而 MISRA 建议的写法,结果是唯一的。

更多的例子可参考文献1。

1998 年, MISRA 出版了“Guidelines for the Use of the C Language in Vehicle Based Software”,简称为“MISRA C”。

MISRA 的建议逐渐得到越来越多的嵌入式软件编译器开发商的认同,使 MISRA C 逐渐成为嵌入式软件的标准。如著名的交叉编译器开发商 Metrowerks、Cosmic、Green Hills、Tasking、IAR 等纷纷宣布新版本的 C 交叉编译器支持 MISRA 标准。

早期的 MISRA 出版物列举了 ANSI 的 C 中的 127 条可能的隐患。2004 年 10 月, MISRA 出版了最新的 MISRA-C:2004,“Guidelines for the use of the C language in critical systems”列出的影响可靠性的条款已达 141 项。

软件可靠性及安全认证

对应用安全紧要系统的软件做安全认证是保证嵌入式软件安全可靠的行政手段之一。著名的可以做软件安全认证的单位有很多,例如:

国际电工委员会(IEC)其官方网站为 www.iec.ch。IEC 不但发布和推荐相关国际标准,还提供测试评估方法,其中就包括可编程电子设备的安全性。

美国食品药品监督管理局(FDA)其官方网站为 www.fda.gov,也是著名

的安全性管理部门,对于涉及公众健康的产品以予以认证。

著名的嵌入式实时操作系统 μ C/OS-II 在得到美国航空航天管理局(FAA)的安全认证后才用到了直升飞机上。FAA 的安全认证使用的是 RTCA DO-178B 号文件“航空系统及仪器的软件认证”。RTCA 是“航空无线电技术委员会”的缩写,是一家研究咨询机构。通过 FAA 认证的 μ C/OS-II V2.52 版本源代码,由作者 Jean Labrosse 先生将其附在于 1998 年出版的著作中的光盘上,该书的书名是“MicroC/OS-II The Real Time Kernel (Second Edition)”,其中文译本见参考文献4。


2002 年, Jean Labrosse 发布了 μ C/OS-II 的 2.62 版本。对照 MISRA 标准对 2.52 版本做了升级和改进,声称对 MISRA 标准的符合度为 99%。2004 年,又对操作系统的安全认证做了进一步的说明。目前最新的 μ C/OS-II 的版本是 2.76,见 μ C/OS-II 的官方网站 www.micrium.com。说明通过 FAA 认证,符合 MISRA 标准的软件,也还在不断改进。

全面提高嵌入式软件的质量

提高嵌入式软件的可靠性、安全性,首先是提高嵌入式软件开发人员的素质。开发策略、程序设计、测试手段、安全分析、代码审核都要规范,避免开发工作的随意性、盲目性。

嵌入式 RTOS 是多年来计算机专家们潜心研究的成果,是他们智慧的结晶。把计算机专家的研究成果拿来使用,可以使其开发出来的产品上一个档次。选用经过安全认

证的可靠的实时操作系统开发嵌入式产品,可部分化解系统安全性方面的风险,因为已经被证明是安全可靠的操作系统会承担部分风险。提倡在计算机嵌入式应用中使用实时操作系统,是因为 RTOS 将应用分解成多任务,大大简化了应用系统软件的设计;多任务间可能的竞争问题、任务间通讯问题,有操作系统替用户考虑;RTOS 使控制系统的实时性得到保证,可以接近理论上能达到的最好水平;良好的多任务设计,有助于提高系统的稳定性与可靠性,也使应用程序更便于测试、维护与扩展。

随着半导体技术的迅猛发展,嵌入式系统在各行各业都得到了规范的应用,但嵌入式系统目前还不是一个政府相关部门认可的学科或专业,各个行业的计算机应用水平也很不平衡。特别是对于与性命攸关的安全紧要系统,相关行业协会、研究机构应加强软件管理,软件质量认证工作的研究,向政府相关职能机构提出建议,出台相应的强制性管理措施,以保证嵌入式软件的安全性,提高产品质量,保护消费者的安全。

参考文献:

1. 'User MISRA Guidelines', www.parasoft.com.
2. 'Test Embedded Software', B. Brokman Addison Wesley.
3. 'Software Safety Certification Primer', www.ValidatedSoftware.com.
4. Jean Labrosse 著 邵贝贝译,“嵌入式实时操作系统 μ C/OS-II (第2版)”北京航空航天大学出版社, 2003