# 软件风险控制与评估的重要性

□ 刘晓东　徐　胜　苏旭军　高邱峰

7·23温州动车事故令人震惊。从公开报道看，事故是因为雷击导致信号系统失灵，发生列车追尾惨剧。这个事故反映出我们在关键系统风险控制技术上的现状：缺乏足够的风险意识，缺乏较强的故障监测与控制能力，缺乏至关重要的安全标准，导致研发的产品安全完整性较差，严重影响公众的生命安全和国家的稳定和谐。

这次动车追尾事故，证明铁路系统控制故障的能力不足，软件内缺乏故障监测控制措施或设计不当。据报道，信号系统一般不会做雷击这种破坏性试验，而只做系统功能测试。证实信号系统没经过抗扰度试验就投入使用，这是个非常严重的安全要求缺陷。如果软件具备经过验证的故障控制措施，这种事故是可以避免的。

本文通过概要介绍危机系统风险管理的基础、软件风险控制的要求与认证，旨在表明：在发展的同时，必须提高风险管理意识，积极开发风险控制技术，提高安全完整性，充分保障生命、财产、环境的安全。

## 一、危机系统风险管理的基础

（一）危机系统基本概念和特性

危机系统（Critical system），指的是这种系统的失灵或紊乱会导致生命损伤、财产损失、环境损害。它的基本组成是：满足使用要求的应用功能，这是系统存在的基础；满足安全要求的保护功能，这是对系统应用的保护措施；确保安全功能的风险控制，这是对安全功能的监视措施，在安全功能失灵的情况下，让整个系统进入保护模式。在传统的系统设计中，只包含应用功能和安全功能，而风险控制技术在国内几乎是空白。

危机系统要求具备可靠性、可行性、可维护，同时必须满足安全要求。例如，对于生命危机系统，国际上普遍采纳的最高安全完整等级是$10^9$小时内损失少于一条生命，就是11万年内死亡少于1人，最低要求是11年内死亡少于1人。

（二）危机系统风险来源

风险是行为导致损害发生的可能性，就是出事的概率。对于危机系统，风险的来源主要是方法错误、设计错误、制造错误、运行故障。

1.方法错误：解决问题的方法错误会导致全面的系统性错误，无论其后的设计、生产、调试正确与否，都会产生一定风险，这是一个决策问题。

2.设计、制造、调试错误：这些错误最终体现在产品上。如铁路设计上缺少安全风险控制措施、信号系统不经过电磁抗扰测试等。

3.运行故障：安全相关系统处于故障运行状态，就需要嵌入故障控制措施，避免发生重大灾害。

（三）危机系统风险管理

对于安全相关系统，风险管理主要指的是风险降低措施。要降低风险，需要风险控制技术，包括风险控制措施的开发和风险控制措施的验证两个关键技术。

危机系统通常是由嵌入式微处理器系统构成，无法使用传感器等硬件来探测微处理器内部的故障，可行的方法是在软件中嵌入自检程序，检查硬件故障和软件误差。控制措施的设计原则是：不能影响系统的正常运行，及时发现并处理遇到的故障。

风险控制措施的作用就是检查危机系统出现故障



21994-2018 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

和误差的时刻、位置及应对措施，包括针对方法、设计、制造阶段采取的避免错误的措施；针对运行期间存在的风险而采取的控制措施，即故障、错误控制措施。风险控制技术通常应用非常复杂、精妙的方法、算法。在国内，多数行业没有风险控制措施要求。

控制措施的验证包括产品试验、仿真试验，一般是这两种试验方法结合。故障注入是措施验证的关键技术，要求既不能影响系统的正常工作，又要能够实时、准确地注入待验证部件。目前，国内尚无发现大型故障注入平台。

## 二、软件风险控制的国际与国内现状

（一）软件风险控制的国际现状

关键软件风险控制技术从80年代中期在美国和欧洲国防领域（航空、航天）开展起来，到90年代中期，在民用方面发展很快，广泛应用在航空航天、国防安全、公路铁路及水运、通讯网络、制造业、政府机构、金融机构、产品认证。近年来，这项技术又被广泛应用到与公众关系密切的医疗器械和家用电器中。

在国际上，危机系统开发、检测、认证几乎全部由美、欧、日等国家垄断，这个局面显然不利于中国产品的发展。由于涉及关键机密，各国对关键软件技术保密，所以国内对这方面的信息了解不多。

（二）软件风险控制的国内现状

在我国，由于认知水平的问题，对危机系统风险控制没有进行有规模、有影响力的研究；公众缺乏风险意识，国家缺乏标准要求，企业普遍缺乏风险控制设计能力，认证机构缺乏风险管理评估能力。

GB4706.1–2005《家用电器安全标准》和GB14536.1–2003《家用控制器安全标准》属强制性标准，由于等同采用IEC标准，率先在CCC认证中开展软件评估。除了家电安全标准GB4706.1/GB14536.1外，其他行业还没有正式颁布的标准。

上海检验检疫局机电中心在2008年率先开展了家电软件评估检测项目研究，检测报告获得国内外认证机构的认可。我们联合中国质量认证中心，于2011年启动了软件评估认证项目研究。今年，国家质检总局批准了医疗电气设备和核反应堆安全仪表系统关键软件风险评估技术研究课题，这说明检验检疫系统对保障公众安全具有高度的责任心，对新兴技术具有专业的敏感和认知。

## 三、危机系统测试认证与软件评估

国际上，涉及生命安全的危机系统需要获得认证才能进入市场投入使用。这类系统包括常规民用产品（家用电器、医疗电器、汽车船只等）、大型工业企业（发电厂、核电站、矿产石油开采等），航空航天国防领域；测试包括安全功能效能测试、安全功能风险控制。在功能安全中对风险控制措施进行评估，目的是保障使用系统的安全运行。

软件评估的主要内容是硬件结构检查和软件结构检查，要求硬件结构能够保障故障检测的实施，软件结构要具备监测分析故障的能力。检测内容主要包括硬件故障和软件偏差；检查方法是设计逻辑、代码结构的视检和验证测试；检查的硬件包括CPU、定时器、存储器、内部数据路径、外部通信、输入/输出外围、监测装置和比较器、定制的芯片；检查的故障主要是数字故障（如滞位故障和DC故障）、顺序故障（如寻址偏差和顺序偏差）、时间故障（如频率偏差和时序偏差）、模拟故障（如A/D或D/A数据偏差）。

根据标准的发展，我们已经开展了家用电器的软件评估，并正在进行医疗电器、安全仪表关键软件风险控制与评估技术的研究，计划与国内外有实力的机构开展汽车、列车、能源、金融、通讯、政府等行业的危机系统风险控制技术的开发与评估。

在民生攸关的行业，如铁路运输、医疗电器，我们应该提高风险意识，系统地开展安全风险控制技术研究，特别是在风险控制措施的开发与验证等关键技术方面，应投入足够的人力、物力进行研究与实践。检验检疫系统在产品安全质量检查控制方面发挥着重要作用，我们要充分发挥技术优势，在关键系统风险控制技术方面，在更广泛的领域开展安全软件风险评估业务。

（本栏责任编辑　冯海秀）



?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net