安全问题与安全控制系统综述

The Summary of Security Issue and Security Control System

重庆市科学技术研究院　孙怀义

作者简介：

孙怀义(1965-)，男，陕西旬阳人，1988年毕业于哈尔滨工业大学，学士学位，教授级高工，现任重庆市科学技术研究院信息与自动化技术研究中心副主任，主要从事可靠性设计技术与应用方面的研究。

摘　要：本文分析了目前多数行业面临的安全局势，阐述了安全控制系统的思路与系统架构，综合介绍了森林安全监测与预警控制系统和村镇饮用水安全监控系统，抛砖引玉，供同行参考。

关键词：安全；安全控制；安全控制系统；物联网；传感网

Abstract: For the reference of colleagues, security situation of most industries was analyzed, system architecture and design of security control system were expound, forest security monitoring and warning control system and security monitoring system of drinking water in villages were introduced in this paper.

Key words: security; security control; security control system; internet of things; sensor network

1 安全面临的严峻形势

安全涉及的范围非常广，几乎涵盖了人们日常生活与工作的方方面面。针对不同的对象，安全性的定义也差异很大，但不对服务对象及环境造成伤害，就是安全的。计算机、信息行业、食品行业、交通行业、森林等领域安全问题日益突出。

1.1 计算机安全面临的严峻形势

计算机领域把计算机安全性（security）定义为防止把计算机内的机密文件泄露给无关的用户，必须采取某种安全保密措施，这些措施的有效程序如何就称为计算机系统的安全性或保密性。

计算机安全包括：计算机实体的安全，如计算机机房的物理条件及设施的安全标准、计算机硬件的安装及配置等；软件安全，如保护系统软件与应用软件不被非法复制、不受病毒的侵害等；计算机的数据安全，如网络信息的数据安全、数据库系统的安全；计算机的运行安全，如运行时突发事件的安全处理等。包括计算机安全技术、计算机安全管理和计算机安全评价等内容。

对于计算机网络的安全问题，一方面，计算机网络具有资源的共享性，提高了系统的可靠性，通过分散负荷，提高了工作效率，并具有可扩充性；另一方面，正是由于这些特点，而增加了网络的脆弱性和复杂性。资源的共享和分布增加了网络受攻击的可能性。现在的网络不仅有局域网(LAN)，还有跨地域采用网桥(Bridge)、网关(Gateway)设备、调制解调器、各种公用或专用的交换机及各种通信设备，通过网络扩充和异网互联而形成的广域网(WAN)。由于大大增加了网络的覆盖范围和密度，更难分清网络的界限和预料信息传输的路径，因而增加了网络安全控制管理的难度。

随着计算机的普及，计算机中涉及的个人隐私越来越多，黑客侵入成为计算机应用最大的安全隐患；各种病毒花样翻新，危害性越来越大；各种盗版软件的横行与泛滥，给计算机安全带来了巨大的威胁。

1.2 信息安全面临的严峻形势

“僵尸网络”，借刀杀人

僵尸网络是指黑客利用一台网络服务器，间接并集中的控制感染了僵尸程序的计算机群，这些被控制的计算机叫做“网络僵尸”或“肉鸡”。由于受控制的计算机数目很大，攻击者可以利用僵尸网络在计算机的使用者不知情的情况下，实施信息窃取、拒绝服务攻击等恶意活动。2009年4月，仅国家计算机网络应急处理协调中心监测发现的位于我国大陆的“肉鸡”就有79,491个。

病毒疫情呈连年上升趋势

公安部公共信息安全监察局组织的年度全国信息安全状况计算机病毒疫情调查结果显示，我国信息安全事件发生比例连续3年呈上升趋势。信息安全事件的主要类型是：感染计算机病毒、蠕虫和木马程序，垃圾电子邮件，遭到网络扫描、攻击和网页篡改。从计算机病毒的传播途径来看，通过移动存储介质传播的比例持续上升。虽然通过网络下载或浏览网页感染病毒比例下降，但通过网络监测和用户求救的实际统计结果来看，大量的网络犯

罪通过“挂马”方式进行攻击。

政府信息系统安全面临严峻挑战，安全检查工作制度化、常态化国务院办公厅2008年和2009年连续发文指出，当前境内外敌对势力大肆利用各种手段对我国各级政府信息系统进行网络攻击、破坏、窃密等活动，政府信息系统安全面临严峻挑战。文件要求通过定期展开全面的安全检查应对安全风险，普通工作人员参加信息安全教育培训、掌握信息安全常识和技能，以及对违反信息安全规定行为和造成泄密事故、信息安全事故的查处情况都是安全检查的重点内容。

IP安全受到极大威胁

近年来，国内电信网络已由过去单一的语音交换网络，逐步演进为一个可提供语音、数据、多媒体业务的综合性网络，IP技术成为电信网络的核心。有专家认为，IP技术的应用有助于电信业务的多样化发展，有利于降低网络建设成本、满足用户个性化需求。但基于IP技术的网络有其先天缺陷，开放的网络形式引入了IP技术特有的安全威胁，传统电信网封闭性受到破坏。另一方面，为了实现灵活的网络配置、降低成本，电信设备功能逐渐趋于软件化，很多传统电信设备功能被移植到计算机系统中，一些专用板卡和设备的功能被软件系统所替代。设备软件化引入新的安全威胁，例如，病毒、木马、蠕虫具备了生存环境；复杂的操作系统影响到设备的稳定性和安全性；公开的操作系统安全漏洞以及开放的远程端口易被恶意人员利用，等等。

随着3G网络IP化、宽带化建设进程的完成，使得移动网络也将面临与互联网类似的安全性问题。特别是用户终端种类的多样化，手机、PDA、计算机等都可直接接入3G网络，给恶意攻击者提供了更多灵活的接入方式和强大的终端能力。另外，3G网络可提供更丰富的业务内容，用户能够灵活地上传和下载各种数据、语音、多媒体业务，基于业务内容的信息安全问题也将随之出现。工业和信息化部电信研究院吕军指出，3G应用所带来的安全威胁远远大于2G时代的移动通信网。

垃圾信息威胁网络安全

当前，电信网、互联网等信息网络融合度越来越高，信息技术、业务形式越来越丰富，安全隐患也随之增多，例如：电子商务、网上银行、手机支付等业务可能造成个人账号被窃和网上欺诈；网上社区、手机交友、虚拟世界可能引发虚拟犯罪、国家或商业机密泄露；而网络视频、个人博客等被广泛应用的同时，也为非法、色情内容的大面积扩散提供了新的渠道。

据12321网络不良与垃圾信息举报受理中心报告，2009年7至9月份连续3个月，我国垃圾和不良信息举报数量持续走高，仅9月份就收到不良与垃圾信息举报12万多起，其中互联网24000起，移动通信网和固定通信网加起来近10万起。垃圾邮件、垃圾短信、色情、骚扰电话等垃圾与不良信息，在占用大量通信资源、严重影响人们正常生活的同时，更伴随着潜在的安全风险和社会不稳定因素。据吕军提供的数据，全国固定和移动电话用户数量突破10亿。2008年全年有记录可查的骚扰电话数量就超过了9000万次，而未被发现的骚扰电话数量据估计至少超过2亿次。在一些特定时期，骚扰电话被作为一种技术攻击手段，干扰国内行政机关的正常工作开展。

信息骚扰从互联网向传统电信网络转移，这是一种值得重视的动态。由于传统电话网络通信的实时性、安全性需求高，用户的信息和通信内容受法律保护，如何在用户无感的前提下，在海量的电话通信信息中找到骚扰电话并进行实时拦截处理，同时又使技术方案易于部署、快速灵活，不影响电信网络正常业务的进行，成为我国网络与信息安全工作的新主题。

1.3 生产安全面临的严峻形势

安全生产作为保护和发展社会生产力、促进社会和经济持续健康发展的基本条件，是社会文明与进步的重要标志和全面建设小康社会的本质内涵，也是提高国家综合国力和国际声誉的具体体现。我国面临的新形势、新机遇和新挑战，对安全生产工作提出了很高的要求和期望。提高安全生产是促进国民经济和社会的可持续发展的重要保障。

2003年12月23日，在重庆市开县高桥镇川东罗家16井发生的天然气“井喷”事故，使人们再次感受到现代大型工艺装置、大型设备生产过程中潜藏的巨大威力，同时人们也真实感受到生产过程潜藏巨大能量失控带给人们的灾难——大量的人员伤亡、巨大的财产损失、严重的社会恐慌和沉重的心理压力。2002年，全国发生各类事故107余万起，死亡人数近14万，每天平均死亡380余人；平均每天发生7.2起一次死亡3～9人的重大事故，每周发生2.5起一次死亡10人以上的特大事故，每月发生1.2起一次死亡30人以上的特别重大事故。工矿企业中，以煤矿安全生产形势最为严峻，事故起数与死亡人数分别占全国工矿企业总数的31.12%和46.87%，一次死亡10人以上特大事故分别占全国工矿企业的86.15%和86.31%。危险化学品的安全管理也不容乐观，2002年，全国发生化学事故592起，死亡1551人，同比均有增加。更应注意的是，2002年事故死亡人数超过5000人以上的10个省基本都是经济大省，其中8个省的事故死亡人数增加幅度超过GDP的增长幅度。除了工业生产过程的工艺、设备和管理方面存在的不足外，对于危险源的生产过程中危险因素的辨识和评价缺乏系统的方法，以及可借鉴的相关标准和要求，对于危险产生的原因认识深度不够，应急计划和措施准备不足。

安全生产科技基础薄弱、安全科学技术落后于生产技术的发展，是我国安全生产形势严峻的重要原因之一。目前，国内生产企业面临的危险源还很多，事故隐患和风险时时存在，若没

有有效的预防和应急措施，后果不堪设想。

1.4 食品安全面临的严峻形势

俗话说：民以食为天。这深刻道出了食品对人类生存和发展的重要性。食品安全，关乎每个人的健康和生命。能否保障食品安全，让人吃得健康、吃得安全，对老百姓来说是“天大的事”。

某资料显示，在2011年，全国侦破食品安全类犯罪案件5200余起，抓获涉案人员7000余人，286人被判处有期徒刑、无期徒刑或死缓。这一食品安全整治的“战绩”公布后，引起了社会的广泛关注和讨论。人们在对“整治风暴”拍手称快的同时，也表达了对食品安全问题多发频发的担忧，对保卫餐桌更加强烈的期待。

2012年年初，有两组数据引起人们广泛关注。一组是调查数据：有80.4%的人对食品没有“安全感”；一组是检测数据：国家质检总局发布我国食品检测合格率超过90%。这看似矛盾的两个数据，恰恰反映了当前我国食品安全现状：总体稳定向好，问题不可忽视。

许多国家的发展历程表明，一个国家的食品安全水平与其经济社会发展阶段密切相关。当前，我国正处于发展转型时期，也处于从保障食品供应转向保障食品安全的进程中。这个阶段，食品安全问题往往多发易发。究其原因，主要有以下几个方面。

食品产业小、散、乱突出。我国是食品生产消费大国，食品生产经营者有1000多万户。但产业素质总体较低，80%以上是10人以下的作坊式小企业，还有2亿多农产品种植养殖户。如生猪养殖，美国养猪户数为7万，而我国有6700万。生产经营者规模小、数量多、分布散，不仅自身安全管理意识和能力较弱，也给监管带来很大困难。

从业人员素质不高。与其他行业相比，食品行业从业人员素质相对较低。据统计，我国从事农产品生产的3.4亿人中，文盲和小学文化程度者约占40%；食品工业和餐饮行业1600万从业人员中，85%以上是受教育水平相对较低的进城务工人员。从业人员缺乏法律意识和专业技能，加大了违法违规的概率。

违法犯罪成本过低。“法不足畏”，往往使一些人逐利而往、知法犯法。如对不法企业的经济处罚，2011年以前上限为“货值金额十倍以下”或“十万元以下”罚款。2010年查处一起案件时，违法企业总经理叫嚣：“最多判我三年就出来了。”同年另一起“窝案”中，有超过20%的涉案人员属于再犯。

监管存在薄弱环节。与食品安全严峻形势相比，监管执法存在“短板”。如多头管理体制，容易产生“人人都管事、事事无人管”的监管盲区。监管人手不够，执法装备匮乏，“眼观目测”难以发现安全隐患。安全标准、检验检测、风险监测等技术体系还不完善，很难实现事前防范、科学管理。另外，有的执法人员法制观念淡薄，存在有法不依、执法不严现象。

1.5 森林安全面临的严峻形势

森林是涵养水源，保持水土、调节气候，增加雨量、防风固沙，保护农田、保护环境，净化空气、减低噪音，美化景观、提供产品，材料，燃料，增加肥源的重要资源，也是天然的制氧机，是人类密不可分的朋友。

随着社会进步和生活水平的提高，旅游休闲成为日常生活的重要组成部分。而旅游资源多数离不开森林。

因此森林安全非常重要。但森林火灾一直是不可回避的常发型灾害，必须采取措施，预防和控制森林火灾，提高森林安全。以重庆2010年上半年的数据为例，重庆市共发生森林火灾91起，其中一般森林火灾70起，较大森林火灾21起，火灾造成3人死亡，死者均为火灾肇事者。

据统计，2009年全国共发生火灾12.7万起，死亡1076人，受伤580人，直接财产损失13.2亿元（不含央视新址园区火灾损失）。

1.6 交通安全面临的严峻形势

随着我国交通事业的飞速发展，交通事故发生率呈直线上升趋势。由于交通事故不仅造成大量人员伤亡，给无数的家庭带来不幸，而且严重影响着经济社会的发展和社会稳定。

我国从1951年开始统计交通事故，当年全国共发生交通事故5922起，死亡852人，伤5159人。直到1984年，交通事故发生频率基本保持平稳。八十年代以后，由于交通业的飞速发展，交通事故及死亡率急剧上升。到2002年，全国一般以上交通事故77.31万起，造成10.94万人死亡，56.21万人受伤，直接经济损失33.24亿元。

最近几年，车辆已经进入普通百姓家里，车辆数量的激增，造成交通事故发生的数量更是触目惊心。交通安全问题的解决迫在眉睫。

2 安全控制系统架构与思路

解决安全问题制定相应的法律法规和规程是重要手段之一，计算机安全和信息安全必须以法律法规和规程来规范使用行为，还要采取必要的安全措施；食品安全则不仅需要有相应的法律法规和规程来规范行为，还必须配套相应的安全检测手段，对安全要素实行一票否决，杜绝不安全食品进入流通领域；交通安全是个复杂的课题，交通安全控制系统的研究方兴未艾，我院信息与自动化技术研究中心正在开展相关的研究，已经取得了阶段性成果；对于生产过程以及特种行业，安全控制系统的应用则是解决安全问题的主要手段。

生产安全控制系统的结构与普通控制系统架构类同，仍然由信息采集、信息传输、信息处理与控制三大部分组成，但检测与控制的对象不同，选用的硬件产品要求也不同，安全控制系统检测与控制的对象是危险源和危险传输渠道，构成安全系统的硬件产品也必须满足安全级别的要求。

安全控制系统重点实现生产过程的安全控制。因此在检测层重点是故障信息以及各种危险信息的检测，在智能处理层重点是对故障影响以及危险状况的分析与诊断；在控制层重点是对故障造成危害的及时报警和应急处理。

安全控制系统的技术焦点在于首先系统本身必须是安全的，其次是对检测的信息真实性的识别，再次是对该信息造成的危害的准确性评估，最后是应急处理措施的及时性、有效性和安全性。

以前的国际安全标准是不允许在自动化控制系统中包含安全控制系统的。但是，随着安全技术的发展，使用软件来实现工业安全的国际标准(IEC61508)　最近已经出台，有理由相信相关的国际安全标准和国标会陆续出台，必将促进安全控制系统在我国的全面发展。

生产过程的安全控制系统国内各大自控系统集成商正在开展相关的研究与推广，国外有关自控系统公司已有部分安全控制系统进入中国市场推广应用。针对不同的行业，安全控制系统因控制要素的差异而不同，重庆市科学技术研究院与重庆英卡技术有限公司联合研制的森林安全监测与预警控制系统和与重庆工业自动化仪表研究所联合研制的饮用水安全监控系统已经得到推广和应用。

3 森林安全监测与预警控制系统

森林安全的重要性不言而喻，要确保森林安全，就必须在火灾早期能准确发现并实施控制。因此，森林防火安全重在预警。目前国内从事森林安全预警控制系统的集成商很多，但多数采用视频信息采集的方法，由于视频信息传输过程困难，同时风向对视频信息采集的准确性和稳定性也影响很大，造成预警准确率和及时性不佳。

重庆市科学技术研究院与重庆英卡技术有限公司联合研制的森林安全监测与预警控制系统是一种无线传感网预警系统，由JTG-HW型红外火焰探测器（自主研发）、SR型预警基站和物联网服务平台三部分组成。本系统综合运用红外探测、人工智能、传感网络等现代高新技术，主要部署在林区的人行道、车行道和农业生产周界及纵深，形成防火传感网络，感知早期森林火灾现象，提供全天候、全自动、全实时的早期森林火灾监测与预警，可自动定位火灾未知，实时动态测算火灾蔓延的速度、方向和范围。森林安全检测与预警控制系统工作原理图如图1所示。

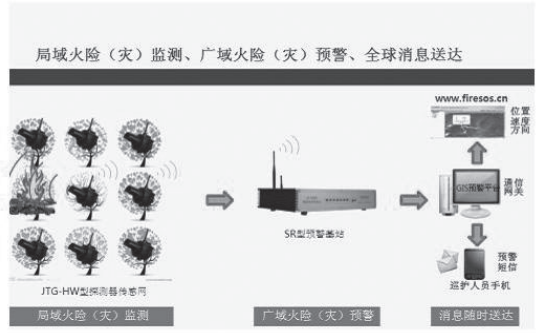

图1 森林安全检测与预警控制系统工作原理图

4 饮用水安全控制系统

饮用水安全是涉及到每一个人的头等大事。城市用水已经采取了相应的手段，对水质进行了严密的检测和监控，确保饮用水安全。但存在几个问题：

城市高楼供水因需要二次加压，输水管道如果使用时间过长后，容易造成二次污染，但后端缺乏水质安全监测，到使用者终端是否安全不得而知；

城市水厂监测装备基本上采用进口装备，价格昂贵，造成供水成本的增加；

有些用户采用的劣质净水装置不仅达不到净化水质的目地，反而造成二次污染。

更为严重的是多数村镇饮用水只是简单的加药，既不检测关键参数，也未进行实时监控，无法保证饮用水的安全。

基于上述需求，重庆工业自动化仪表研究所从2007年开始进行对饮用水安全监测与控制系统及相关产品的研究，2009年与重庆市科学技术研究院信息与自动化技术研究中心展开深度合作，着力于低成本高精度水质监测传感器的研究，从水质安全的源头着手，研制完成了村镇饮用水安全监控系统，目前已经在多个村镇水厂使用，取得了良好的使用效果。

5 结束语

目前，安全控制系统的研究开发在国内还处于初期阶段，安全评价方法和相关标准还极度缺乏，针对不同的对象，安全要求不同，因而安全控制系统也有一定的差异，相信在不久的将来在国内呈现百花齐放、百家争鸣的局面，为我国各行各业的安全和我国经济社会的又好又快建设和发展提供安全保障。

由于资料有限，一叶障目，欢迎各界专家批评指正。

（下转第36页）

4 现场总线对系统可靠性影响的分析

从直观常识对比看，在现场执行的控制回路可靠性比传统DCS更高些。如表2所示。

表2 现场执行的控制回路可靠性与传统DCS的比较

故障模式	对传统系统影响	对现场执行控制的总线系统影响
变送器故障	回路失控，系统可能不知道	进入故障安全模式
定位器故障	回路失控，系统可能不知道	系统自诊断，知道故障
控制器故障	回路失控，也无法监视	回路正常，但无法监视
电缆故障	有 2 根，不能坏	仅一根，不能坏
电源故障	不允许	不允许

Andy Clegg博士还利用“故障树-fault tree”分析方法计算出图2系统在控制器实现控制安全回路的平均无故障时间（MTBF）是15.9年，而在现场实现则达到48.2年，下图是FTA的顶部。如图6所示。

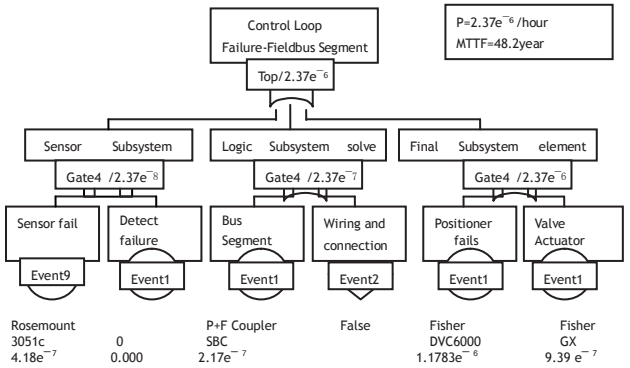

图6 现场总线回路可靠性FTA分析图（顶部局部）

目前控制系统接入现场总线的结构有两类。一类是在传统DCS结构上通过H1或HSE接口卡。如果我们没有接这些卡件，那么系统就是传统DCS结构。我称之为“外延”式结构，例如图2系统。另一类是主控制器CPU同时就是H1和HSE接口。但这个卡件也可以通过背板总线连接传统I/O卡件。如果我们没有使用总线现场设备，那么系统就是基于FF通信和功能块协议的DCS结构。我称之为“内涵”式结构。下图是控制器和H1总线均冗余的结构。如图7所示。

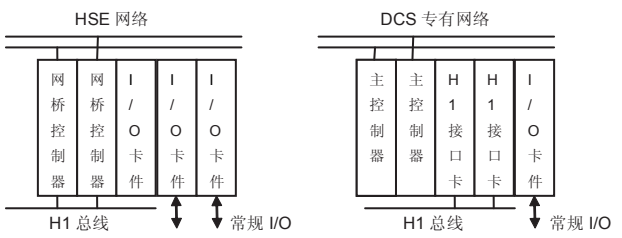

图7 两种接入现场总线的系统结构

根据FTA思想方法，我们可以对这两种系统结构的可靠性简单进行对比。由于没有专业数据库支持，我们简单的将系统部件失效率分为p1、p2、p3三类。其中复杂的控制器类失效率最高为p1，总线接口，电源为中等失效率p2，相对简单的传统I/O卡和背板的失效率最低为p3。如表3所示。

表3 外延结构po与内涵结构pi的比较

系统结构	电源	主 CPU	总线接口	背板	n 块传统 I/O
外延结构 po	p2* p2	p1* p1	p2*p2	p3	n*p3
内涵结构 pi	p2 *p2	p1* p1		p3	n*p3

为提高系统的可靠性，重要的部件如控制器电源等都采取了冗余措施，所以它们整体的失效率被相乘以后（p1* p1）就变得更低了。

Po= 2*p2* p2+ p1* p 1+(n+1) * p3

pi= p2* p2+ p1* p 1+(n+1) * p3

显然pi<Po，即内涵结构因减少一个环节而失效率相对较低。

5 结论

综上所述，控制在现场设备实现是基金会现场总线技术所特有的技术，它不但是更可靠的而且控制性能也是更好的。

参考文献：

[1]Dr Andy Clegg,Control in the Field:Ananlysis of Performance Benefifs ,ISC Ltd May 2010 Fieldbua Foundation

（上接第33页）

参考文献：

[1] 佚名.中国道路交通安全现状[EB/OL] . http://wenku.baidu.com/view/a619d8f8770bf78a65295445.html.

[2] CNET科技资讯网.工业控制系统安全体系架构与管理平台[EB/OL]. http://www.cnetnews.com.cn/2012/0301/2081345.shtml.

[3] 孙怀义,石祥聪.可靠性、安全性与功能安全的关系研究[J].机械与电子，2010,7(1): 23-28.

[4] 孙怀义,石祥聪.自控系统综述[J].自动化与仪器仪表，2011,(1)：1-9.

[5] 通用电气智能设备(上海)有限公司.PAC8000安全控制系统SafetyNet在西气东输火气系统中的应用[J].国内外机电一体化技术, 2011,(5): 38-40.

[6] 张钊谦，吴重光.安全控制系统的设计思想[J].安全与环境学报，2002,2(6):23-25.