DOI:10.3969/j.issn.1009-6868.2017.06.012
网络出版地址:http://kns.cnki.net/kcms/detail/34.1228.TN.20171108.1844.002.html

智能工业装备操作系统技术及创新

Technologies and Innovations of Intelligent Industrial Equipment Operating System

崔云峰/CUI Yunfeng
钟卫东/ZHONG Weidong
刘东/LIU Dong
(中兴通讯股份有限公司,广东 深圳 518057)
(ZTE Corporation, Shenzhen 518057, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2017) 06-0056-005

摘要: 针对工业技术的发展和中国制造2025发展规划,探讨了智能工业装备操作系统的重要性和意义。围绕智能工业装备的4种关键需求(关键性能、智能化、信息安全、功能安全),中兴通讯提出了智能工业装备操作系统及其创新方案,通过5种创新技术(安全可信的微内核架构、嵌入式虚拟化技术、健康管理技术、智能互联技术、安全防御技术)解决智能装备的关键需求,并将在通信、汽车、工业控制等诸多领域促进智能工业装备发展。

关键词: 智能工业装备;实时操作系统;微内核;嵌入式虚拟化

Abstract: In this paper, the importance and significance of the operating system of intelligent industrial equipment are discussed. Focusing on four key requirements of intelligent industrial equipment including key performance, intelligence, security and safety, the intelligent industrial equipment operating system and its innovative scheme are proposed by ZTE Corporation. In this way, key requirements of intelligent equipment are solved by five innovation technologies, such as safety credible micro-kernel architecture, embedded hypervisor technology, health management technology, intelligent ecosystem and interconnection technology, and security technology. Furthermore, the development of intelligent industrial equipments including communications, automotive, and industrial control should be promoted too.

Key words: intelligent equipment; real-time operating system; micro-kernel; embedded hypervisor

1 智能工业发展趋势

信息化和工业化的发展以及深度融合,将在世界范围内带来深刻的变革。以物联网、大数据、人工智能为代表的新一代信息技术与现有工业进行深度融合,并推动工业技术变革。全面和持续的技术变革必将改变产业格局,因此部分发达国家相继颁布再工业化战略,国际竞争日趋激烈。

中国连续多年制造业总产值世界第一,成为世界的制造大国。但中国与先进国家相比还有较大差距:创新能力弱,关键核心技术与高端装备对外依赖度高;产业结构不合理,高端装备制造业和生产性服务业发展滞后;信息化水平不高,与工业化融合深度不够;产业国际化程度不高,企业全球化经营能力不足等。

为了推进中国从制造大国向制造强国的转变,国务院组织编制并正式发布了《中国制造2025》,对中国制造业转型升级和跨越发展作了整体部署,总体分三步走的战略规划。为了力争到2025年达到国际领先地位或国际先进水平,《中国制造2025》选择了十大优势和战略产业作为突破点,包括:新一代信息技术产业(含芯片、操作系统、信息通信等基础产业)、高档数控机床和机器人、航空航天装备、海洋工程装备及高技术船舶、先进轨道交通装备、节能与新能源汽车、电力装备、农业装备、新材料、生物医药及高性能医疗器械。

新一代信息技术产业是其他行业发展的基础,而操作系统是整个智能工业发展的核心基础。在《中国制造2025重点领域技术路线图》中也明确指出:"新一代科技革命与产业变革是以数字化网络化智能化为特征,操作系统是工业数字化网络化智能化的基石,是新一轮工业革命的核心要素。"《中国制造2025重点领域技术路线图》中对智能工业装备操作系统领域有明确的规划:"到2025年,绝大部分核心技术取得突破,形成自主可控的操作系统与工业软件及其标准体系,自主工业软件市场占有率超过50%"。

2 智能工业装备操作系统的关键需求

智能工业装备操作系统作为底层的基础软件,存在两个方面的需求来源。首先需要满足传统嵌入式系统的功能和性能需求;其次是由物联

收稿日期:2017-10-11
网络出版日期:2017-11-08

网、大数据、人工智能等新技术引入的智能化的功能和性能需求。总体来说包括4方面需求，如图1所示。

（1）关键性能需求。首先，智能工业装备由传统的嵌入式实时系统发展而来，系统具有明确的硬实时需求。例如：高速行驶汽车上自动驾驶系统属于硬实时系统，需系统及时处理外部事件，否则可能造成不可预期的后果。其次，嵌入式实时系统存在严格的确定性需求。系统的某些关键业务必须在确定的时间内完成。Windows、Linux、Android等桌面操作系统或手机操作系统，采用相同的软硬件，有时业务运行快，有时业务运行慢。而嵌入式系统中的关键任务需要明确固定的执行节奏，从而保证系统行为的确定性。

（2）智能化需求。首先，智能工业装备引入互联网、大数据、人工智能等新技术，这些新技术需要操作系统提供开放的智能软件生态。新技术多数从IT行业发展而来，依赖开放的智能软件生态，例如：Android的应用生态、深度学习软件生态等。其次，智能工业装备可能由多个系统相互协同完成工作任务。因此需要底层操作系统提供互联互通技术，以及进一步提供互操作互调用的机制。

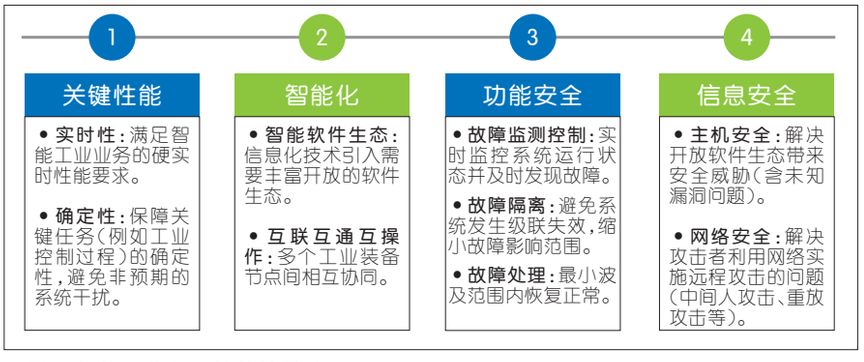
（3）功能安全需求。部分嵌入式系统涉及到行业以及个人生命安全，例如：工业控制设备、轨道交通控制设备、汽车自动驾驶系统等。对于这类系统需要进行系统全面的失效分析，从失效概率、危害大小、危害可控性等维度评估出业务模块的功能安全等级。需要底层的操作系统符合响应功能安全等级的要求，并且提供故障监测控制、故障隔离以及故障恢复的功能。

（4）信息安全需求。开放的软件生态环境以及互联网技术引入到嵌入式实时操作系统上，也给现有封闭的嵌入式系统带来了安全隐患。大规模的开放软件生态环境可能含有安全漏洞、未知后门；高速的以太网接入方式也给黑客提供了便捷的攻击路径。但是嵌入式系统的网络安全问题不能直接照搬IT领域的安全解决方案，需要考虑到现有嵌入式系统的实时性、确定性要求；同时频繁升级、打补丁会影响系统可用性，因此同样不适用于嵌入式系统。

3 中兴通讯智能工业装备操作系统及技术创新方案

中兴通讯立足于自主创新，从2003年开始研发自主可控的嵌入式操作系统，经过10余年的积累掌握底层操作系统的核心技术。中兴通讯所研制的电信级嵌入式实时操作系统于2016年荣获了第4届中国工业大奖（工业领域最高荣誉），并于2017年荣获了国际软件博览会金奖。目前中兴嵌入式操作系统广泛应用于通信、电力、轨道交通、汽车、航空等众多工业领域，累计发货量达到2亿，稳定运行于全球160个国家和地区。

针对智能工业装备的关键需求，中兴通讯自主研发了智能工业装备操作系统ZEOS。如图2所示，中兴智能工业装备操作系统以安全可信的微内核架构和嵌入式虚拟化技术为支撑，同时具备实时操作系统和嵌入式Hypervisor的功能。通过健康管理技术实现故障隔离、运行状态监测控制、故障恢复，保障系统持续稳定运行；通过面向服务的互联网络架构支持多种异构系统互联互通，并借助虚拟机支撑智能应用生态；通过内建的安全可信体系架构保障基础系统安全可信，引入移动目标防御技术防御未知威胁。



▲图1 智能工业装备的关键需求

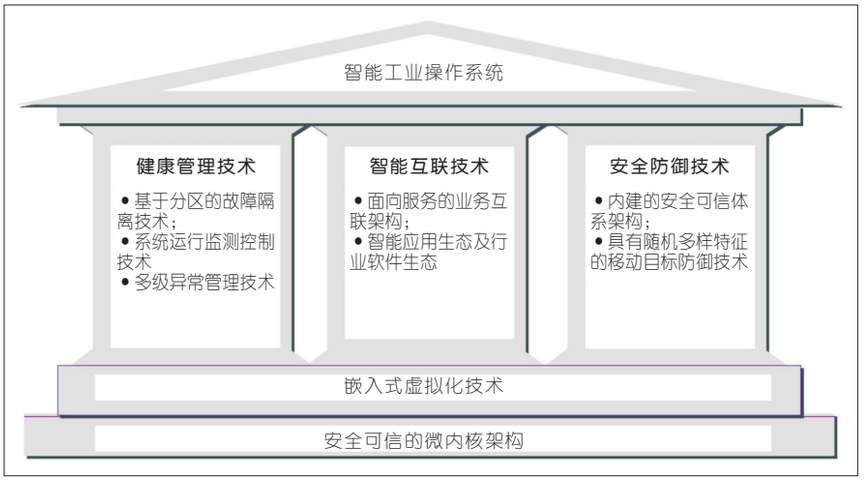
3.1 安全可信的微内核架构

中兴通讯从关键需求出发，研究系统实时性、确定性的关键影响因素以及内核各个模块的代码变更和质量特征，得出智能工业装备操作系统的微内核软件架构。依据安全系统的最小特权原则（POLP），建立智能工业装备操作系统的可信计算基（TCB）。如图3所示，在处理器最高特权模式下仅保留少量的核心功能模块（空间管理、线程管理、进程间通信机制、中断管理部分）作为系统的可信计算基；其余的操作系统功能模块运行于普通模式（普通模式）。以此基础架构为支撑，中兴智能装备操作系统提供实时操作系统功能和嵌入式虚拟化功能。

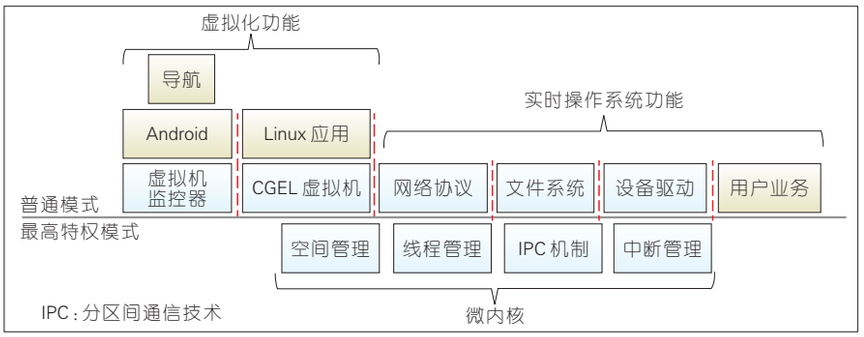
智能工业装备操作系统的基础架构有利于保障智能工业装备的关键需求，例如实时性、确定性、功能安全、信息安全。

（1）实时性：利用微内核的软件架构可以保障硬实时性能。通过减少内核功能模块，减少系统关中断、关抢占的频度和时长，从而有效地提升系统的实时性指标（中断延时、调度延时）。

（2）确定性：利用微内核架构可减少后台干扰，保障业务的确定性。从架构设计上减少内核功能模块，减少后台任务和定时器，降低系统自身



▲图2 中兴通讯智能装备操作系统创新技术



▲图3 安全可信的微内核架构

开销，从而保障用户业务的确定性。

（3）功能安全和信息安全：利用微内核架构可隔离核心功能模块和业务功能模块，避免宏内核架构下单个模块故障或安全威胁波及影响整个操作系统。采用微内核架构可将少数稳定的核心模块置于处理器的特权模式下，其他业务功能模块放置于用户态模式下，隔离了高缺陷率的功能模块并缩小了核心模块的对外攻击表面。

3.2 嵌入式虚拟化技术

虚拟化技术已在IT领域广泛商用，但应用到嵌入式设备上有两个方面的挑战：首先是虚拟机的性能问题。嵌入式系统对实时性以及关键业务性能有比较高的要求，引入Hypervisor仍需要保证虚拟机的关键性能。其次，嵌入式处理器发展相对滞后，部分处理器不具备硬件辅助虚拟化特性，需要在传统硬件上提供虚拟化解决方案。

在IT领域广泛使用I型和II型Hypervisor架构：II型架构中虚拟机管理监测控制程序（VMM）作为应用程序运行在主机操作系统之上，虚拟机的性能受主机操作系统和虚拟机监测控制程序的影响；I型架构将虚拟机直接运行在Hypervisor之上，相对而言虚拟机的性能更高。

为了保障虚拟机的性能，中兴智能装备操作系统采用更加轻量级的0型Hypervisor架构。将Hypervisor做的更“薄”：去除去除虚拟机迁移、容灾热备份等IT虚拟化功能特性；仅保留CPU虚拟化、内存虚拟化以及部分外设虚拟化等核心功能；对于性能要求较高的虚拟机或实时业务通过分区隔离机制保障其物理资源分配，从而达到与物理机相近的性能指标。

针对处理器相对滞后（不支持嵌入式虚拟化特性）的问题，中兴智能装备操作系统引入半虚拟化技术。通过对客户机操作系统和底层Hypervisor的深度定制和融合，实现在普通硬件环境下支持多个半虚拟化客户机操作系统（例如Linux、Android）。具体包括了以下技术。

（1）处理器虚拟化：在定制的客户机操作系统中实现了虚拟机处理器架构，并在非特权模式下客户机操作系统与Hypervisor配合完成特权指令的模拟执行。

（2）内存虚拟化：针对半虚拟化虚拟机和全虚拟化虚拟机，分别提供基于影子页表技术和基于硬件辅助虚拟化的内存虚拟化功能，从而保障客户机虚拟机的内存访问性能。

（3）外设虚拟化：对于不同需求的场景提供外设透传技术（高性能使用场景）和外设模拟共享技术（共享使用场景）。外设模拟技术通过Hypervisor模拟多个虚拟外设，并将虚拟外设请求转交给实际物理外设，实现多个虚拟机共享物理外设功能。

3.3 健康管理技术

在通信、汽车、工控、航空、轨道交通等高可靠领域，对于系统的功能安全要求比较高。例如：汽车电子的ISO26262 ASIL D级要求每小时失效概率小于10^{-9}，需要系统底层操作系统提供多种功能安全保障措施。中兴智能装备操作系统从故障隔离、运行监测控制、异常恢复等角度保障系统的持续稳定运行。

3.3.1 基于分区的故障隔离技术

在高可靠领域故障隔离是解决功能安全的核心关键。汽车电子领域ISO26262标准指出避免波及影响的重要性，系统必须提供两个或多个单元发生级联失效的手段。航空航天领域ARNIC653标准提出分区隔离方式支持多种电子应用，通过分区隔

离保障单点失效不影响其他业务。

中兴通讯智能装备操作系统采用微内核架构，对于用户态的不同功能安全等级业务提供分区隔离机制。当某个业务发生故障并失效后，其他分区业务不受影响。如图4所示，具体技术包括：分区间的时间隔离机制、空间隔离机制、权限隔离、硬件隔离机制。

3.3.2 系统运行监测控制及多级异常处理技术

中兴智能装备操作系统提供多种不同粒度的系统运行状态监测控制功能，包括：任务级、分区级、系统级、硬件级的运行监测控制。通过不同粒度的健康监测控制功能可以及时发现不同范围的异常或告警事件，并实时监测控制关键任务的运行状态，确保其运行状态与预期一致。

当发现系统不同类型的故障后，中兴智能装备操作系统提供多级的异常处理机制。通过任务级、分区级、系统级、硬件级逐级处理异常，确保每个异常问题可以在系统最小波及、影响范围内恢复，避免恢复异常造成过大的影响。

中兴智能装备操作系统基于高可靠行业标准设计功能安全特性，及时监测控制系统的运行状态并细粒度地恢复系统运行状态，从而保障高可靠性业务持续、稳定运行。

3.4 智能互联技术

随着工业化和信息化的深度融合，智能化和网络化是智能装备的主要发展趋势。在智能化方面，中兴智能装备操作系统通过嵌入式虚拟化技术引入成熟的开放软件生态，并提供POSIX等基础库支撑硬实时的智能任务；在网络化方面，中兴智能装备操作系统通过分区间通信技术（IPC）打通不同智能节点间的通信通道，通过支持各个行业的互联管理协议支撑多种异构系统的互联互通互操作。嵌入式虚拟化技术已在前述章节描述，在此重点介绍网络互联方面相关技术。

中兴智能装备操作系统采用微内核架构，所有内核功能和业务功能都以服务方式对外提供，并支持本地和远程的连接和访问，具体过程如图5所示。首先由智能应用服务业务向本地服务管理器注册，并由服务管理器发布此服务；再由本地业务通过IPC机制访问服务管理器，并由服务管理器建立服务连接实现本地访问服务功能。远程业务也同样访问服务管理器并查找到服务节点，由服务管理器建立远程服务通信通道。通过此技术实现跨节点的智能互联互操作功能，应用业务可透明使用本地服务或远端服务。

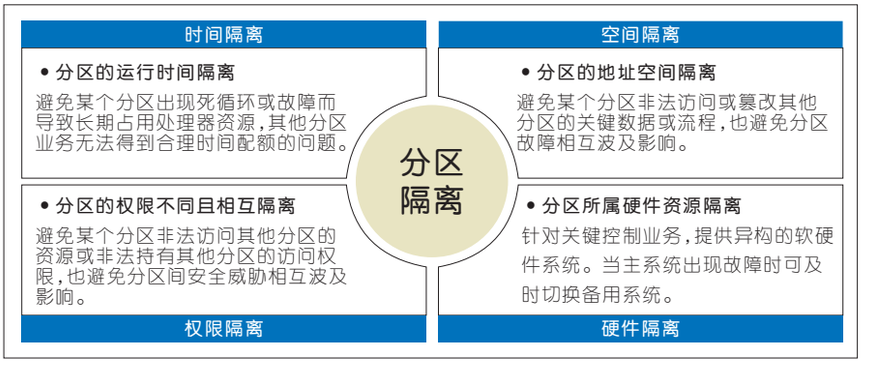
中兴智能装备操作系统针对不同行业需求，提供应用互联互通互操作的业务协议和安全管控协议。例如：在物联网领域的约束应用协议（CoAP）和消息队列遥测传输协议（MQTT）等应用互联协议；在汽车电子领域的AUTOSAR SOME/IP协议；在工业控制领域的IEC62351(传输层安全协议（TLS））。通过上述应用互联和管控协议，实现多种异构系统的相互协同，形成了一个完整的智能工业系统。

3.5 安全防御技术

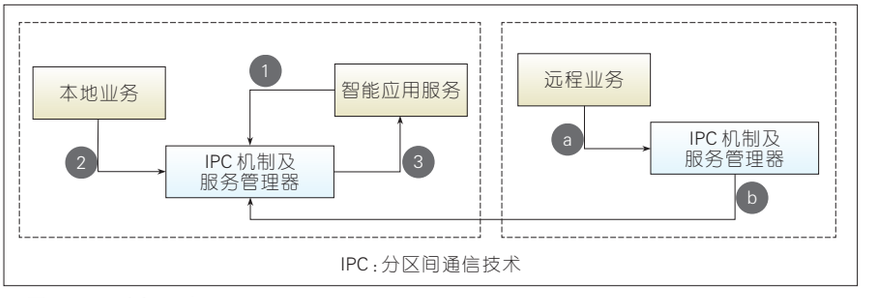
智能工业装备引入开放的软件生态以及互联网技术，也引入了安全威胁：开放的智能软件生态可能包含各种安全隐患（甚至包括未知安全威胁），互联网技术也给攻击者提供了便利的攻击途径。中兴智能装备操作系统基于可信计算的理念，设计安全可信的操作系统体系架构；同时从攻击链入手，利用底层基础软件随机多样的变化改变攻击路径，实现主动防御。利用基础软件建立智能工业装备内生的信息安全机制，无需叠加外部信息安全功能，保障了智能工业装备的实时性、确定性以及关键业务性能。

3.5.1 内建的安全可信体系架构

首先，基于前述安全可信的微内核架构，建立智能工业装备操作系统



▲图4 分区隔离技术功能



▲图5 IPC过程示意

的可信计算基(TCB)。可信计算基从两个方面实现内建的安全可信:一是控制可信计算基的规模和复杂度,杜绝其自身的安全漏洞;二是缩小及加固可信计算基的对外攻击面,采用基于权限映射表的强制访问控制技术实现外部接口的安全控制功能。

其次,中兴智能装备操作系统支持内核分离保护轮廓(SKPP),通过分区隔离机制保障单个分区的安全威胁不扩散。操作系统非核心功能及智能节点业务之间都处于时间隔离、空间隔离、访问权限隔离、多核和外设隔离的运行环境中。单个分区业务故障不会影响到其他分区业务功能。

中兴通讯通过上述技术途径搭建了一个安全可信的体系架构,实现内建的可信体系架构,解决了工业装备系统的核心问题。

3.5.2 具有随机多样特征的移动目标防御技术

高级持续威胁(APT)是智能工业装备面临的最大的安全威胁形式,例如:伊朗震网事件、乌克兰电网事件、康明斯发动机事件等。如图6所示,高级持续威胁攻击过程包括如下4个步骤:系统探测、漏洞挖掘、系统突破、系统控制。通过对此攻击模型分析可以看出,攻击者在攻击过程依赖系统中固定的、一致性的、可预期的系统规律。例如:全局符号布局相对相对关系、关键数据结构的布局结构、关键函数的地址信息等。

中兴智能装备操系统基于移动目标防御(MTD)的思想,打破攻击者所依赖的系统固定的、一致性的规律。通过编译器和操作系统等底层基础软件,实现全局符号随机化、关键数据结构随机化、运行地址空间随机化、异构发布等技术。通过上述技术对整个系统引入随机、多样的变化,使攻击者无法找到系统或漏洞的规律,有效阻断攻击链。

4 结束语

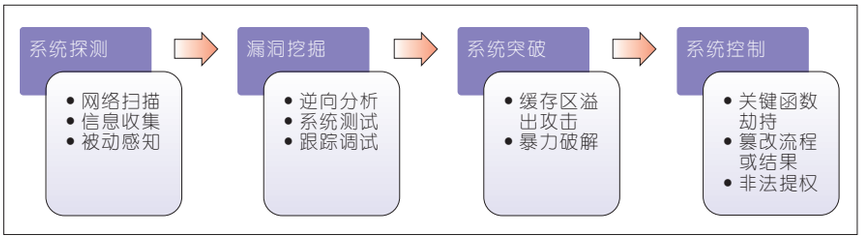
中兴智能装备操作系统通过技术创新,解决了智能工业装备的4个核心需求:关键性能(实时性、确定性)、智能化、功能安全、信息安全。结合智能工业行业特点,提供全面的解决方案。

在电信行业:电信业务中数据面业务可直接运行于中兴智能装备操作系统,由操作系统保障业务的实时性、确定性和吞吐性能;控制面业务和云化网络功能可通过虚拟化方式运行在电信级嵌入式Linux操作系统之上,满足业务对软件生态的要求。

在工业控制行业:首先,中兴智能装备操作系统通过硬实时、高确定特性,保障工控组态业务的实时性和确定性;其次,通过虚拟化技术和电信级嵌入式操作系统支持多个控制器集约化发展,降低产品成本;最后,通过安全可信的体系架构和移动目标防御技术解决工业控制系统的安全问题。

在汽车电子行业:针对车载电子,中兴智能装备操作系统利用虚拟化技术支持"一机多屏",在一个硬件环境上同时支持仪表业务(Linux+QT)和中控台业务(Android),并满足仪表快速启动和功能安全和信息安全要求。针对车控电子,中兴智能装备操作系统利用虚拟化引入自动驾驶软件生态,提供感知、决策的底层中间件;同时多分区的软件架构支持不同功能安全等级的业务,并兼容AUTOSAR行业基础软件标准。

综上所述,中兴智能装备操作系统满足不同行业的智能装备发展的关键需求,为中国制造2025的规划奠定坚实的软件基础。



▲图6 高级持续威胁攻击模型

参考文献

[1] 中华人民共和国国务院. 中国制造2025[R]. 北京: 中华人民共和国国务院, 2015
[2] 国家制造强国建设战略咨询委员会. 中国制造2025重点领域技术路线图[R]. 北京:国家制造强国建设战略咨询委员会, 2015
[3] Lynx Software Technologies. The Rise of the Type Zero Hypervisor[EB/OL].(2012-09-18)[2017-10-08]. http://www.lynx.com/the-rise-of-the-type-zero-hypervisor/
[4] ISO. ISO26262 Part 1[S]. Geneva: ISO, 2011: 11
[5] Aeronautical Radio. ARNIC653 Standards[EB/OL]. (2013-10-20)[2017-10-08]. http://store.aviation-ia.com/cf/store/catalog_detail.cfm?item_id=496
[6] AUTOSAR. AUTOSAR Standards[EB/OL]. (2017-03-31) [2017-10-08]. https://www.autosar.org/standards/

作者简介

崔云峰,中兴通讯股份有限公司操作系统产品部技术总工;主要研究方向为嵌入式操作系统、网络安全等;参与国家重大专项2项,获得国家级、省部级奖励3项;已申请专利10余项。

钟卫东,中兴通讯股份有限公司操作系统产品部部长;主要研究方向为程控交换机、数据通信、操作系统等;承担多项"863"、核高基等项目,获得国家级、省部级科技奖7项;已申请专利20余项。

刘东,中兴通讯股份有限公司操作系统产品部资深研发经理;主要负责嵌入式操作系统产品经营与研发管理;先后参加2项重大专项课题,获得3项国家级科学技术与产品大奖。