

第四届国产嵌入式操作系统技术与产业发展论坛 会议手册

以“**构建安全可靠的工业操作系统**”为主题的第四届国产嵌入式操作系统技术与产业发展论坛暨嵌入式系统联谊会主题讨论会(总第28次)在2022年12月17日(周六)以线上方式举办,知名学者和产业大咖专家云集,嵌入式软件安全技术和汽车操作系统等热点议题成为本次会议关注重点。



论坛主办方:

北京航空航天大学计算机学院
北京航空航天大学杭州创新研究院
中国电子技术标准化研究院物联网研究中心
嵌入式系统联谊会
《单片机与嵌入式系统应用》杂志社

论坛承办方:

北京航空航天大学杭州创新研究院
嵌入式系统联谊会
《单片机与嵌入式系统应用》杂志社

论坛时间:2022年12月17日(周六)9:30-12:00,13:30-17:00)

论坛地点:论坛将采取线上方式举办,演讲与参会均为免费,谢绝纯商业宣传。

主办方直播通道:

腾讯会议 ID: 525244892 (报告人和嘉宾请进入腾讯会议室)



B站和发烧友直播频道(听众可以选择下面的直播频道)



联系方式:

“嵌入式系统小编”的微信号(esbf123)手机:18513907378,
关注“嵌入式系统专家之声”微信公众号访问 www.esbf.org 更多会议内容。

时间	报告题目	报告人
09:25-9:30	暖场和播放历届论坛花絮视频	
上午 学术报告	主题： 嵌入式操作系统安全设计-方法与实践	
	会议主席和主持人：牛建伟 北京航空航天大学计算机学院教授	
9:30-10:00	嵌入式系统安全性的最新技术挑战	李奕骁博士 日本名古屋大学情报学研究科助理教授
10:00-10:30	面向机载航空电子系统的嵌入式实时操作系统	崔西宁研究员 中国航空工业集团有限公司首席技术专家
10:30-11:00	基于订阅者/发布者的微内核操作系统进程间通信的形式化验证	郭建 华东师范大学副教授
11:00-11:30	操作系统的安全认证	赵永望 浙江大学计算机与技术学院教授
12:00	上午议程结束	
13:25-13:30	暖场和播放历届论坛花絮视频	
下午 产业报告	主题： 汽车操作系统技术与生态	
	会议主席和主持人：何小庆 嵌入式系统联谊会秘书长	
13:30-14:00	新一代智能汽车操作系统关键技术	常万里 湖南大学教授
14:00-14:30	车载软件的跨系统融合	熊谱翔 上海睿赛德电子科技有限公司 CEO、RT-Thread 创始人
14:30-15:00	虚拟化技术在汽车电子电气架构中的应用	杨波涛 中瓴智行(成都)科技有限公司产品总监
15:00-15:30	基于微内核架构的自主车载操作系统应用研究	龚鹏程 北京东土科技股份有限公司副总经理兼操作系统 CTO
15:30-16:00	汽车操作系统技术发展与实践	徐贵洲 北京翼辉信息技术有限公司副总经理
16:00-16:45	嘉宾讨论： 发展国产汽车操作系统的机遇与挑战	主持人：芦潇静 《单片机与嵌入式系统应用》执行主编 嘉宾：①周庆国 兰州大学教授、开源软件与实时系统教育部工程研究中心主任②刘寿永 中科创达首席架构师③苑中魁 中汽工程研究院北京院汽车网络与数据安全中心④朱玉龙 汽车产业研究专家
17:00	全天议程结束	

报告人和报告内容简介：（按照论坛议程顺序）

①嵌入式系统安全性的最新技术挑战

摘要：随着物联网及智能化等技术的发展，嵌入式系统的软硬件复杂度不断提升，对安全性的保证带来很多新的挑战。除了传统的单核心 MCU 架构，多核处理器、异构计算、虚拟化、Linux、GPU 等技术也开始被车载和无人机等有高安全性要求的实时系统所采用。本报告中将结合实际应用示例，讨论最新的嵌入式系统的特征、面临的安全性课题以及相关研究方向。

报告人：**李奕骁**

博士，名古屋大学情报学研究科助理教授，在 ERTL（嵌入式实时系统研究室）和 NCES（附属嵌入式系统研究中心）担任硕士博士课题指导及企业合作研究等工作。

2019 年获得名古屋大学信息科学博士学位。主要从事面向机器人、车载、无人机等的嵌入式系统的软件平台、实时系统的安全性提升的相关研究。

②面向机载航空电子系统的嵌入式实时操作系统

摘要:随着计算机技术的飞速发展,航空电子系统至今已经历了分立式、联合式、综合化和高度综合化(IMA)的发展历程。航空电子系统的软件规模急剧膨胀,软件越来越复杂,引发的系统的安全性与可靠性问题也越来越突出。为了适应性高度综合化航空电子系统,具有时间隔离和空间隔离的分区操作系统应运而生,天脉操作系统是一款满足 GJB5357 标准的具有自主知识产权的分区操作系统,已经广泛地应用在机载领域和相关其他嵌入式领域。

报告人: 崔西宁

工学博士,研究员,在航空工业计算所从事机载计算机软件开发工作,中国航空工业集团有限公司首席技术专家。CCF 系统软件专委会常委、软件工程专委会委员、嵌入式系统专委会委员,航空学会高级会员。先后主持和参加了多项预研、型号和核高基项目。在航电系统体系架构、容错重构、信息安全、嵌入式系统等多个领域有深入研究,先后在多项型号、预研项目中做出了突出贡献。发表论文 50 余篇,授权专利十余项,编写了集团标准 7 项,工信部行业标准 HB 5 项,主编了《嵌入式系统设计师教程》。获航空学会一等奖 1 项,部级奖 9 项、集团级 8 项;荣立二等功 2 次,三等功 4 次。

③基于订阅者/发布者的微内核操作系统进程间通信的形式化验证

摘要:事件总线将多线程模型与发布订阅模式结合在一起,实现了多线程与事件驱动两种编程模型。提出了应用 EventB 方法对事件总线进行形式化模型与验证,在每层模型中都对事件总线混合编程模型的安全性和活性进行了证明。通过清晰的模型描述和细致的精化策略设计,整个工作的自动验证率达到了 91%。

报告人: 郭建

华东师范大学副教授,主要研究领域嵌入式系统可信计算及形式化验证,特别是嵌入式实时操作系统,包括 AUTOSAR、 $\mu\text{C}/\text{OS-II}$ 、微内核等 OS 的规范、建模及验证方面的研究。涉及到重写逻辑、模型检验、在线模型检验、B 方法等形式化技术和方法。迄今已发表相关领域论文 60 余篇,申请专利 17 项,其中授权 11 项,获得软件著作权 13 项,2021 年出版“基于 ISO26262 的汽车电子功能安全:方法与应用”。先后获得上海市科技进步特等奖、教育高等学校科学研究优秀成果奖(科学技术)技术发明一等奖等。

④操作系统的安全认证

摘要:操作系统是计算机系统的基础软件,处于软件栈的最底层,它的安全可靠性至关重要。国际上主流嵌入式操作系统大多开展了安全认证以及基于形式化验证的高级别安全认证,包括 DO-178C、IEC 61508 和 Common Criteria 等。本报告主要介绍国内外操作系统的安全认证与形式化验证现状,探讨高级别安全认证的重要性,重点介绍 CC 信息安全认证的产业现状、方法论等。最后,介绍我们开展国产操作系统安全认证的一些实践。

报告人: 赵永望

浙江大学教授、博士生导师,移动终端安全浙江省工程研究中心主任,CCF 杰出会员,CCF 系统软件专委会、形式化方法专委会和抗恶劣计算专委会执行委员,国际 ARINC653 操作系统标准委员会成员等。主要研究方向为形式化验证、操作系统安全、编程语言等,主持和参与工信部重大专项、国家自然科学基金重点项目、载人航天工程重点项目、浙江省尖兵计划项目等二十余项,获省部级科技进步一等奖

2 项。相关成果发表在 ACM TOPLAS、IEEE TDSC 等期刊和 CAV、FM、TACAS 等会议上。

⑤新一代智能汽车操作系统关键技术

摘要：智能汽车对车控、自动驾驶、以及座舱操作系统有不同的实时性要求，总体上需以有限资源实现复杂功能，同时兼顾低功耗与高可靠。本次报告围绕任务调度这一核心，向内存访问与车载通信延展，讨论新一代智能汽车操作系统的若干关键技术。

报告人：常万里

湖南大学教授，国家海外高层次人才，科技部高端外国专家，华为公司嵌入式系统领域首席科学顾问，世界计算机学会 ACM 嵌入式系统专委会 SIGBED 秘书长，ACM 嵌入式系统领域最佳博士论文奖评审委员会主席。常万里教授主要研究嵌入式与实时系统，近三年在该领域顶会发表论文数世界排名第一（csranking 统计），获得 RTSS，EMSOFT 等会议杰出论文奖和最佳论文提名奖，曾任 Bosch 资深专家顾问，与 Raytheon Technologies 等国际主流相关企业有密切交流与合作，主导了面向多核嵌入式与实时系统的多项核心技术开发。博士毕业于德国慕尼黑工大，获最佳博士论文奖，本科毕业于新加坡南洋理工大学。

⑥车载软件的跨系统融合

摘要：汽车电控系统是一个复杂的系统，主题结合当下的汽车架构演变情况，探讨车载软件下的跨系统融合，涉及到 CP AUTOSAR，POSIX RTOS，虚拟化技术，功能安全等。

报告人：熊谱翔

上海睿赛德电子科技有限公司 CEO，RT-Thread 创始人。毕业于重庆邮电大学，国内实时操作系统专家，RT-Thread 创始人，具备 20 年的丰富嵌入式实时操作系统经验，先后在上海海贝尔阿尔卡特、宇梦通信、Marvell 任软件架构师，软件研发经理等职位。于 2006 年创立了 RT-Thread 开源操作系统，并以开源社区的形式，带领中国国内优秀的工程师，融入实时面向对象设计开发了 RT-Thread 自主操作系统内核和微内核架构操作系统 RT-Thread Smart，及大量周边成熟、稳定软件组件，如文件系统，PersimUI 等。

⑦虚拟化技术在汽车电子电气架构中的应用

摘要：虚拟化技术在域控制器架构和中央计算架构上得到越来越广泛的应用。虚拟化可实现同一硬件多系统架构，并满足智能汽车不同功能分区隔离和资源共享需求，同时兼顾安全性、实时性、应用生态等。虚拟化可屏蔽硬件差异，以软件的形式定义硬件设备，使得多个虚拟机共享所有受管理的资源。硬件平台满足要求前提下，通过 ASIL D 认证的 Hypervisor 可满足 DCU 和 CCU 的全场景应用。

报告人：杨波涛

10+年头部 ICT 厂商操作系统及系统软件的研发和产品化工作经验，在通信设备、智能终端、物联网、智能汽车等产品方向拥有丰富的软件开发、项目管理和产品应用经验。曾参与国家核高基重大专项，并深度参与了多个行业设备上对国外操作系统的自主替代工作。目前担任中瓴智行产品总监，持续带领团队研究操作系统技术在智能汽车、轨道交通等领域智能设备的行业应用，助力客户实现操作系统国产替代。

⑧基于微内核架构的自主车载操作系统应用研究

摘要：随着车载电气架构的演进，车载操作系统从传统的嵌入式操作系统、终端操作系统的应用向基于微内核架构操作系统演化，支持多级安全体系、多业务融

合，更便捷地支撑 OTA；国产微内核架构的操作系统在工业控制、航空航天领域有多年的应用积累，面向车载操作系统的新需求，需要在生态、架构方面做新的突破，适应我国新能源汽车、城市立体交通工具的多种需要。

报告人：龚鹏程

北京东土科技股份有限公司副总经理兼操作系统 CTO。二十年操作系统研发、应用经验，参与“道系统”/Intewell 多个产品版本的研发，参与航空航天、船舶、工业控制、汽车等多个领域的操作系统国产化应用，参与制定了多项嵌入式实时操作系统相关国军标和行业标准；产品获得了工信部科学技术进步奖二等奖、中航工业集团科学技术进步奖一等奖、中船重工集团科学技术进步奖一等奖等多个奖项。

⑨汽车操作系统技术发展与实践

摘要：新能源汽车的渗透率越来越高，其电子电气架构从域控向中央计算机发展趋势业内专家也形成了共识。汽车软件架构，尤其是汽车操作系统，还处于探索阶段。目前市面上新能源汽车的各个域控制器，以集成现有操作系统，实现功能为优先目标，整车中域控之间分布式协同的 SOA 软件尚未形成主流。报告中以翼辉信息在汽车领域操作系统技术为例，针对车控、自动驾驶、车联网、座舱等域控的技术特点，说明不同域控中原创操作系统的作用。最后介绍翼辉安全关键云原生软件体系，说明 VSOA 车载微服务架构、ECS 实时容器以及 ECSM 容器管理平台等关键技术，及其在整车软件架构中的应用。

报告人：徐贵洲

北京翼辉信息技术有限公司副总经理。开源实时操作系统 SylixOS 内核开发者，参与 SylixOS 体系结构开发、音频子系统、网络子系统等内核组件开发，负责公司航天领域操作系统产品开发，负责的航天项目商业卫星九天微星瓢虫一号，航天科技八院风云翼辉星载平台卫星和行云星座卫星成功发射并稳定在轨运行。

参加讨论的嘉宾：

周庆国

理学博士，教授，博士生导师，IET Fellow，教育部新世纪人才基金获得者，现为兰州大学开源软件与实时系统教育部工程研究中心主任，兰州大学分布式与嵌入式系统实验室主任。目前主要从事安全关键系统、嵌入式系统、智能驾驶、虚拟化技术的研究，2018 年荣获甘肃省科技进步奖二等奖，荣获 2021 年甘肃省教学成果特等奖

刘寿永

中科创达首席架构师，毕业于西安电子科技大学硕士，2011 年至今在中科创达主要负责负责操作系统相关技术和产品的研发。主要聚焦在智能汽车，物联网操作系统等，为行业客户提供端到端的解决方案。

苑中魁

智能网联汽车行业安全专家，现就职中国汽车工程研究院股份有限公司北京院汽车网络与数据安全中心。从业汽车以及相关领域行业工作多年，先后从事芯片嵌入式系统开发、芯片安全技术研究、整车安全及软件升级安全测评工作，为国家市场监督管理总局缺陷产品管理中心、工业和信息化部装备工业发展中心等部委提供技术支撑工作，并参与多项企业整车与零部件网络安全、软件升级项目，具有智能网联汽车丰富行业经验。

朱玉龙

汽车产业研究专家，互联网汽车产业博主和投资人。