科技发展研究

第 22 期

（总第 491 期）

上海科技发展研究中心　　2017 年 11 月 2 日

编者按：2017浦江创新论坛——智能网联汽车产业论坛于9月22日下午举行。论坛以“智能网联汽车的信息安全”为主题，与会嘉宾[1]围绕智能网联汽车的信息安全问题，深入探讨如何提升信息安全水平、促进信息安全技术创新，为智能网联汽车产业的未来健康发展建言献策。本期简报基于分论坛嘉宾观点整理而成。供参考。

2017 浦江创新论坛专题简报之三

加快信息安全技术创新　促进智能汽车产业发展

当前，智能化、网联化、共享化已成为汽车产业发展的必然趋势。随着汽车智能网联技术的快速发展，信息安全问题也变得日益突出。如何提升信息安全水平，促进信息安全技术创新已成为智能网联汽车产业发展中的关键性环节。**与会嘉宾一致认为：信息安全问题已成为智能网联汽车产业发展的重大瓶颈，关注信息安全技术创新，强化信息安全技术实践和应用是促进智能网联汽车产业发展的重要保障。**

1 与会嘉宾包括：科技部高新技术发展及产业化司副司长续超前，嘉定区委常委、副区长沈华棣，上海市科学技术委员会副主任干频，德国机动车监督协会首席技术官 Torrecilla Torregrosa，奇虎 360 公共事务部副总裁王奋宇，同济大学教授涂辉招，中国软件评测中心智能网联汽车测试部主任宋娟，中国信息通信研究院高级工程师葛雨明。

一、发展历程：从智能汽车扩散到智能交通

当前，随着汽车不断向智能化、网联化和信息化发展，信息安全已成为智能网联汽车的关键技术。而智能交通与智能汽车密不可分，信息安全同时也影响着智能交通的发展方向。

一方面，智能网联汽车面临巨大的安全风险。科技部高新技术发展及产业化司副司长续超前指出，随着汽车产业智能化、网联化、共享化的趋势愈渐强烈，产业发展的过程中的信息安全隐患越来越多，提升信息安全的技术水平显得尤为重要。**奇虎 360 公共事务部副总裁王奋宇**指出，最新的智能汽车上至少有 100 台车载 ECU，运行 600 万行代码，而无人驾驶汽车上至少要有 2 亿行以上的代码。**德国机动车监督协会首席技术官** Torrecilla Torregrosa 也指出，互联网汽车中 100 多个电子设备都将面临各种风险，如恶意固件更新、用户密码和信息泄露、其他下载程序的攻击、手机应用程序的攻击以及车辆内部总线被攻击等等。**中国软件评测中心智能网联汽车测试部主任宋娟**指出，智能网联汽车面临的安全威胁可分为外部风险和内部风险，外部风险主要来自于手机-车机、充电接口、T-BOX、娱乐设备等接触式设备的风险和传感设备、手机 APP、无线车钥、远程更新等，内部风险主要来自于 ECU/MCU、车载网关、车载总线、车载操作系统等。

另一方面，智慧交通系统也面临各种信息安全问题。同济大学教授涂辉招指出，智慧交通环境下的交通运输必定具有大数据的特点，是全样本、全出行链、全周期、细颗粒度及互联互通的，这些特点也使得智慧互联交通系统面临各种安全风险，如黑客入侵、车路通讯系统遭破坏、恶意攻击造成电子地图定位不准确等等。**王奋宇**认为，人类正进入智能时代，万物互联，随之而来的也出现了各种有别于传统的风险，其中智能产品如智慧交通系统的云端大数据也将面临被窃取

的风险。

二、主要挑战：行业人才与标准体系亟待突破

一是汽车信息安全行业人才匮乏。近年来我国汽车产业快速发展，汽车人才数量已很可观，**王奋宇**指出，据 360 公司估算，目前我国汽车人才达 1500 多万，而其中从事汽车安全的人才却不足万人；另一方面，我国从事信息安全的人才有 230 万人，但其中专业从事汽车信息安全的人才却不足百人，可见人才缺口巨大。

二是行业标准体系有待建立和完善。就汽车信息安全的评估问题，Torrecilla Torregrosa 认为，“安全评估”服务涵盖内容广泛、复杂而多样，但目前还缺少国际认可的机动车产品安全评估标准。从行业来看，**王奋宇**指出，目前还缺少相关行业标准与规范，难以形成以车辆驾驶安全及车生活服务为中心的服务产业链，各汽车制造商的内部操作标准也不统一。因此还需要通过构建产业联盟，在不断创新积累和转化过程中形成车联服务行业标准和规范。

三是行业内外的壁垒尚未打通。智能网联汽车的信息安全涉及方方面面，**王奋宇**指出，从服务来看，不仅涉及通信、导航及位置服务等，还涉及安防、娱乐、远程访问等多种服务；从实体来看，不仅涉及 TSP 中心、汽车制造商、内容提供商、汽车销售商等，还涉及交通设施、停车场、相关支持团队、消防、警务等等。然而，目前还缺乏汽车信息安全体系漏洞共享平台，汽车行业内外部的壁垒难以打通。Torrecilla Torregrosa 也指出，目前各个汽车制造商各自的内部操作标准并不统一，使得不同汽车系统产品难以实现无缝对接。

三、未来重点：构建功能型平台、开展示范应用

一是关注智能系统全生命周期的安全管理。系统安全防护、数据安全保护和全生命周期的安全管理是智能系统安全的三个重要方面，

王奋宇认为，要重点关注智能系统全生命周期的安全管理，要将安全管理渗透到规划设计、系统建设、上线验收、安全运维及系统退服的各个阶段。Torrecilla Torregrosa 也指出，未来汽车的信息安全必定会嵌入到产品的设计阶段，贯穿到智能网联汽车产品的设计、研发、生产和应用的整个过程中。

二是构建开放共享的功能型平台，制定行业标准。上海市科学技术委员会副主任干频指出，功能型平台让更多的企业能积极开展技术创新，使更多配套进行聚集。**嘉定区委常委、副区长沈华棣**则表示，嘉定区将重点推进国家智能网联汽车（上海）试点示范区等一系列的产业平台和重大项目的建设，促进新型价值网络的形成。**王奋宇**指出，要着力搭建以车辆驾驶安全及车生活服务为中心的服务产业链，推动产业链商业模式发酵，形成规模化的服务运营商体系；要依托整体服务平台，逐步梳理和规范车服务 TSP 平台线上线下流程，结合用户、市场、行业、社会对车联服务要求的提升，制定车联服务行业规范。

三是加强智能网联汽车信息安全的技术测试与应用示范。Torrecilla Torregrosa 认为，要加强汽车信息安全的评估服务，制定和应用国际通用标准，提供安全评估的一站式服务和定制化服务。**宋娟**指出，车内控制器的网络化和 IT 化，使得汽车智能控制水平不断提升，促进汽车技术与 ICT 等技术的深度融合。这种形势下，要不断强化智能网联汽车驾驶的测评和车机安全的测评等实践工作。**中国信息通信研究院高级工程师葛雨明**指出，目前我国政府和企业都在积极推进 LTE-V2X 通信的应用示范，尤其重点关注 C-V2X 通信安全和车联网安全等方面，其政策环境、标准环境及行业环境均在不断完善。

整　理：傅翠晓、张　虹

责任编辑：汤天波　　编辑：张　虹　　联系电话：64311988-456　　传真：64315005
地址：淮海中路 1634 号 412 室　　邮政编码：200031　　电子邮件：fzzx@stcsm.gov.cn