软件功能安全标准
白皮书

工业和信息化部电子第五研究所&华东师范大学
嵌入式软件功能安全联合实验室
国家嵌入式软件质量监督检验中心
2017 年 12 月

版权声明

《软件功能安全标准白皮书》

专家指导工作组（排名不分先后，按姓氏笔画数排序）：

组　长：何积丰

组　员：王　野　王小敏　王维建　刘　畅　刘豫湘　孙　猛

李　冬　李宗华　汪岳君　张晓先　陈华军　林　晖

周庭梁　封　亮　赵永望　钟益林　徐福祥　郭　进

宾建伟　黄志球　蒲戈光　缪淮扣

主　编：杨春晖

副主编：刘奕宏　　郭　建

编写组：张宝林　　许　朋　刘梦玥　姚日煌　黄晓昆　缪炜恺

吴振宇　　乐　亮　王剑亮　林　军　吴　蕾　谢浪雄

参编单位（排名不分先后，按首字笔画数排序）：

工业和信息化部电子第五研究所

上海富欣智能交通控制有限公司

上海新华控制技术集团科技有限公司

比亚迪汽车工业有限公司

中车株洲电力机车有限公司

中电 32 所软件测评中心

中国商用飞机有限责任公司

卡索(北京)科技有限公司

卡斯柯信号有限公司

北汽福田汽车股份有限公司

北京大学

北京纵横机电技术开发公司

西南交通大学

华东师范大学

南方电网有限公司

南京航空航天大学

普华基础软件股份有限公司

前　言

18 世纪中叶以来，人类历史上先后发生了三次工业革命。第一次工业革命所开创的“蒸汽时代”（1760-1840 年），标志着农耕文明向工业文明的过渡；第二次工业革命进入了“电气时代”（1840-1950 年），使得电力、钢铁、铁路、化工、汽车等重工业兴起；第三次工业革命，开创了“信息时代”（1950-），全球信息和资源交流变得更为迅速，工业化与信息化深度融合。前三次工业革命使得人类发展进入了空前繁荣的时代。与此同时，这种发展方式也造成了巨大的能源、资源消耗，付出了巨大的生态成本环境代价，急剧地扩大了人与自然之间的矛盾。人类已开始意识到，粗放型发展方式必将是一条杀鸡取卵的不归路，绿色、集约、高质量的发展方式将成为是 21 世纪人类的必然选择。

曾经繁荣昌盛的中华民族在错过前两次工业革命后，在第三次工业革命后期奋起直追。在短短 50 年间，中华民族从落后挨打的封建国度发展到举足轻重的中国特色社会主义国度，完成了历史性的大跨越；特别是近十年来，神州天宫、深海蛟龙、太湖之光、中国天眼、华龙一号、纵横高铁等成就举世瞩目，中华民族踏上了伟大复兴的道路。然而，我们同时也应该清楚的认识到，我国众多产业中的关键零部件和材料仍依赖进口，基础产业仍处于大而不强状态，如何进一步攻克核心领域的关键技术，如何全面提高核心产业的整体质量水平，如何快速实现我国经济发展的转型升级是摆在中华民族伟大复兴之路上的关键问题。

当前，软件已成为各行各业智能化、互联化的关键，广泛应用于金融、电力、交通、航空航天、国防等重点领域。随着软件的规模越发庞大、结构日趋复杂，软件中容易驻留缺陷，缺陷可能导致失效，失效引发事故。纵观历史，爱国者导弹失效、阿丽亚娜火箭爆炸、7.23 甬温线特别重大铁路交通事故等均是因嵌入式软件的安全性缺陷而导致。软件的安全性、可信性成为业内广泛关注的焦点，软件安全性分析、设计、验证、维护等关键基础技术更加凸显其重要性。

在这个问题的研究上，国外研究比我们早先一步。自 1995 年，麻省理工研究团队针对嵌入式软件安全性（Safety）发起了 MIT Safety Project 项目，依托该项目，该团队发表了大量关于软件安全性分析、安全需求管理、软件安全性设计和验证的论文、著作，为嵌入式软件安全性研究奠定了较好的理论基础。在

此之后，该领域的研究得到了国际社会的广泛关注，2001 年国际上电气和电子工程师协会发布了首个产品安全性标准——IEC61508《电气/电子/可编程电子安全相关系统的功能安全要求》，该标准从研发过程管理、安全保障技术等多个方面对安全相关产品(含软件)提出了要求，并得到了国际上知名检测认证机构(TUV、SGS、UL、CSA 等）、领军企业（波音、空客、GE、ABB、宝马）的广泛支持，在世界范围内产生了较大的影响力。经过十多年的发展，以该标准为基础，结合各领域知识背景，已形成了适用于航空、核电、轨道交通、过程工业仪表、医疗设备、扶梯、电驱设备、智能家电等领域的产品安全技术标准，涉及国计民生各重点行业。虽然标准体系逐渐健全，但是具体检测的技术方法、工具仍十分缺乏，西方对我国的技术封锁也比较严重。

华东师范大学与电子五所是国内研究该领域关键技术工比较早的团队。经过十多年的共同努力，华东师范大学与电子五所组建了软件功能安全联合实验室，该联合团队在航空、轨道交通、汽车电子、装备制造、核工业等安全关键领域开展了多方面的实践，也取得了一定的学术与工程技术成果，同时也在促进我国的软件功能安全标准与技术体系也在逐渐与国际接轨，推动行业生态逐渐向更为健康、更为高效的方向发展。为进一步推动软件功能安全技术在“中国制造 2025”的变革浪潮中更好地为人所知、为人所用，该团队编写《软件功能安全标准白皮书》。本白皮书分析了当前国内外软件功能标准的制修订现状，梳理了各国对软件功能安全法规的管理现状和行业发展趋势，简单说明了软件功能安全技术在汽车电子、过程工业、轨道交通、航空行业、核电、医疗设备等领域的典型应用，并基于此，从落实“质量为先”的国家战略角度，在标准研制、人才培养和技术应用方面提出了工作建议。望此白皮书的发布，能够与众多行业专家分享电子五所与华东师范大学在软件功能安全领域的认知和成果，能够更为广泛的建立技术沟通和交流的平台帮助人才成长，能够积极更多的政府、企业、高校的力量来推动相关技术应用，为“中国制造 2015”目标的顺利达成更添一块基石。

目录

第一章绪论

1.1 功能安全概念

工业文明在给人类带来巨大利益的同时，也不可避免地带来伴随了灾难。据国际劳工组织(ILO)在第十五届世界职业安全健康大会公布的数据，全世界每年发生在生产岗位的死亡人数超过 100 万人，加之因安全管理和控制缺陷引发的安全事故而导致的人员伤亡，使全世界每年死亡死于工伤事故和职业病危害的人数约为 200 万，工业安全事故是已成为人类最重要大的杀手之一。为了实现“安全工业”的目标，越来越多的安全相关系统（包括自动控制系统和自动保护系统）被用在不同各个领域，保护人员免受伤害，保证机械、整套装置甚至整个工厂自动、正常、安全地运转。

安全事故带来的危害和造成的经济损失是触目惊心的。1974 年英国 Nypro 公司在弗利克斯伯勒镇的环已烷装置泄露爆炸、1976 年意大利塞维索市伊克梅萨化工厂二恶英泄漏、1984 年印度中央邦博帕尔市的美国联合碳化物公司农药厂发生氰化物泄漏、1986 年苏联基辅州切尔诺贝利核电站核反应堆爆炸、1994 年英国 Millford 港口炼油厂可燃炭氢化合物泄漏、2001 年法国图尔兹 AFZ 化工厂发生硝酸铵爆炸、2005 年英国邦斯菲尔德油库发生火灾、2010 年墨西哥湾“深水地平线”钻井平台爆炸、2011 年中国温州南甬温线动车追尾事故等不断发生的事故，其原因都是安全相关系统的功能失效。业界开始

意识到必须采取相应措施，必须用标准来规范管理和控制工业领域内安全相关系统的使用，必须使技术在安全的框架内发展，让人们在享受现代工业新技术带来的舒适与便捷的同时，又能规避安全风险避免危害，防止技术缺陷和安全事故的发生。功能安全标准的研究由此开始。

国际电工委员会（IEC）率先为促进安全攸关产品的安全性水平提升，国际上电气和电子工程师协会于 2000 年发布了首个产品安全性标准——IEC 61508-1:1998《电气/电子/可编程电子安全相关系统的功能安全要求》，该标准从研发过程管理、安全保障技术等多个方面对安全相关产品（含软件）提出了要求，并得到了国际上知名检测认证机构（TÜV、SGS、UL、CSA 等）、领军企业（Boeing、Airbus、GE、ABB、BMW）的广泛支持。国际电工委员会作为世界上成立最早的国际性电工标准化机构，其权威性在为促进安全相关产品的安全性水平提升上起到引领作用。

该标准对功能安全（Functional Safety）的定义是：“part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures”（功能安全是指受控装备和受控装备控制系统整体安全相关部分的属性，其取决于电气/电子/可编程系统功能的正确性和其他风险降低措施。）标准制定的目标是保证电气、电子、可编程安全相关系统的安全可靠，当系统发生故障（包括硬件随机故障和软件故障）或错误时，安全相关系统会采取预先设定的措

施，保证故障不会引起人员的伤亡、环境的破坏和设备财产的损失。

该标准的内容可概括为以下三个方面：

1、对软、硬件在内的安全相关系统及其部件，在生命周期范围提供了一个安全监督的系统方法；

2、推荐了确定安全相关系统安全功能 SIL 等级的方法；

3、建立一个基础标准，使其可以直接应用于所有工业领域，同时，亦可指导其他领域。

经过十多年的发展，以该标准为基础，结合各领域的知识背景，已形成了适用于航空、核电、轨道交通、汽车、工业仪表、医疗电子、扶梯、电驱设备、智能家电等领域的功能安全技术标准，涉及国计民生各重点行业。

1.2 行业需求分析

随着各类设备中软件控制的占比越来越高，功能结构日趋复杂，在各行业内软件密集型产品/装备的安全问题日益出现，集中在以下方面。

1、产品装备因安全问题召回频繁，软件引发的安全问题凸显

在医疗器械领域，国内因功能安全相关系统故障而被召回的医疗器械数目逐年在增加，尤其因软件设计问题而导致的医疗行业的功能安全问题越来越突出。

在轨道交通领域，根据轨道交通事故调查数据显示，因列车脱轨、列车相撞、停运等安全相关系统因素引起的事故比例较高，轨道交通

领域由功能安全引起的安全问题逐渐凸显。

在汽车电子领域，随着传感技术、计算机技术、网络技术的发展，汽车电子日益智能化、网络化、集成化。同时，软件在汽车电子控制系统中的作用越来越突出，譬如汽车安全驾驶辅助系统、防抱死制动系统 ABS、制动辅助系统 BAS、驱动防滑装置 ASR、电子制动辅助系统 EBA、电子稳定程序 ESP、车辆偏离警告系统、碰撞规避系统、胎压监测系统 TPMS、自动驾驶公路系统等，软件的失效和功能安全问题往往会引发汽车的安全问题，导致了汽车召回总量逐年增多。

如何解决软件引发的功能安全问题成为多数企业需要面临的重要问题。

2、各行业软件功能安全标准和规范落实情况参差不齐，企业缺乏系统化、规范化的软件研发流程

欧洲国家一直致力于制定相关的功能安全标准，来促进和规范安全相关的控制，保护系统的设计、制造和应用。随着仪表控制技术和控制系统可靠性技术的发展，为适应各工业部门对安全相关系统的性能要求，有关安全相关系统的标准也在不断更新和完善。IEC 61508、IEC 61511 等标准发布后，欧洲首先采用，并将其列为强制性法规的内容。

国内各行业的软件功能安全标准大多直接采用国外的功能安全标准，但功能安全标准在我国仅为推荐性标准，而非强制性标准。由于各行业监管部门不同，各行业对于功能安全标准的落实情况和执行情况监督力度不同，导致各行业功能安全实施情况参差不齐，很多企

业未按功能安全标准规范研发产品，软件功能安全问题日益突出。

同时，部分行业缺乏相应的软件功能安全标准规范，导致企业在软件研发过程中缺乏系统化、规范性的功能安全研发流程指导，导致软件引发的安全问题较为突出。

软件功能安全标准规范的完整性和可实施性成为企业降低软件安全风险，优化产品，提高产品安全水平，保证产品功能安全的必备条件。

3、缺乏规范化、体系化、实施性高的软件测评监督体系

IEC 61508、IEC 61511 等标准发布后，欧洲首先采用，并将其列为强制性法规的内容。美国于 2003 年底开始采用并将其列为强制性法规的内容。同时，欧美各国出台了相应的标准实施规范和管理办法，各测评认证机构遵循管理办法开展认证测评监督，搜集产品缺陷数据，建立软件功能安全保障数据库，提升软件质量，进而保证产品的功能安全。

功能安全标准在我国仅为推荐性标准，而非强制性标准，并且尚未发布与标准相应的应用指南或指令，未形成相应行业功能安全测评管理办法、测评过程指南等测评体系文件。国内测评认证机构在功能安全领域起步较晚，尽管开展了相关研究，但由于实践经验相对较少，难以建立各行业完整的软件缺陷数据库，只能参考一些国际通行的数据库进行分析，难以为各行业软件功能安全提供保障服务，更无法在行业功能安全标准制定方面占据主导地位，一定程度上限制了国内功能安全测评监督的作用，导致软件功能安全隐患逐渐增多。

第二章标准制修订现状

2.1 标准系列

在软件功能安全领域，2000 年 IEC 发布了功能安全基础标准 IEC 61508《电气、电子、可编程电子安全相关系统的功能安全》。随后，各行业以 IEC 61508 标准作为功能安全的参考标准，制定了不同行业的应用标准，功能安全标准系列如下图所示：

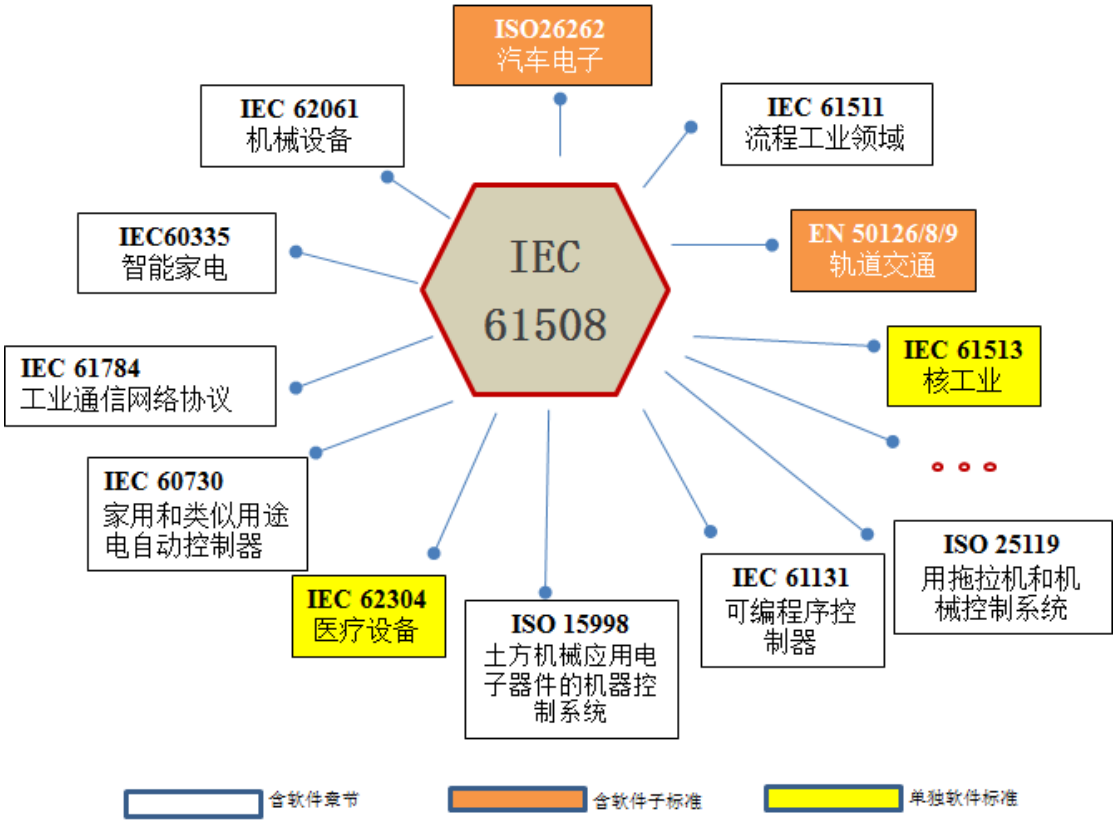

图 2-1 功能安全标准簇

IEC 和 ISO 颁布的功能安全各领域标准详细情况见下表所示。

表 2-1 功能安全标准系列列表

标准号	名称	行业/领域	颁布方	对应国标
IEC 61508:2010	电气/电子/可编程电子安全相关系统的功能安全	电气/电子/可编程电子	IEC/TC 65	GB/T 20438:2006
IEC 61511:2003	过程工业安全仪表系统的功能安全	过程工业仪表	IEC/TC 65	GB/T 21109:2007
IEC 61513:2011	核电厂核能工业的安全仪表系统	核电	IEC	/
IEC 62061:2005	机械安全与安全有关的电气、电子和可编程电子控制系统的功能安全	机械安全	IEC/TC 44	GB 28526:2012
IEC/TR 62061-1:2010	指导 ISO 13849-1 和 IEC 62061 中用于机械的安全相关控制系统设计的应用指南	机械安全相关控制系统	IEC/TC 44、ISO/TC 199	GB/T 34136:2017
IEC 61784-3:2016	工业通信网络协议集第 3 部分：现场总线功能安全	数据通信	IEC/TC 65	GB/T 34040:2017
IEC 61131-6:2012	可编程序控制器第 6 部分：功能安全	设备安全	IEC/TC 65	GB/T 15969.6-2015
IEC 62304:2015	医疗设备软件	医疗设备软件	IEC	/
IEC 60730-1:2003	家用和类似用途电自动控制器第 1 部分：通用要求	家电	IEC/TC 72	GB/T 14536.1:2008
IEC 61800-5-2:2007	可调速的电气传动系统第 5-2 部分：安全要求功能	电驱设备	IEC/TC 22	GB/T 12668.502:2013
ISO 25119:2010	农业和林业用拖拉机和机械控制系统的安全相关部件	农林业	ISO/TC 23	/
ISO 26262:2011	道路车辆功能安全	汽车	ISO/TC 22	GB/T 34590:2017
ISO 15998	土方机械应用电子器件的机器控制系统(MCS) 功能性安全的性能准则和试验	土建	ISO/TC 127	GB/T 34353-2017

2.2 国内外标准制定组织

2.2.1 国内外标准制修订组织

1、国际标准化组织（International Organization for Standardization，ISO）是一个全球性的非政府组织，是国际标准化领域中一个十分重要的组织。ISO 国际标准组织成立于 1946 年，中国是 ISO 的正式成员，代表中国参加 ISO 的国家机构是中国国家技术监督局(CSBTS）。ISO 负责目前绝大部分领域（包括军工、石油、船舶等垄断行业）的标准化活动。

2、国际电工委员会（IEC）成立于 1906 年，它是世界上成立最早的国际性电工标准化机构，负责有关电气工程和电子工程领域中的国际标准化工作。

3、欧洲电工标准化委员会（CENELEC）1976 年成立，和 CEN 以及它们的联合机构 CEN/CENELEC 同为欧洲最主要的标准制定机构。CENELEC 的宗旨是协调欧洲有关国家的标准机构所颁布的电工标准，以及消除贸易上的技术障碍。CEN 于 1961 年成立于法国巴黎，在业务范围上，CENELEC 主管电工技术的全部领域，而 CEN 则管理其它领域。

4、美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）直属于美国商务部，从事物理、生物和工程方面的基础和应用研究，以及测量技术和测试方法方面的研究，提供标准、标准参考数据及相关服务。其主要任务是：建立国家计量基准与标准；发展为工业和国防服务的测试技术；研制与销售标准服务；提供计量

检定和校准服务；参加标准化技术委员会制定标准；进行技术转让，帮助中小型企业开发新产品。此外还承担着防火、抗地震技术及应用计算技术等研究工作。

5、美国电子工业协会、美国仪表学会负责过程工业仪表功能安全标准的制定实施。

6、美国汽车工程师学会（Society of Automotive Engineers，SAE）是世界上汽车、海洋和航空/航天运输机械技术信息的主要来源之一，每年都会推出大量的标准资料、技术报告、参数（工具）书籍和特别出版物，建有庞大的数据库。

7、欧洲标准化委员会（法文缩写：CEN）成立于 1961 年，以西欧国家为主体、是由国家标准化机构组成的非营利性国际标准化科学技术机构，是欧洲三大标准化机构之一。CEN 负责制定本地区需要的欧洲标准（EN，除电工行业以外）和协调文件（HD），并与 CENELEC 和 ETSI 一起组成信息技术指导委员会（ITSTC），在信息领域互连开放系统（OSI）制定功能标准。

8、德国标准化学会（德文缩写：DIN）成立于 1917 年，是德国最大的具有广泛代表性的公益性标准化民间机构，通过有关方面的共同协作，制定和发布德国标准及其他标准化工作成果并促进其应用，有助于经济、技术、科学、管理和公共事务方面的合理化、质量保证、安全。

9、法国标准化协会（英文缩写：AFNOR）成立于 1926 年，为法国标准化主管机构，按政府指示组织和协调全国标准化工作，代表

法国参加国际和区域性标准化机构的活动。

10、英国标准协会（BSI）成立于 1901 年，是集标准研发、标准技术信息提供、产品测试、体系认证和商检服务五大互补性业务于一体的国际标准服务提供商，面向全球提供服务。BSI 倡导并制定了世界上流行的 ISO9000 系列管理标准。

11、日本工业标准调查会（Japanese Industrial、Standards Committee，JISC），是根据日本工业标准化法建立的全国性标准化管理机构，制定国家级标准中最重要、权威的标准。JIS 除对药品、农药、化学肥料、蚕丝、食品以及其他农林产品制定有专门的标准或技术规格外，还涉及到各个工业领域。

12、国家标准化管理委员会（Standardization Administration of China，SAC）为我国国家质检总局管理的事业单位，是统一管理全国标准化工作的主管机构，负责管理各行业的标准化工作，负责组织国家标准的制定、修订工作，负责国家标准的统一审查、批准、编号和发布。

2.2.2 国内外评估与咨询机构

国外依据标准开展功能安全评估和咨询起步较早，并且已经被广大用户、设备供应商和集成商、工程承包商所接受。功能安全评估和咨询主要有产品安全评估和认证、过程评估和认证、管理过程认证、人员资格认证和项目安全评估。国内外功能安全评估和咨询机构详见表 2-2。

表 2-2 国内外评标与咨询机构情况表

国家	认证机构	机构简介及职责
美国	UL 认证	UL 安全试验所是美国最有权威的，也是世界上从事安全试验和鉴定的较大民间机构。
英国	Intertek	Intertek 天祥集团，提供家用电器、暖通空调、汽车零部件、燃气具、制冷产品、照明产品、电动工具、多媒体产品、信息技术产品、医疗设备、工业机械、建筑设备等产品的电气安全测试认证、电磁兼容性测试、性能测试以及管理体系认证服务。
德国	TÜV 南德	TÜV 南德意志集团成立于 1866 年，总部位于德国慕尼黑，在领域如工业、交通和人力管理方面积极运作，提供资讯、检验、测试、专家意见、认证和培训服务。南德意志集团的功能安全部门建立了一套专门的认证体系，一方面可以检验企业现有的安全管理系统，另一方面可以协助企业建立并实施功能安全管理。
德国	TÜV 莱茵	TÜV 莱茵集团成立于 1872 年，总部位于德国科隆，提供工业服务、交通服务、产品服务、生命科学服务、教育与咨询服务、管理体系服务。
瑞士	SGS	SGS 于 1878 年成立于鲁昂，是检验、鉴定、测试和认证机构，SGS 通标标准技术服务有限公司是瑞士 SGS 集团和隶属于原国家质量技术监督局的中国标准技术开发公司共同成立于 1991 年的合资公司。SGS 作为功能安全方面的公认机构以及机械方面的指定机构，其功能安全服务涵盖移动、农业和林业、自动化、机械、医疗技术、加工行业、半导体和软件等领域。
法国	BV	必维集团（BV）创立于 1828 年，是测试、检验和认证服

		务机构，BV 的功能安全服务涉及石油化工、轨道交通、汽车电子、公共设施、核电仪控、智能电网、工厂自动化等众多安全相关领域，涉及产品包括电梯安全控制板、铁路信号系统、汽车制动装置、机械设备安全控制系统、电子感应防护装置、安全仪表系统（SIS）等。
荷兰	KEMA	KEMA 成立于 1927 年，为能源产业链提供全球性的优质服务，包括业务与技术咨询、运营支持、测量与检测，测试与认证等服务。
中国	工业和信息化部电子第五研究所	中国最早从事可靠性研究的权威机构。实验室提供从元器件到整机设备、从硬件到软件直至复杂大系统的产品检测试验、分析评价、认证计量、信息服务、技术培训、专用设备和专用软件开发等技术服务。在轨道交通、汽车电子、家电、核电等领域提供测评、咨询和培训服务。
中国	机械工业仪器仪表综合技术经济研究所	机械工业仪器仪表综合技术经济研究所功能安全中心承担全国工业过程测量控制和自动化标准化技术委员会第十分技术委员会（SAC/TC124/SC10）秘书处工作，在国际上对口国际电工委员会 IEC/TC65A。功能安全中心专业从事功能安全标准和技术研究、评估、咨询认证和培训，致力于功能安全技术在中国的推广与发展。

2.3 国内外标准制修订情况

在功能安全技术应用领域中，汽车电子、过程工业行业、轨道交通、航空、机械控制、核电和医疗电子领域是近年来标准与技术发展最快的领域。国外在这些领域的功能安全标准的修订、颁布情况见表 2-3 所示。

表 2-3 国外各行业/领域功能安全标准制修订情况

序号	行业/领域	标准标识号	名称
1	电气/电子/可编程电子安全相关系统	IEC 61508:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements; — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems; — Part 3: Software requirements; — Part 4: Definitions and abbreviations; — Part 5: Examples of methods for the determination of safety integrity levels; — Part 6: Guidelines on the application of parts 2 and 3; — Part 7: Overview of techniques and measures.
2	汽车电子	ISO26262:2011	Road vehicles — Functional safety — Part 1: Vocabulary — Part 2: Management of functional safety — Part 3: Concept phase — Part 4: Product development at the system level — Part 5: Product development at the hardware level — Part 6: Product development at the software level —Part 7: Production and operation —Part 8: Supporting processes —Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses —Part 10: Guideline on ISO 26262
3	过程工业	BS IEC 61511-1:2003	Functional safety —Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system,hardware and software requirements
		BS IEC 61511-2:2003	Functional safety —Safety instrumented systems for the process industry sector — Part 2:Guidelines for the application of IEC 61511-1

		BS IEC 61511-3:2003	Functional safety —Safety instrumented systems for the process industry sector — Part 3:Guidelines for the determination of the required safety integrity levels
4	轨道交通	BS EN 50126-1:1999	Railway applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) -Part 1: Basic requirements and generic process
		PD CLC/TR 50126-2:2007	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Guide to the application of EN 50126-1 for safety
		PD CLC/TR 50126-3:2006	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 3: Guide to the application of EN 50126-1 for rolling stock RAMS
		BS EN 50128:2011	Railway applications —Communication, signaling and processing systems —Software for railway control and protection systems
		IEC 62279:2015（与上标准等同）	Railway applications - communication, signaling and processing systems - software for railway control and protection systems
		EN 50129:2003	Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling
		BS EN 50159:2010	Railway applications —Communication, signaling and processing systems —Software-related Communication in transmission system
5	航空	DO-178B	Software Considerations in Airborne Systems and Equipment Certification
		DO-178C:2011	Software Considerations in Airborne Systems and Equipment Certification
6	机械控制	IEC 62061:2005	Safety of machinery - Functional safety of safety-related electrical, electronic and

			programmable electronic control systems
7	核电	IEC 61513:2011	Nuclear power plants - Instrumentation and control important to safety - General requirements for systems
		IEC 60880:2006	Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions
8	医疗电子	IEC 62304:2015	Medical device software - Software life cycle processes

在我国，IEC 61508 标准于 2006 年等同转化为国家标准 GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》。GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》是一项用于工业领域的标准，作为一个基本的功能安全标准应用于各种工业行业。

与 IEC 功能安全标准体系相似，国内的功能安全标准体系建设以 GB/T 20438 标准作为功能安全的基本标准，衍生出不同的行业应用标准。GB/T 20438 系列标准是功能安全的基本标准，各个行业均参考该标准，衍生出行业领域的功能安全或技术基础标准和应用标准。

作为国内功能安全体系的顶层标准，我国还制订了 GB/Z 29638 标准，该标准是对 GB/T 20438 标准的补充，主要介绍功能安全的概念以及 GB/T 20438 系列标准的概况。下文对国内不同行业功能安全标准制定现状分别进行说明。

1、汽车电子行业

汽车功能安全标准 ISO 26262-2011，其中第 6 部分为汽车电子功能安全对软件部分的安全要求。2017 年国内等同采用和对电动汽车动力系统的安全标准。本标准可以看作从整车层面对电动发布了该标

准，国标号为 GB/T18384 系列标准，更确切的说是针汽车动力系统提出的安全通则，共分 3 个部分：第 1 部分车载可充电储能系统；第 2 部分操作安全和故障防护；第 3 部分人员触电防护，GB/T18384 系列标准更侧重于针对电能和电磁能的安全规范和故障保护。

直至 2017 年，国家标准化管理委员会将汽车行业功能安全标准 ISO 26262 转化为国家标准 GB/T 34590:2017《道路车辆功能安全》。

2、过程工业行业

国内过程工业领域，IEC 61511 标准于 2007 年转化为我国的国家标准 GB/T21109.1-2007《过程工业领域安全仪表系统的功能安全第 1 部分：框架、定义、系统、硬件和软件要求》、GB/T21109.2-2007《过程工业领域安全仪表系统的功能安全第 2 部分：GB/T 21109.1 的应用指南》、GB/T21109.3-2007《过程工业领域安全仪表系统的功能安全第 3 部分：确定要求的安全完整性等级的指南》，用于规范我国过程工业领域安全仪表系统的功能安全。它分为三部分：第 1 部分为框架，定义，系统、硬件和软件的要求；第 2 部分为标准的应用导则；第 3 部分为定义需要达到的安全完整性水平的导则。可以看到，第 1 部分为规范性要求，第 2、3 部分则是对要求的指导和示例，与 GB/T 20438 系列标准的结构相似。GB/T21109 标准的应用对象主要是安全仪表系统的设计者、集成商、或用户；GB/T 20438 标准的应用对象主要是设备制造商或产品供应商。

3、轨道交通行业

目前，国内轨道交通行业标准主要来源于欧洲标准 EN 50126、

EN 50128、EN 50129 等，是欧洲标准的中文本地化，包括：

GB/T 28808《铁路应用——通信、信号和处理系统——铁路控制和防护系统软件》

GB/T 28809《铁路应用——信号领域的安全相关电子系统》

GB/T 24339.1《铁路应用－通信、信令和处理系统第 1 部分：封闭传输系统中安全相关的通信》

GB/T 24339.2《铁路应用－通信、信令和处理系统第 2 部分：开放式传输系统中安全相关的通信》

上述 4 个标准是对铁路中与安全密切相关的子系统与安全通信方面进行了说明。

4、航空行业

国内民用航空领域，DO-178C 标准的推行和认证是民航领域的必然趋势。但与国外相比，我国航空领域的适航性起步较晚，1987 年国务院颁布《中华人民共和国民用航空器的适航管理条例》，1996 年中航工业总公司参照引进了软件适航标准，发布了航空工业标准 HB/Z 295-96《机载系统和设备合格审定中的软件考虑》，2012 年国务院出台了《国务院关于促进民航业发展的若干意见》，其中明确提出“积极支持国产民机制造”，包括加强适航的审定和航空器的适航评审能力建设，健全适航审定组织体系，积极为大飞机战略服务，积极拓展中美、中欧等双边适航范围，提高适航审定国际合作水平等。

虽然目前国内制定了航空工业适航性标准 HB/Z 295-96，但是在民航领域，国内的适航审定是由中国民用航空局主导，依据民航局颁

布的《运输类飞机适航标准》（CCAR-25-R4）、《民用航空产品和零部件合格审定规定》（CCAR-21-R3）和《民用航空器及其相关产品适航审定程序》（AP-21-AA-2008-05R2）等进行适航性审定，在适航审定过程中，对航空机载软件要求按照 DO-178B/C 审定其符合性。但我国航空机载软件适航性工作开展较晚，软件研制单位目前尚未开发出完全符合 DO-178B/C 标准的机载软件。

5、机械控制行业

机械电气设备的功能安全标准，国外主要为 ISO13849 标准和 IEC62061 标准。国内针对上述两个标准，分别制订了 GB/T 16855《机械安全控制系统有关安全部件》和 GB 28526《机械电气安全安全相关电气、电子和可编程电子控制系统的功能安全》，其中 GB/T 16855 标准对应 ISO 13849 标准，GB 28526 标准对应 IEC 62061 标准。

GB/T 16855 标准主要是对控制系统的安全相关部分的要求；GB 28526 标准主要是对安全相关的电气、电子、可编程电子控制系统的功能安全要求。GB/T 16855 标准中有两个部分涉及功能安全，给出了对控制系统有关安全部件所提供的安全功能和所达到的类别进行分析和试验时，需要遵循的程序和条件，侧重于分析控制电路的结构。GB 28526 标准主要参考了 GB/T 20438 标准的第 2、3 部分，也就是软、硬件开发的部分，在一个标准中给出了功能安全设计、集成和确认的要求和建议。

6、核电行业

我国已编制 440 多项核电标准，其中 20％为国家标准，80％为

核行业标准。在这些标准中，绝大部分是与核岛相关的标准，而常规岛和核电厂配套子项 BOP 方面主要采用常规电力标准以及其他一般工业标准。

我国已制定对应的核安全法规 HAF102《核动力厂设计安全规定》，提出了陆上固定式热中子反应堆核动力厂的核安全原则，明确了保证核安全是必需的安全要求。核安全导则 HAD102/10 和 HAD102/14 主要涉及安全重要 I&C 系统的设计要求，是对 HAF102 法规中有关安全重要 I&C 系统章节的阐述和补充，其目的是对核动力厂中的安全重要 I&C 系统的设计提供指导。核安全导则 HAD102/16《核动力厂基于计算机的安全重要系统软件》，描述了从计算机系统的需求、设计到计算机软件的需求、设计和实现、计算机系统的集成、安装和调试直到运行和交付后修改的整个软件生存周期，并规定了周期各阶段的活动、过程和文件编制。

下面是核动力厂安全重要 I&C 系统的、针对软件功能安全的主要标准：

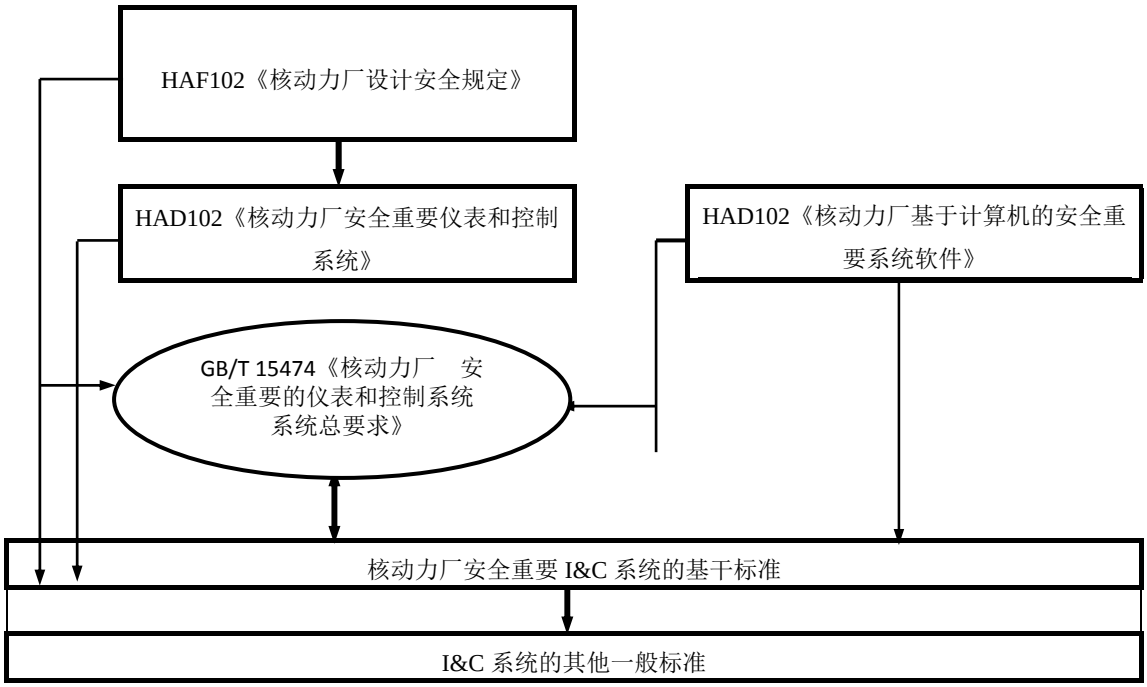

图 2-2 核电行业软件标准图

1）安全系统准则：

GB 13284-1998《核电厂安全系统准则》；

GB/T 13629-1998《核电厂安全系统中数字计算机的适用准则》；

GB/T 12788-2000《核电厂安全级电力系统准则》；

2）功能分类和系统分级：

GB/T 15474-1995《核电厂 I&C 系统及其供电设备的安全分级》；

GB/T 15475-1995《核电厂 I&C 系统及其供电设备质量保证分级》。

3）计算机的硬件和软件：

EJ/T 529-1990《用于核电厂安全重要系统数字计算机》；

EJ/T 1058-1998《核电厂安全系统计算机软件》；

EJ/T 1058.2-2005《安全系统计算机软件第 2 部分：预防软件导致的共因故障（CCF）、软件工具和预开发软件的使用》；

NB/T 20055-2011《核动力厂安全重要 I&C 系统对执行 B 类和 C

类功能的基于计算机系统的软件要求》；

4）通信系统要求：

EJ/T 637-1992《核电厂安全有关通信系统》；

EJ/T 1223-2007《核动力厂安全重要的仪表和控制系统多路数据传输的功能要求》。

7、医疗设备行业

目前，国内医疗行业依据 IEC 60601 标准、IEC62304 标准，针对医用电气设备，制定了国家标准 GB 9706.1-2007《医用电气设备第一部分：安全通用要求》，并于 2008 年 7 月 1 日实施。但该国标系列中只涵盖了 IEC 60601 系列中的部分标准，还有一部分转化为医药行业标准（YY）。IEC 标准中，IEC 62304《医疗设备软件——软件生存期过程》描述了医疗用电器设备的软件要求，目前国内还未有与该标准相对应的国家标准。

2.4 技术标准总结与比较

通过比较第 2.3、2.4 章节国内外标准的制修订情况，可以发现国内软件功能安全标准和国外的差异如下：

1、国内软件功能安全标准完整性和齐全性需加强

目前，国外软件功能安全标准覆盖了汽车电子、过程工业、轨道交通、航空行业、机械控制、核电、医疗设备等各个行业，标准规范相对较为齐全，并且正在不断地更新和完善。

国内各个行业功能安全标准多数等同采用国外的标准，而且在部

分行业如医疗设备、航空、汽车电子等行业目前还没有相对应的国家标准，软件功能安全标准目前没有覆盖各个行业，同时，部分行业标准只是部分采纳了国外的标准。因此，目前国内软件功能安全标准的完整性和齐全性还需加强。

2、国内软件功能安全标准制定自主化程度较低，影响力薄弱

目前国内各行业如过程工业、轨道交通、机械控制、核电等已有对应功能安全标准的行业，其标准规范多数等同采用或部分采用国外对应行业的标准规范，缺乏符合国内行业情况、具有中国特色的自主化内容，没有将国内行业的特点归纳填充到标准中，本地化元素较少，在软件功能安全标准的发展中影响力薄弱。

3、标准的执行情况差异明显，缺乏影响力和约束力

目前，国外各行业的功能安全标准多数为强制性标准，企业严格按照标准规范的要求进行生产制造，保证了产品的功能安全。

国内由于相关标准规范为参考性推荐标准，标准的约束力和影响力较为薄弱，进而制约着产品质量，降低企业竞争力，反过来从成本角度又会增加标准落地执行的难度。

第三章行业贯标现状

3.1 汽车电子行业

3.1.1 国外标准贯标现状

2011 年 11 月推出 ISO 26262 标准之前，汽车行业遵照的功能安全标准是电子、电气及可编程器件功能安全基本标准 IEC 61508。然而，作为一种通用基础安全标准，对于汽车行业的特殊性而言，该标准有很多的不足，特别是近年来汽车系统的复杂性日益增长。从 IEC 61508 标准派生出来的 ISO 26262 标准为当前汽车行业量身定制，特别是 ISO 26262 标准对于硬件研发、软件研发的要求适合于当前先进汽车工业的实际现状。ISO26262 标准主要定位于汽车行业中特定的电气器件、电子设备、可编程电子器件等专门用于汽车领域的部件，旨在提高汽车电子、电气产品的功能安全。

除了 ISO26262 标准应用于车辆软件的验证和确认外，还有 MISRA 标准用于汽车软件的静态分析。自从汽车工业软件可靠性协会 MISRAC 标准问世以来，静态分析一直是汽车应用软件开发过程中很大的一部分。“车辆软件 C 语言使用指南”是 1998 年首次出版的，它包含了一些规则，这些规则定义了一个现已被普遍认可的、作为良好编程实践典范的 C 语言子集。“MISRA C++：2008 关键系统 C++语言使用指南”标准发布于 2008 年，用于为 C++语言定义类似的规则。

ISO 26262 标准根据安全风险程度对系统或系统某组成部分确定划分为由 A 到 D 的安全需求等级(汽车安全完整性等级——ASIL)，其中 ASIL D 级为最高等级，具有最苛刻的安全要求。对系统供应商而言，必须满足这些因安全等级提高而提出的更高设计要求。ISO26262 标准于 2009 年出版草案，正式标准于 2011 年底出台，并希望被 EU 指令（欧洲 EU 指令适用于所有向欧盟（EU）出口的、附带原有功能的、并且面向一般消费者直接销售的电子产品。这些产品需要符合 EU 统一的安全规格，负有在产品上粘贴表示符合的 CE 标志义务。）所采用。汽车厂商及部件厂商等要在欧洲市场开展业务，必须符合这一标准。

目前，国外在汽车电子行业的管理现状总结如下：

1、国外将 ISO 26262 标准纳入汽车法规

欧洲计划将 ISO 26262 标准正式纳入汽车法规，美国也计划将 ISO26262 标准纳入国家的强制性标准，促使满足 ISO 26262 标准的部件成为车厂标配，进而推助该标准应用。

2、国际汽车行业积极响应

ISO 26262 标准发布后，虽然世界范围内，暂时没有出现官方层面的强制执行要求，但该标准的执行，将减少因为电子器件失效造成的交通事故和降低潜在召回风险，所以目前国际大型车企非常重视 ISO 26262 标准的应用和推广。标准颁布后，国际上许多知名品牌车企对电子电气部件的采购已经明确提出新的要求，即部件需要符合 ISO26262 标准并获得独立的第三方认证。如果部件无法满足标准的

要求，部件供应商可能痛失大量订单。国内大量零部件供应商对此也十分关注，积极进行标准的培训、咨询和产品的认证。

3.1.2 国内标准贯标现状

目前，国内汽车电子行业标准管理现状如下：

1、国内汽车电子软件功能安全标准出台不久，缺乏应用技术支撑能力

在国内，ISO 26262 标准发布后，国家标准化管理委员会于 2012 年 8 月批复了全国汽车标准化技术委员推荐性国家标准《道路车辆功能安全》的立项申请；正式下达了推荐性国家标准《道路车辆功能安全》的制定计划。按照国家标准制定计划安排，全国汽车标准化技术委员会组织国内外整车和零部件企业共同开展《道路车辆功能安全》国家标准的研究和制定工作，并于 2017 年发布了汽车行业功能安全标准 GB/T 34590 《道路车辆功能安全》。

由于国内汽车电子软件功能安全标准刚发布不久，目前，汽车软件功能安全方面的分析研究工作局限在少数大型整车企业、高等院校和科研机构内，国内汽车电子软件功能安全标准应用技术支撑能力不足。

2、部分车企积极跟进，但能力薄弱

目前，国内汽车厂商在整车电磁兼容、电气环境、碰撞防护等领域已经做出了较多努力，但目前国内汽车电子领域的功能安全标准尚未出台。部分意识比较超前的民族品牌企业一直在关注 ISO26262 标

准的制定和发展，并且已经针对该标准的相关要求做出了计划，少数企业在执行 ISO26262 标准方面，已经明确推出了具体的时间表。

虽然国内很多企业在跟踪 ISO26262 标准，但能够完全遵照要求设计流程并满足该标准的产品目前还很少。国内大量汽车行业的民企在安全性分析、设计、实现、测试、管理方面的能力仍然非常薄弱，亟待帮扶。值得注意的是，随着中国汽车工业的快速发展，国内的汽车保有量大幅度增加，促使各大汽车厂商不得不关注软件功能安全，对软件功能安全的研发投入大幅增加，同时大量的研发人员投入到对汽车软件功能安全的研究中。

3.2 过程工业行业

3.2.1 国外过程工业标准贯标现状

1、欧美各国已强制执行相关标准，并出台标准应用指南

在过程工业行业功能安全管理方面，美国和欧洲走在先进行列。欧美工业发达国家在研究并致力解决功能安全问题，2003 年 IEC 发布了适用于石油、化工等过程工业的标准 IEC61511。随即美国将 IEC61511 标准作为国家标准。欧美等多个国家在功能安全标准出台之初就开始强制采用该标准，并将功能安全国际标准同本国的工业实践相结合，由本国安全监管部门提出明确的标准应用指南。

美国仪表协会（ISA）1996 年 2 月提出了 ISA S84.01《过程工业安全仪表系统的应用》。该标准迅速成为美国国家标准（ANSI），并被美国职业安全与卫生管理局（OSHA）的过程安全管理程序、美国

环保署（EPA）的风险管理程序立法强制执行。美国国家标准协会（ANSI）负责协调指导美国标准化活动，同时进行行业的行政监管。

在欧洲，德国标准化学会（DIN）、法国标准化协会（AFNOR）、英国标准协会（BSI）各自负责本国的过程工业仪表功能安全标准的制定实施以及行业的监督管理。

2、欧美各国在过程工业领域具有完善的检查认证服务体系

美国具有 UL（美国保险商试验所）负责进行专业、权威的安全检测、鉴定和认证。欧洲具有 INTERTEK（英国）、TÜV（德国）、BV（法国）、SGS（瑞士）、KEMA（荷兰）等咨询认证机构负责过程工业仪表功能安全的咨询、测评和认证。

3.2.2 国内过程工业标准贯标现状

1、国内已等同转化国际标准，但没有出台应用指南

在国内工业控制领域，中国国家标准化管理委员会将 IEC 61511 标准于 2007 年转化为我国的国家标准 GB/T21109 系列标准，用于规范我国过程工业领域安全仪表系统的功能安全。中国国家标准化管理委员会、中国机械工业联合会、中国工业过程测量和控制标准化技术委员会负责跟进国际标准，制定过程工业仪表功能安全领域的国家标准，并协助工业和信息化部装备司进行该行业的监督管理。目前，过程工业中的功能安全标准在我国仅为推荐性标准，而非强制性标准，并且尚未发布与标准相应的应用指南或指令，这在某种程度上限制了功能安全标准在我国的实施步伐。

2、部分机构已开展相关软件功能安全测评认证，但不够系统化、

规范化

机械工业仪器仪表综合技术经济研究所功能安全中心在借鉴国外权威检测认证机构的基础上，从事过程工业仪表功能安全的技术研究、咨询、培训、测评评估和认证。在某些大型企业内部也在自行组织功能安全评估工作，如中国石化安全工程研究院已在中石化内部开展功能安全评估工作，但只局限于对过程进行风险分析和硬件安全完整性等级计算。

3.3 轨道交通行业

3.3.1 国外标准贯标现状

国外，轨道交通行业已形成完善的软件功能安全标准体系。世界发达国家的城市轨道交通系统已经有百余年的发展历史。这些国家不断总结经验教训，完善管理，已经形成了一整套科学的安全评估、认证、管理体系，制定了一系列切实可行的安全评估的技术标准。

根据国际标准 IEC61508，欧盟已制定包括 EN50126，EN50128，EN50129 等在内的一系列体现安全新理念的铁路相关标准，对于轨道交通装备系统，系统安全主要参照 EN50129 标准定义，软件安全主要参照 EN50128 标准定义。其标准的适用范围如下：

EN50126《铁路应用：可靠性、可用性、可维护性和安全性（RAMS）规范和说明》

EN50129《铁路应用：安全相关系统》

EN50128《铁路应用：铁路控制和防护系统的软件》

EN50159-1《铁路应用：通信、信号和处理系统》

日本在应用 IEC61508 标准上已经走在了前面，已将 IEC61508 国际标准转化为 JIS2C20508 国家标准，由日本铁路部门具有丰富安全技术经验的专家组成列车保安控制安全技术研讨委员会，讨论并制定了《列车保安控制系统的安全性技术指南》，在日本轨道交通系统的研制中发挥了重要作用。

3.3.2 国内标准贯标现状

轨道交通行业软件功能安全标准应用力度薄弱，认证仍以国际标准为主。我国轨道交通发展迅速，但功能安全规范与标准的制定还是相对落后。2012 年发布了 GB/T 28808《轨道交通通信、信号和处理系统控制和防护系统软件》，作为轨道交通领域软件功能安全标准，但只作为推荐性标准。目前主流的标准规范基本按照国际上通用标准实施。IEC61508 标准已等同转化为我国行业标准 GB/T20438《电气/电子/可编程电子安全相关系统的功能安全》，并在我国轨道交通工业中发挥了重要作用。

目前，国内很多轨道研制单位主要参考 EN50128、EN50129 标准的安全等级进行认证。

3.4 航空行业

3.4.1 国外标准贯标现状

1、国外航空行业具有比较完备的标准体系

自从百余年前飞机发明至今，航空机载控制系统经历了纯机械式、电子控制直到近 20 年广泛应用的计算机控制系统。随着计算机技术在航空领域的应用日趋深入，航空机载控制软件在整个航空机载控制系统中所占的比重越来越大。这在带来巨大积极作用的同时也带来了潜在的风险。一旦控制软件发生故障，可能直接导致飞机失控。因此，软件的适航性对于飞行安全至关重要。业界经过长期研究与实践，制定了相关的标准来规范软件的适航性。一般来说，世界各国均将飞机分成军用与民用两类。各国对军用飞机的研制有自己的标准和质量监督体系。而对于民用飞机说，由于跨国甚至洲际航线的存在，要求有一套能够被国际普遍认可的标准和质量体系来保证飞机的安全。DO-178 标准因此应运而生。

1982 年，RTCA 和 EUROCAE 正式发布了 DO-178 标准。这是民用航空机载软件开发中安全保证的一个里程碑。DO-178 标准一般有两个称呼，在美国（RTCA）被称为 DO-178 标准，在欧洲（EUROCAE）被称为 ED-12 标准。经过深入研发与实践，依据 DO-178 标准进行开发和认证的经验表明，DO-178 标准尚不完善。1985 年，新的版本 DO-178A 标准诞生，与之等价的欧洲版本则称为 ED-12A 标准。

DO-178A 标准是面向软件的开发技术和开发方法的标准，即规定了民航机载控制软件应该按照怎样的流程研发、应用哪些开发技术和方法。但是，20 世纪 80 年代至 90 年代正是软件行业蓬勃发展的时段，软件的开发技术更新很快，新的技术和方法层出不穷。这直接导致 DO-178A 标准难以满足日益发展的软件技术本身。

为了解决这个问题，RTCA 再次修订该标准。RTCA 和 EUROCAE 的专家们设定了标准的制定原则，从原来的“面向开发技术和方法”改成“面向目标”和“面向进程”。DO-178A 标准由此而重新更新为 DO-178B 标准，在 1992 年推向航空工业界，成为至今为止航空机载控制软件经典标准。按照航空界普遍规范要求，民用飞机未经“民航标准体系”的适航认证不得投入飞行。而“民航标准体系”中，针对机载软件适航认证的，就是 DO-178B 标准。

2011 年，DO-178B 标准升级为 DO-178C 标准，与此同时颁布的标准还有 DO-330 标准，DO-331 标准，DO-332 标准，DO-333 标准等。新标准为适应技术的发展在软件工具验证、基于模型的开发和验证、面向对象编程、形式化方法等方面提出了新的要求。美国航空无线电委员会（RTCA）制定的 DO-178C 系列标准包括：

DO-178C《机载软件的审定考虑》

DO-248C《178C 的说明性文件》

DO-278A《空中交通管制等地面软件标准》

DO-330《工具鉴定要求标准》

DO-331《基于模型的设计和开发补充文档》

DO-332《面向对象技术补充文档》

DO-333《形式化方法补充文档》

这是民机适航领域的重要标准，是对民机机载软件、软件工具以及民航交通管理软件的研制和适航的指导材料。目前在航空工业界，DO-333 标准为代表的软件形式化方法正越来越受到重视，以确保机

载控制软件能建立在坚实的理论基础之上，从源头确保软件的正确性、安全性和可靠性。

2、国外航空行业具有比较完备的管理体系

美国联邦航空管理局制定了一系列法律法规，如《联邦航空条例》来保证航空安全。同时受政府和工业界的委托，美国航空航天工业协会、美国航空无线电协会负责国家航空航天行业标准库的建设与维护，形成了一系列的航空安全法规标准体系。

欧盟委托欧洲航空安全局起草了一系列的民用航空安全法规，同时给欧盟提供技术上的专家，并对有关国际协议提供技术上的帮助。欧洲航空航天与防务工业协会标准化分会承担起草航空领域标准的任务，完成标准后提交欧洲标准化技术委员会投票表决并成为欧洲标准，形成系统的标准体系。

3、国外航空行业建立了严格的监督管理认证机制

美国联邦航空局负责航空行业的监管，在民用航空领域内对飞机的设计、生产、使用、维护以及空中运输、地面保障等进行全面的监督、控制和管理；同时，为民用航空产品颁发型号合格证、生产许可证和适航证，为航空运输企业颁发营业执照，为机场和各类航空设施颁发合格证，没有获得适航证、营业执照或合格证的产品或企业不得进入航空服务领域。

欧洲航空航天与防务工业协会航空航天产品认证中心按照EN9133《航空航天系列质量管理体系航空航天标准部件的质量鉴定程序》的要求对航空航天产品进行标准符合性评估，提供航空航天产

品的认证证书，未通过认证的产品不得被使用。

随着 DO-178C 标准的发布，该标准已作为全球认可的用于指导机载软件研制流程的指南，民机上使用的机载软件均需要通过 DO-178C 标准适航认证。在欧洲和美国，如果一架民用飞机没有通过 DO-178C 标准适航认证就不允许在其领空飞行。

3.4.2 国内标准贯标现状

我国航空行业软件功能安全标准缺乏，缺少对 DO-178B/C 标准的技术支撑能力。在国内，航空发展相对国外尚存在较大差距，目前主流的标准规范基本按照国际上通用标准实施。1996 年 DO-178B 标准已等同转化为我国航空行业标准 HB 295-96《机载系统和设备合格审定中的软件考虑》，并在我国航空工业中发挥了重要作用。

目前，国内很多航空研制单位的机载设备已经通过了 DO-178B 标准认证。ARJ21-700，C919 大型飞机等民机型号的研制都极大的推动了 DO-178B 标准在中国的普及。目前我国自行研发的大型客机已经在部署应用 DO-178C 标准，包括对软件开发管理采用形式化方法的 DO-333 标准等。

3.5 核电行业

3.5.1 国外核电行业标准贯标现状

1、国外核电软件相关标准较完善

2001 年，IEC 发布了 IEC 61513《核动力厂安全重要的仪表和控制系统系统总要求》，并在 2011 年发布了修订版。本标准遵循国际原

子能机构（IAEA）关于核动力厂安全规定和导则等文件，采用与基本安全标准 IEC 61508《电气/电子/可编程电子安全有关系统（E/E/PES）的功能安全》相同的“生存周期”模式，给出了核动力厂安全重要仪表和控制（I&C）系统总要求。

IEEE 依据美国核电工程的设计、建造和运行经验，以及大量的研究、试验成果，编制和修订了一系列标准。IEEE 核安全有关标准体系是以 IEEE603《核电厂安全系统准则》、IEEE308《核电厂 IE 级电力系统准则》和 IEEE323《核电厂 IE 级设备鉴定》为基本标准，连同其他相关子标准共同构成满足核电厂安全准则的安全级电气系统和设备的标准体系。

RCC-E《核岛电气设备设计和建造规则》是法国依据国际标准（IEC 核电专用标准和 IEC 常规工业的基础标准）、法国标准和欧洲标准，结合法国核电工程实践经验编制的一套电气设备和系统在设计、建造方面的“技术规则”，用于核岛系统安全级电气系统和设备（包括仪表、控制和供电系统）的设计和建造。

2、美国和法国走在核电领域的前列，管理也较完善、先进

美国有关核电标准是以联邦法规和管理导则为依据，各技术学会（如电气和电子工程学会IEEE、核学会ANS、仪表和自动化学会ISA）编制的本专业范围的行业标准。这些标准经国家标准研究院认可后成为国家标准，并由美国机械工程师学会完成对核电设备的设计、分析和建造、运行和维护、质量保证和控制监管等一系列管理技术的监督和认证，保证核电的安全、高效运行。

法国也拥有自己完备的核电法律法规制定执行机构和系统的标准修订发布机构，更具备高科技的核电生产建设企业，以及专业高效的核电检测、测评、认证组织，保证了法国核电的高效、安全运行。

3.5.2 国内核电行业标准贯标现状

国内核电领域标准、法规不够完善，检测认证体系不够完善。截至 2008 年，我国已编制 440 多项核电标准，其中 20％为国家标准，80％为核行业标准。在这些标准中，绝大部分是与核岛相关的标准，而常规岛和核电厂配套子项 BOP 方面主要采用常规电力标准以及其他一般工业标准。中国的核电生产量还较少，相关法规、标准不够完善。

中国目前核电的发电量还比较少，在国内核电领域，我国具备了包括国务院、国家核安全局、国家原子能机构、国防科工委等核安全管理机构，有国家标准化委员会和核能行业协会负责相关标准的修订，但 IEC 61513 标准尚未转换为我国的国家标准，我国主要借鉴国际先进标准，结合我国已有的核电工程经验编制适用于我国核电自主化建设的标准。我国现行的核电厂安全重要仪控系统的标准（包括国家标准和行业标准）基本上由国际标准或国外标准转化而来。采标策略以国际标准（IEC 标准）为主，辅以 IEEE 标准、ISA 标准和 RCC-E 标准。同时，我国核电测评、认证机构也不完善，正处于学习成长阶段，需积极借鉴国外检测认证机构的经验，不断积累强化。

3.6 医疗设备行业

3.6.1 国外医疗行业标准贯标现状

1、国外医疗软件具有完备的法规标准体系

2006 年，IEC 发布了 IEC 62304《医疗设备软件软件生命周期过程》，IEC 62304 标准是欧盟和美国均采纳的医疗设备软件标准。美国和欧盟在医疗器械安全分析管理方面，具备完备的法规标准体系。

美国食品药品管理局（FDA）作为医疗行业的一个主要职能部门，负责食品药品、医疗器械等方面的法律、法规、标准的制定、采用、修改和废除，形成了《医疗器械安全法案》、《食品药品和化妆品法案》、《食品和药品管理现代化法案》等一系列法案标准。

欧洲标准化委员会和欧洲电工标准化委员会负责欧洲医疗器械标准的制定、采用和修改，形成了 EN 60601-1-2006《医疗电气设备. 基本安全和基本性能的一般要求》、EN 60601-1-8-2007《医用电气设备.基本安全和基本性能的通用要求》和 EN 60601-2-12-2006《医疗电器设备.第 2-12 部分：肺呼吸机安全性特殊要求》等一系列标准。

2、国外医疗软件和设备具有严格的行业监管和认证测评机制

欧美各国具有严格的行业监管措施，同时也具有多家认证和第三方测评机构。在美国，有器械与放射健康中心（CDRH）、生物制品评价研究中心（CBER）和药物评价研究中心（CDER）等负责监督医疗器械的生产和经营，生产经销商必须在法律约束下进行经营活动。美国具有如 NAMSA 等机构专门从事医疗器械、包装材料、药物/器械组合产品的功效性和安全性检测、评价和认证。

欧盟有专门的部门负责医疗器械法律、法规的制定、采用、修改和废除，形成了《有源植入医疗器械指令》、《医疗器械指令》和《体外诊断医疗器械指令》等法律法规。在欧洲也有专业的第三方测试认证机构，如 TÜV 南德意志集团，在医疗器械领域提供包括咨询、认证、测试和工程师培训等服务。

3.6.2 国内医疗行业标准贯标现状

我国积极制定标准和进行医疗行业的监管，但医疗行业软件标准目前仍然缺乏。国内方面，国家食品药品监督管理局负责食品、药品、医疗器械、化妆品监管法律法规的起草，制定食品行政许可的实施办法并监督实施，组织制定、公布药品和医疗器械标准，组织实施各种稽查制度，严格查处重大违法行为。

国家标准化管理委员会、医疗器械标准管理中心紧跟相关国际标准，负责医疗器械国家标准的制定、评审、修订和发布，制定了 GB 9706.1-2007《医用电气设备第一部分：安全通用要求》等标准，并于 2008 年 7 月 1 日实施。

中国医疗器械质量认证中心负责按照医疗器械的质量体系标准对企业质量体系进行审核和检查，按照确认的产品标准对医疗器械产品实施检验，对通过认证的产品和单位颁发符合法律和标准要求的产品质量认证证书、质量体系认证证书和认证标志。同时，也有浙江省医疗器械检验院、北京市医疗器械检验所、上海市医疗器械检测所等多家获得国家食品药品监督管理局（CFDA）认可的检测机构可按照国家相关标准对医疗器械进行检测认证。

但在医疗软件方面，国内标准比较缺乏，没有具体的相关标准发布。

3.7 国内外情况比较与差异分析

功能安全技术涉及安全设备、仪器仪表和安全监测控制系统等各个方面，随着各类设备中软件控制的占比越来越高，加强软件功能安全技术的研究和开发，可以极大地提高我国工业领域安全防护和管理水平，推动以电气、电子、计算机技术为核心的安全监测、监控系统的广泛应用，提高对整套装置、重大危险源和事故隐患的监控水平，降低整套装置及重要危险源、事故隐患点的风险，大幅度减少经济损失和事故死亡人数，达到用技术为国民创造安全的生产生活环境目标。

通过上述几个章节，我国工业领域软件功能安全标准体系与国外相比，存在以下差异：

1、**我国需加速推广应用软件功能安全的理念和技术标准**。国外的实践证明，以安全完整性等级和全安全生命周期管理为特色的软件功能安全是解决和提高电气/电子/可编程电子安全系统或装置功能安全水平的有效技术和管理模式。

2、国内外标准有差距，需积极转化国外先进标准，制定更具指导性的软件功能安全标准。在国外，尤其是欧洲在安全标准方面已经有很多成熟的标准和法规，各行业软件功能安全标准体系已初步形成。因此，我们应紧密跟踪和研究 ISO、IEC 和 EN 标准，积极转化国外先进标准。同时，由于国内外功能安全标准体系尚有差距，我们更需

要根据我国国情制定更具指导性的软件功能安全标准，进而建立我国功能安全标准体系。

3、梳理各行业软件功能安全标准，提高各行业标准的互补性和有效性。应参考国外成熟的安全保障体系和流程，对现有的安全领域的国家标准和行业标准进行系统地审查分析，搭配和协调各行业的软件安全标准，注重标准的有效性、配套性，解决目前安全相关标准存在的重复、交叉等问题。

4、加强第三方检验检测机构的监督机制建设。建立安全保护屏障必须依靠法律法规，我国功能安全法律法规和管理程序不完善，行业内缺少第三方检验检测机构的监督。软件功能安全体系作为功能安全标准体系的有机组成部分，都需通过法律、法规提高其实施性和应用程度。安全事故调查方面，欧盟的各成员国内成立事故调查机构，与第三方评估机构一道在延伸安全构架和安全监督方面发挥了关键作用，有效提高了安全管理水平。我国目前有第三方安全评估机构，但还没有与事故调查机构形成良好的配合机制，已影响到政府的公信力和企业的形象。

5、建立规范的功能安全测评认证体系，加强互认机制建设。加强软件功能安全标准的贯彻，应该借鉴国外功能安全（企业、人员、产品）认证经验，建立中国特色的功能安全认证机制，进而推动与国外机构的互认机制建设。

第四章行业发展趋势

4.1 国外发展趋势

软件功能安全标准将在现有标准的基础上，随着科技新技术的应用、结合各行业发展要求不断更新和完善，并逐渐淘汰不适合现阶段要求的标准规范，软件功能安全标准体系将不断壮大。标准近两年的发展主要集中在汽车电子、轨道交通和航空三个方面，其发展趋势如下：

1、汽车电子

随着汽车电子的发展，越来越多的电子控制单元（ECU）被安置在汽车上，SC22/SC88 等小组委员会（SC）已经发布了委员会草案（CD）以征求意见，这些草案于 2016 年 9 月最终确定为国际标准草案（DIS），并将最终版本作为 ISO 26262 标准第 2 版于 2018 年 1 月进行发布。

更新的目标之一是简化一些复杂活动，因此，为了简化功能安全管理，许多规划活动被放在第 2 部分（功能安全管理），将大多数与过程相关的要求归于该部分。另一个新的关键要求规定了在功能安全和其他相关条目之间建立有效的交流渠道，旨在提高网络安全和功能安全。

由于当前版本的缺陷，修订后的标准将包括重要应用范围的一些扩展，涵盖卡车、公共汽车、摩托车、半导体，ADAS 以及自主系统。

虽然 ISO 26262：2011-2012 标准在应用于乘用车的开发时展现出显著的益处，却并没有涵盖卡车，公共汽车和摩托车。

尽管卡车与公共汽车的要求大多数整合在标准的主要部分，但是正在考虑针对 3.5 吨以上的车辆进行一些小的更改。另一方面，由于 ISO 26262 标准中规定的许多要求也适用于安装在摩托车上的 E/E 系统，SC22 已经接受摩托车上的 E/E 系统也将被纳入到 ISO 26262 标准中。摩托车行业在全球建立的技术水平表明，现有的 ASIL 要求不适用于摩托车，解决这一问题的方法是将已提议的 MSIL 与现有 ASIL 达成一致。

2、轨道交通

在轨道交通系统领域，功能安全目前是一个从政府主管部门（发改委、中城协、政府）到业主（各地建设运营单位）、到供应商（信号系统总包方、国内外自研单位）、到认证方（TÜV 莱茵、劳氏、TÜV 南德等）都已达成基本共识的要求。从安全功能分配来看，关键设备如联锁、轨旁控制器、车载控制器均需达到 SIL4 等级要求，非关键设备需要达到 SIL2 等级要求。

同时，轨道交通领域目前已经形成了一整套科学的安全评估、认证、管理体系，制定了一系列切实可行的安全评估的技术标准。后续将在现有标准的基础上，结合轨道交通和新技术的发展要求，继续更新和完善轨道交通功能安全标准体系。

3、航空行业

当前，国际航空工业界对机载控制软件的功能正确性和安全性的要求日益提高，并已经从传统的软件开发过程控制管理和孤立的开发技术规定转向采用具有特定理论基础依据的更为严格的软件开发方法学。例如，2011 年升级而来的 DO-178C 系列标准中，规定了软件开发按照模型驱动（Model Driven）的方法并应用形式化方法完成软件需求分析、建模、验证和测试。与此相对应的规范标准文档分别是 DO-331 标准和 DO-333 标准。

值得一提的是，DO-333 标准对形式化方法的应用做出了强制要求，并推荐了形式化建模和验证等核心方法与技术，然而未明确规定具体的验证方法和技术。例如，当前著名的形式化方法 B 方法或 Event-B 方法并未明确被引入。

从发展趋势来看，由于航空机载控制软件是典型的安全攸关软件，采用具有严格数学基础的形式化方法是大势所趋，在未来很长一段时间内应有更广阔的发展空间。

4.2 国内发展趋势

国内软件功能安全标准的发展在一段时间内将处于不断学习国外先进标准并进行转化的状态，由于部分行业软件功能安全标准尚未发布，部分行业功能安全标准覆盖范围不够充分，标准的制定和修改将是国内功能安全标准发展的常态。

对于已转化国外标准的行业，标准的修订和本地化修订需不断加强，建立更具有指导性适用于国内行情的功能安全标准。其中汽车电

子、航空等领域的国内标准发展趋势如下：

1、汽车电子

全国汽车标准化技术委员会于 2012 年开始，基于 ISO26262 标准全面推进《道路车辆功能安全》国家标准的研究和制定工作，制定符合我国汽车行业发展需求的功能安全标准，并于 2017 年发布了汽车行业的功能安全标准 GB/T 34590 《道路车辆功能安全》。

在国家标准发布之前，部分国内自主汽车厂商及零部件供应商一直在关注 ISO 26262：2011 标准的实施应用，但大部分企业只是考虑应用引入标准，并制定了计划表，但真正应用该标准的汽车厂商比较少。由于汽车行业功能安全国家标准刚刚出台不久，对标准落地的技术支撑能力不足，国内自主品牌企业大多仍处于关注状态，部分企业已经针对该标准的相关要求做出了应用计划。

随着汽车智能化、网络化发展，软件在汽车电子中发挥的作用越来越大，地位越来越突出，汽车行业对汽车电子软件安全性的需求越来越迫切，汽车行业功能安全标准的推广应用将是大势所趋，国内自主品牌企业将逐渐与国际接轨，在功能安全标准的应用方面投入研究。同时，国内大部分汽车行业的研发企业在安全性分析、设计、实现、测试、管理方面的能力仍然非常薄弱，亟待帮扶。

2、轨道交通

随着我国城市化进程的加快，轨道交通已成为当前我国各大城市发展的重点。从我国城市轨道交通行业发展现状来看，近五六年我国城市轨道交通保持快速发展势头，“十二五”前四年已完成投资 8600

亿元，建成 1600 公里，预计 2020 年总里程达到 6000 公里。“十三五”期间每年要完成 500 公里，保持快速发展趋势。

与此同时，我国城轨装备产业高速增长，到“十三五”末年产值有望突破 6000 亿元，是国家重点发展的战略性新兴产业。《中国制造 2025》明确将先进城市轨道交通作为战略产业突破发展的重点领域。为了保证城轨装备符合安全、高效、绿色出行的要求，亟需运用产品认证的方式，对城轨装备进行有效的质量控制和准入管理。开展城轨装备认证，是通过与国际接轨的质量管理方式，促进城轨装备提质升级、助力中国先进城轨装备产业走出去的有效途径。

国家发展改革委、国家认监委联合发布通知，部署开展城市轨道交通装备认证工作。通知提出，按照自愿性认证和强制性产品认证相结合的原则，对车辆、信号系统等重点装备及关键零部件逐步推进自愿性产品认证，其中包括依据 EN50128 标准开展软件功能安全认证，力争到 2020 年实现城轨装备重点产品认证全覆盖，对直接关系运营安全和公共安全的城轨装备，依法开展强制性认证。

3、航空行业

国内目前在机载控制软件开发方面，由于考虑到适航认证需要，也已经开始推广 DO-178C 系列规范标准。其中的 DO-333 等标准已经被纳入新一代国产大型民航客机项目中予以实施。

2017 年 9 月 28 日，中国民用航空局与美国联邦航空局《适航实施程序》，于 2017 年 10 月 17 日正式生效。该协议根据《中华人民共和国政府与美利坚合众国政府促进航空安全协定》制定，实现了两

国民用航空产品的全面对等互认，内容涵盖适航审定在设计批准、生产监督活动、出口适航批准、设计批准证后活动及技术支持等方面的合作。该协议的签署为两国民航当局更深入和广泛的合作奠定了基础，也为两国民用航空产品的交流和工业部门的合作创造了良好的双边环境。

第五章标准示范应用案例

5.1 汽车电子控制系统软件

✓ 项目背景

随着电气器件、电子设备、可编程电子器件在汽车控制领域的大量使用，一些全新的安全问题不断地被媒体曝光。为降低汽车电子器件及软件等给企业、个人带来的众多安全风险，2011 年 11 月国际上发布了 ISO26262 标准。ISO 26262 标准受到了国内外各大汽车制造商、汽车零部件商的高度重视和支持，并纳入到 EC 法规认证。

2016 年 11 月，某公司为使新研发的“整车控制器底层软件”达到 ISO 26262 标准要求的 ASIL C 级，委托权威第三方测评机构开展软件功能安全技术咨询。在测评与咨询工作中，该项目团队首先依据 ISO 26262 标准检查产品研发生命周期各阶段形成的工作产品，分析差距;之后,指导其修订产品文档、完善软件安全设计、开展 ISO 26262 标准要求的各项测评。最终,该产品安全功能相关软件成功达到 ASIL D 级要求，并获得了功能安全认证证书。该项目最终实现的底层控制系统软件安全性架构见图 5-1 所示。

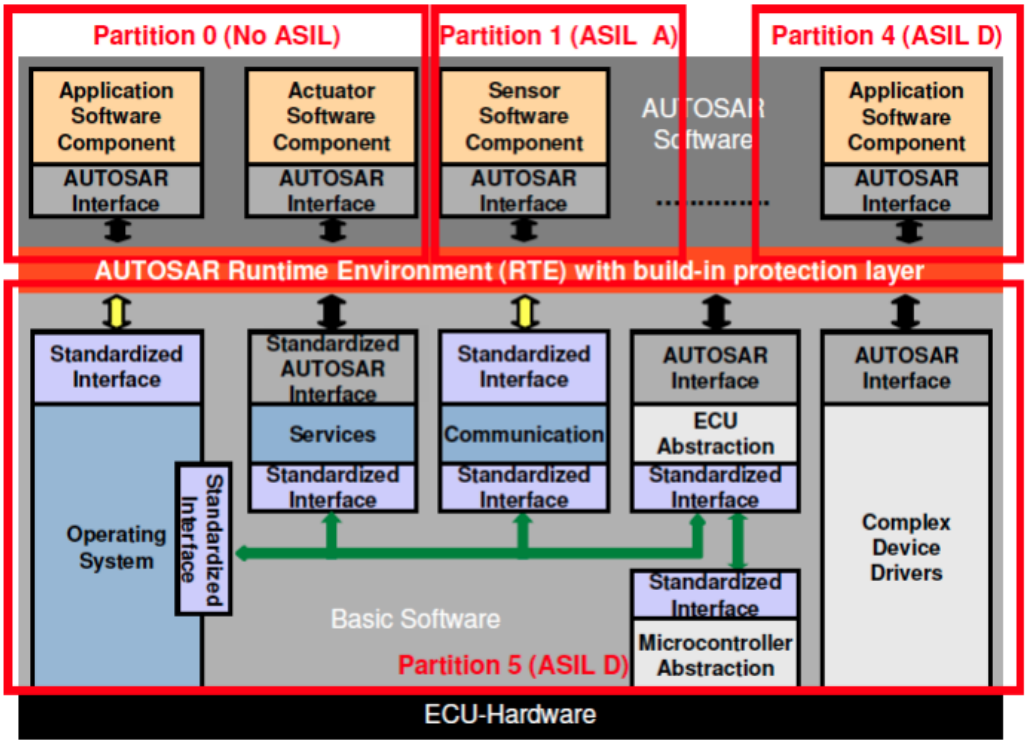

图 5-1 某型汽车电子控制器功能安全架构

✓ 主要工作内容

标准符合性测评认证

- 产品安全概率设计评估
- 安全完整性等级判断（ASIL）
- 产品生命周期各阶段产品审核
- 出具测评报告及认证证书

标准符合性认证咨询

- 故障树（FTA）分析、失效模式及影响分析（FMEA）
- 软件质量度量
- 用例设计方法
- 功能单元测试、集成测试及覆盖率分析
- 故障注入测试

- 性能测试（实时性、内存使用）

✓ **解决问题**

- 将最先进的安全标准应用到产品中
- 通过采用安全标准降低产品的风险
- 经过第三方认证可以获得竞争优势
- 证书可以证明产品符合标准要求
- 从我们多年的软件安全设计技术积累中获益
- 学习先进软件测试工具的使用方法

5.2 过程工业控制系统软件

✓ **项目背景**

近年来，随着石油化工、冶金等过程工业的快速发展，工艺复杂度和设备数量急剧提升，生产过程的信息化和自动化水平逐步提高，关键的自动控制系统如果在安全方面存在问题或薄弱环节，很可能导致恶性安全事故，对人员、设备和环境造成灾难性后果。因此，防止和减少火灾、爆炸、泄漏和失控等危险事故的发生成为过程工业领域面临的严峻问题。为了实现“安全工业”目标，越来越多的安全相关系统（包括自动控制系统和自动保护系统）用在不同领域，保护人员免受伤害，保证机械、整套装置甚至整个工厂自动、正常、安全地运转。

但是现有安全系统设计是否存在缺陷、安全系统的安全防护功能是否足够、安全系统是否已失效等这些问题仍然困扰着工业企业。IEC 61511 标准作为过程工业领域安全相关系统的功能安全标准，从系统、

硬件、软件、应用、安全完整性水平等方面对安全仪表系统进行了规范，随着 IEC 61508 标准和 IEC 61511 标准的颁发和在过程工业中的应用，上述问题有了规范化和标准化的解决方案。在国外，尤其是工业发达国家，在功能安全评估方面有着越来越强烈的要求，以致取得 SIL 认证的产品越来越多,而且产品的范围也在逐渐扩大。近年来，国内企业也越来越重视功能安全，陆续开展相关的认证和功能安全评估工作。

2016 年，某公司为其过程控制安全仪表系统软件委托权威第三方测评机构开展软件功能安全技术咨询服务。测评与咨询工作包括 SIL 定级、SIL 验证和 SIS 系统全生命周期管理、标准符合性咨询工作。该项目团队使用保护层分析方法（分析影响因素、严重程度、发生原因、发生频率、保护层等）确定每一个安全仪表功能的安全完整性等级，并验证 SIL 等级。同时，依据功能安全标准检查产品研发生命周期各阶段形成的工作产品，分析差距；之后，指导其修订产品文档、完善软件安全设计、开展标准要求的各项测评。

✓ **主要工作内容：**

标准符合性测评

- 安全概率设计评估
- 安全仪表系统安全完整性等级确定与分配
- 产品功能安全管理体系审核
- 安全生命周期各阶段产品审核
- 出具测评报告

功能安全技术应用咨询

- 故障树（FTA）分析、失效模式及影响分析（FMEA）
- HAZOP 分析服务
- LOPA 保护层分析服务
- 安全性分析、安全回路失效概率
- 应用软件质量度量
- 应用软件单元测试、集成测试及覆盖率分析
- 用例设计方法
- 故障注入测试
- 验证各种安全相关参数（SFF、PFD）
- 安全生命周期各阶段文档编制咨询

✓ **解决问题和效果**

- 将过程工业行业的功能安全标准在产品中应用落地
- 通过采用安全标准降低产品的风险，提高产品质量
- 规范企业管理研发流程，形成规范的安全管理体系
- 借助第三方测评认证服务，提升产品竞争力
- 企业在标准落地过程中学习软件安全设计技术
- 学习和提升软件测试水平，以及软件测试工具的使用方法
- 为后续产品的研发积累标准应用和安全开发经验

5.3 轨道交通产品软件

为了确保轨道交通信号系统的安全可靠运行，国际上普遍遵从

EN50128 标准为代表的一系列安全标准规范，要求轨道交通控制系统严格按照标准规范所推荐的方法与技术进行开发与维护。

某信号有限公司，通过与权威第三方测评机构开展软件功能安全技术咨询和自主研发，于 2012 年以列车控制系统通过国际最高安全等级 SIL4 级认证；并研发了自主知识产权的城市轨道交通信号系统整体解决方案，成功部署于上海轨道交通 17 号线，并走出国门应用于埃塞俄比亚首都亚的斯亚贝巴 LRT 线路，成为埃塞俄比亚乃至东非地区第一条城市轻轨，也是中国公司在非洲承建的首个城市轨道交通项目。该系统不仅完全由中国企业掌握全部自主知识产权，并且具有与进口信号系统同等的技术、功能和安全级别。

类似地，上海富欣智能交通控制有限公司，采用了形式化方法的部分技术，例如形式化分析与验证，所研发的列车自动保护系统与 2014 年成功通过 SIL4 级认证。

✓ **主要工作内容**

标准符合性测评认证

- 产品安全概率设计评估
- 安全完整性等级判断（SIL）
- 产品生命周期各阶段产品审核
- 出具测评报告及认证证书

标准符合性认证咨询

- 故障树（FTA）分析、失效模式及影响分析（FMEA）
- 软件质量度量

- 用例设计方法
- 功能单元测试、集成测试及覆盖率分析
- 故障注入测试
- 性能测试（实时性、内存使用）

✓ **解决问题**

- 将最先进的安全标准应用到产品中
- 通过采用安全标准降低产品的风险
- 经过第三方认证可以获得竞争优势
- 证书可以证明产品符合标准要求
- 形式化方法的实际应用
- 在上述基础上，给出了自主知识产权的完整解决方案

5.4 航空行业控制系统软件

相比于欧美发达国家，我国航空事业起步较晚，其电子控制系统软件研制能力也因此受到了一定的制约与局限。特别是大型商用客机的开发，目前正处于起步阶段。

相对于大型干线客机的电子控制系统软件，支线飞机和特种行业飞机的系统软件开发，则积累了更丰富的经验。一般来说，当前此类软件的开发普遍遵照 RTCA 的 DO-178B/C 标准来进行研制。该标准在应用实施过程中，主要引导了研制方从软件生命周期的各个阶段来组织软件的开发与交付，包括如下主要活动：

- 需求分析过程

- 需求验证过程
- 设计过程
- 设计验证过程
- 代码分析与测试过程
- 集成测试与系统测试过程

DO-178B/C 标准是否被贯彻落实，则由审定方来确认，我国民航总局下设审定机构。审定方主要根据软件生命周期中的文档、过程数据和辅助说明等佐证材料，来审定软件开发是否与标准所要求的一致。

5.5 核电反应堆安全检测系统软件

✓ **项目背景**

某核电站反应堆数字化控制安全保护系统工程样机应用软件属于属核安全级控制软件，主要实现监测核反应堆安全壳中的压力、温度、功率等工作参数，当监测到安全壳内出现超压、超温、超功率等故障时，及时控制反应堆停堆，以保证核反应堆的正常运行。按照核安全法规和相关标准的要求，软件 V&V（验证&确认）是保证软件安全性与可靠性的必要步骤，必须通过软件 V&V 过程才能证明和确认 DCS 产品中软件的安全性和可靠性。

为满足核电监管部门的技术要求，提高核安全级数字化仪控软件 V&V 的质量水平，弥补某公司核电安全级仪控软件在源代码评测方面的技术短板，增强该公司“仪控设备鉴定与软件 V&V 实验室”在工程样机应用软件 V&V 所出具结果报告的可信度，实现工程样机应

用软件的顺利上线，2014 年 5 月，该公司委托在软件源代码评测与实验室认证方面有着丰富工作经验的第三方测评机构，协助其完成“工程样机应用软件源代码评测”的工作。

✓ **主要工作内容**

软件测试

- 文档审查
- 代码静态分析
- 代码审查
- 代码走查
- 单元测试
- 软件集成测试
- 系统测试
- 软件可靠性评估

软件测评技术培训与指导

- 软件测试基础培训与指导
- 软件测试技术与方法培训指导
- 软件测试工具使用培训与指导

✓ **解决问题**

提高软件质量可靠性

- 发现大量问题、并指导整改，提高软件质量
- 指出开发过程、质量管理、配置管理的缺陷，提高工程化管理水平

提升该公司测评人员能力

- 规范测试作业流程
- 掌握科学的测试技术和方法
- 提高测试实战能力
- 掌握专业的测试工具使用方法和技巧

5.6 医疗设备控制系统软件

✓ 项目背景

医疗器械是世界上管制最严格的产品之一，某个功能性故障对患者可能意味着生与死的区别。确保医疗器械的功能安全对于生产商、进口商和分销商具有至关重要的意义，因为这些设备可能会影响使用它们的操作者和患者的健康和安全。2006 年，IEC 发布了 IEC 62304《医疗设备软件软件生命周期过程》，IEC 62304 标准是欧盟和美国均采纳的医疗设备软件标准。

2016 年 4 月，某公司委托权威第三方测评机构开展针对“某医用电子内镜视频采集控制系统软件”的软件功能安全技术咨询。在测评与咨询工作中，该项目团队首先依据 IEC 62304 标准审核软件质量管理体系和产品生命周期各阶段形成的证明文件，分析差距；之后，指导其修订文档、通过软件安全分析完善软件安全设计、开展符合标准要求的各项测评。

✓ 主要工作内容

标准符合性测评认证

- 软件安全级别判断
- 产品生命周期各阶段产品审核
- 出具测评报告及认证证书

标准符合性认证咨询

- 独立安全评估（ISA）
- 用例设计方法
- 单元测试、集成测试及系统测试
- 故障注入测试
- 性能测试（实时性、内存使用）

✓ **解决问题**

- 将先进的安全标准应用到产品中
- 通过开展风险分析降低产品的风险
- 经过第三方认证可以获得竞争优势
- 证书可以证明产品符合标准要求

第六章软件功能安全贯标工作建议

1、成立国家软件功能安全标准工作组

我国功能安全标准绝大部分是由国外已有的功能安全标准等同转化而来的，同时，很多领域目前没有转化国外标准或发布各自领域的软件功能安全标准。因此，建立覆盖工业各领域软件功能安全标准体系具有重要指导作用。

我国功能安全标准绝大部分是由国外已有的功能安全标准等同转化而来，虽然可以借鉴国外标准在功能安全领域已有的研究成果和先进经验，但是使用等同转化国外标准建立我国自己的功能安全标准体系，使得功能安全标准中同样缺少了适应我国工业发展特点及具体国情的特殊性。针对应用领域的企业标准制定方面也存在着与国家标准之间继承关系不强的特点。

参考国外成熟的安全保障体系和流程，对现有的安全领域的国家标准和行业标准进行系统地审查分析，搭配和协调各行业的软件安全标准，注重标准的有效性、配套性，解决目前安全相关标准存在的重复、交叉等问题。

为了确保软件功能安全标准的落地实施，成立软件功能安全标准工作组是重要前提。标准工作组主要承担软件功能安全标准体系规划的编制、国家标准的研究制定与审定、标准化学术交流和标准实施效果评价等工作。

成立软件功能安全标准工作组可以推动我国软件功能安全标准

的制定、发展和创新，充分发挥政府、企业、高校、研究机构、用户、中介组织等的作用，切实做好软件功能安全的标准化工作。

2、应用导向，试点先行，开展软件功能安全贯标行动

在工业和信心化部的指导下，结合国内外软件功能安全标准先进经验，面向汽车、工控、轨道、核电、航空、医疗领域企业的多样化、个性化需求，选择合适的试点企业，开展软件功能安全贯标行动。平台依托产业集群和工业园区，为广大中小企业提供政策咨询、能力对标、技术辅导、人才培训、检测评估等线上线下相结合的服务。

针对各行业生产企业，贯标行动可以为各行业生产企业的软件产品研发过程提供指导，优化和规范管理制度，有助于企业改进软件产品质量，降低产品安全风险，提高产品竞争力。

针对政府主管部门，贯标行动在规范生产企业产品、提高产品竞争力同时，有助于政府主管部门对生产企业的管理，提高管理效率和约束力，发挥政府主管部门的监督作用，保证企业的健康发展，建立主管部门和企业的良好发展机制。

3、紧急先行，成熟先上，推进软件功能安全技术全面应用

依托我国产业界、学术界和标准化方面的技术创新资源和成果，根据国家以及市场需求，梳理出紧急、成熟的技术，特别在安全关键基础设施、智能制造等领域加快软件功能安全标准的制定与技术应用。

面向软件功能安全生态体系建设，加快培育一批优秀的系统解决方案提供商，通过利用中央财政现有资金渠道，鼓励地方设立专项资金，加大对软件功能安全领域关键技术的投入力度，为符合条件的第

三方机构开展软件功能安全测评认证、技术应用提供支持，并在各领域组织开展行业系统解决方案应用试点示范工程，促进软件功能安全技术体系由点到面进行推广，从而调动产业链上下游企业对软件功能安全技术研究的积极性，推进各行业技术水平的快速发展。

参考文献

[1]国务院.《中国制造 2025》(国发〔2015〕28 号).

[2]IEC 61508(all parts),Functional safety of electrical/electronic/programmable electronic safety-related systems[S].

[3]靳江红,吴宗之,赵寿堂,胡玢.安全仪表系统的功能安全国内外发展综述[J].化工自动化及仪表,2010,37(5):1-5.

[4]GB/T 20438-2006 电气/电子/可编程电子安全相关系统的功能安全[S].

[5] ISO 26262-6:2010 Road vehicles - Functional safety -Part 6:Product development at the software level[S].

[6]GB/T 34590-2017 道路车辆功能安全[S].

[7]BS EN 50126 (all parts) Railway applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS)[S].

[8]BS EN 50128:2011 Railway applications —Communication, signaling and processing systems —Software for railway control and protection systems[S].

[9]BS EN 50129:2010Railway applications —Communication, signaling and processing systems —Software-related Communication in transmission system[S].

[10]DO-178C:2011 Software Considerations in Airborne Systems and Equipment Certification[S].

[11]IEC 62061:2005Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems[S].

[12]史学玲.功能安全标准的历史过程与发展趋势[J].安全控制技术,2006:6-8.

识别下方二维码，关注软件功能安全

微信公众号