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）

操作系统的安全认证

赵永望

浙江大学 计算机科学与技术学院/网络空间安全学院

zhaoyw@zju.edu.cn

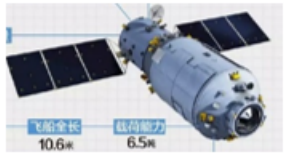
https://person.zju.edu.cn/zhaoyw

2022年12月17日

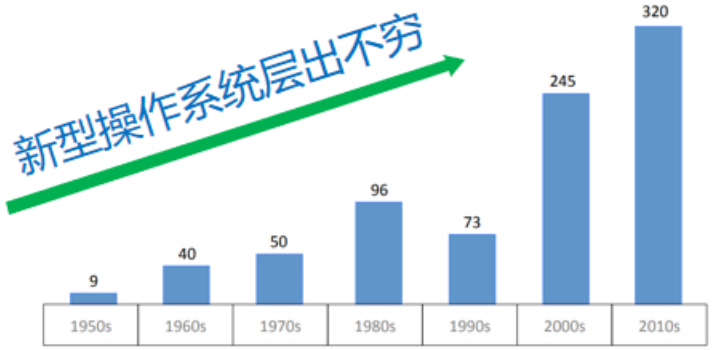
操作系统安全

安全攸关系统









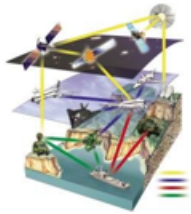
OS处于软件栈最底层
OS的Bug致命

OS安全面临新挑战，security成为关键

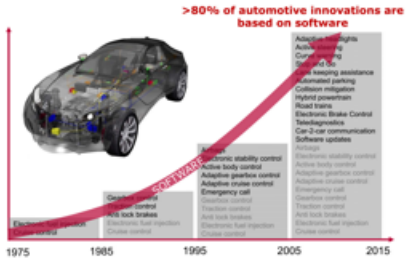
综合化
网络化
智能化
软件化

物联网

工业互联网



空天网络



操作系统的缺陷

Windows WannaCry

Kernel Version	Updates	Fixes
3.0	94	3,764
3.1	10	694
3.2	50	3,943
3.3	8	699
3.4	60	3,122
3.5	7	824
3.6	11	762
3.7	10	724
3.8	13	1,000
3.9	11	751
3.10	10	670

Linux内核缺陷

VxWorks

2019年，研究人员发现VxWorks 6.5版本11个漏洞，影响2亿台关键设备

ARINC INDUSTRY ACTIVITIES
An SAE ITC Program

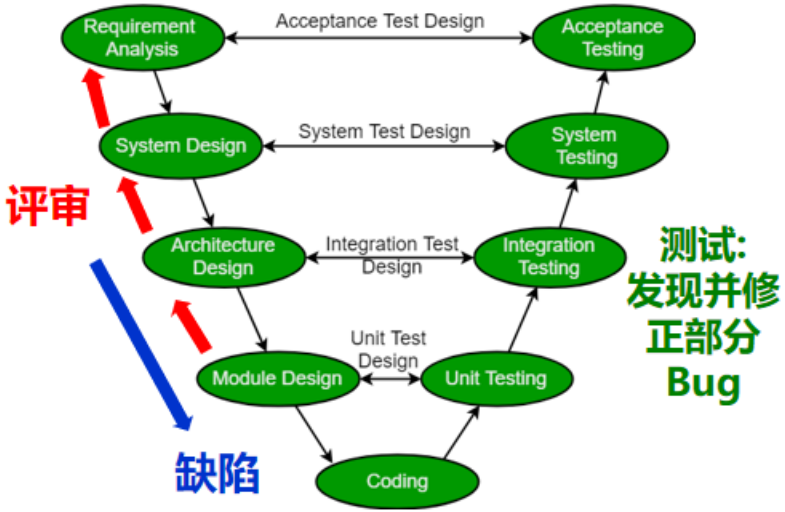
我们发现ARINC653标准10多个错误，商业RTOS中也存在

THE LINUX FOUNDATION
Zephyr™

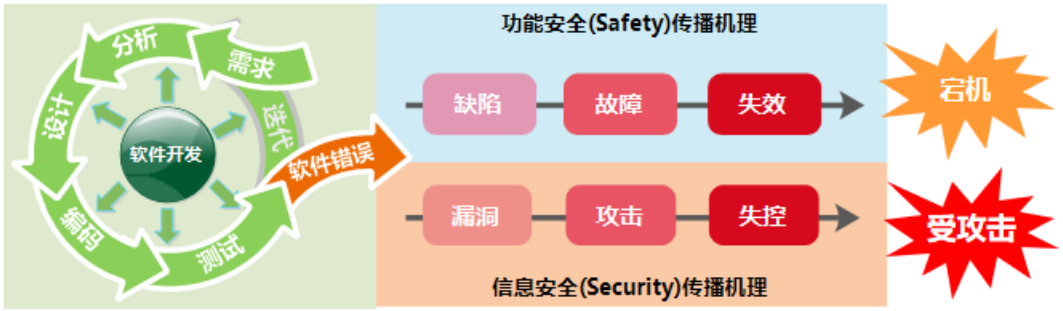
我们发现Zephyr RTOS的多个内存管理错误

为什么软件有这么多问题?

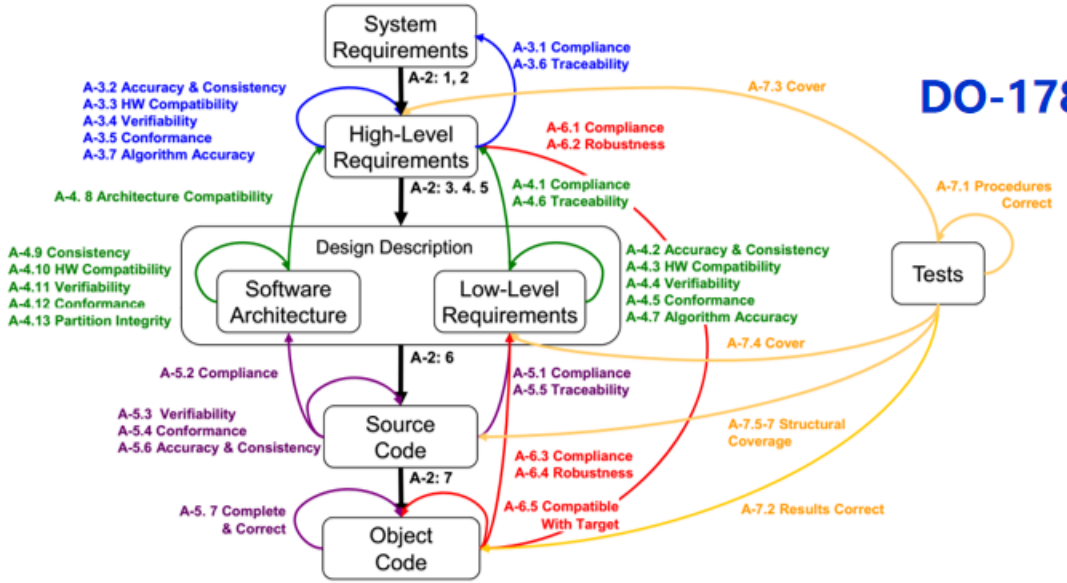
- **客观原因**: 软件太复杂，很难摸透运行规律和质量特征
- **主观原因**: 主流软件开发方法难以满足高安全可靠要求
  - 评审+测试：很多意想不到的情况，很多测试不到的情况



描述不精确、模型不一致、测试不完备

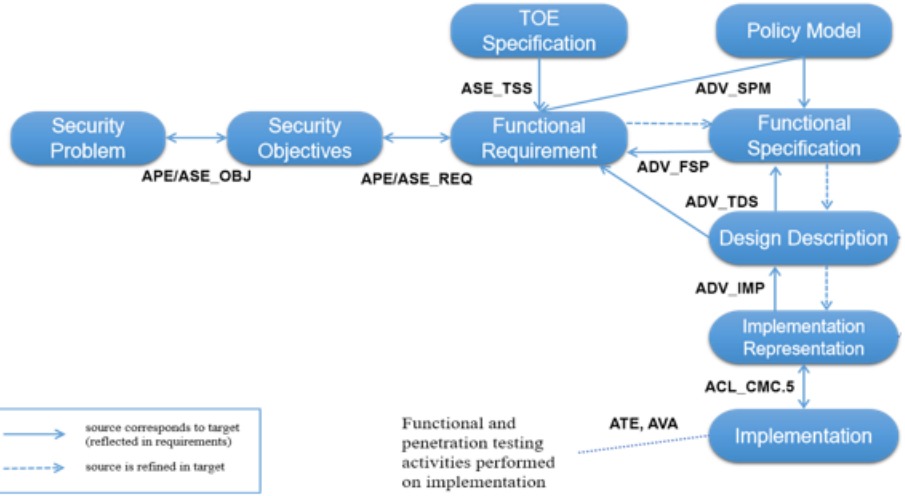


安全认证 如何解决软件的问题：严格的过程与证据



DO-178C

Common Criteria



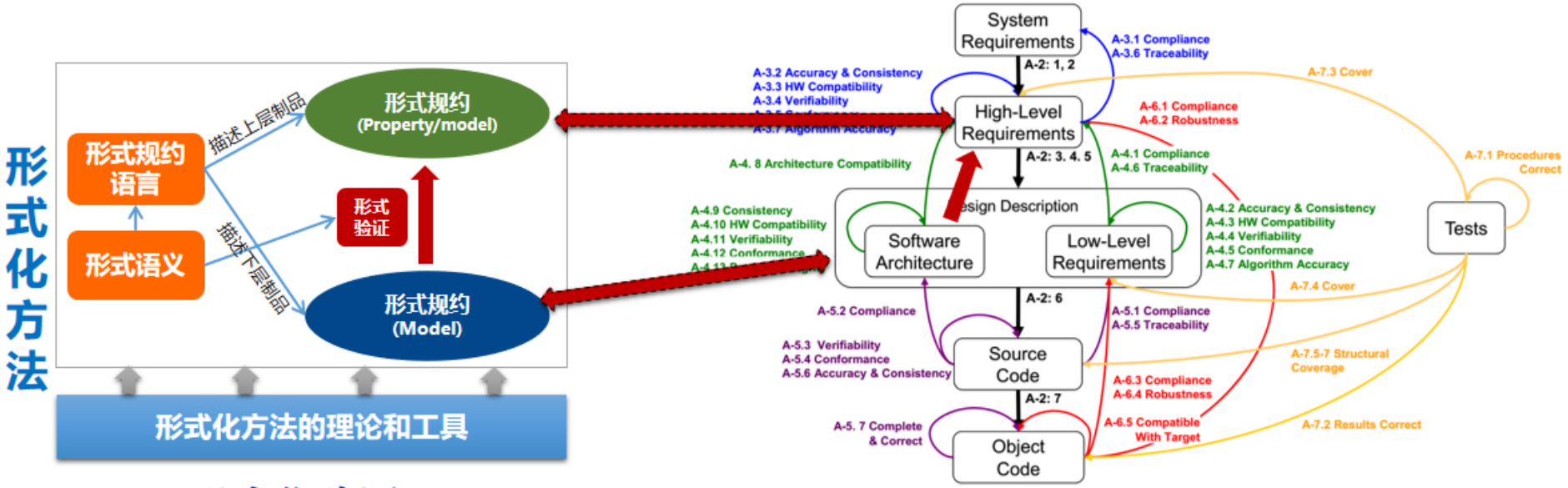
证据链

- Compliance
- Verifiability
- Traceability
- Accuracy
- Consistency
- Correct
- Conformance
- Compatibility

文档/数据/模型等
(非形式化/半形式化/形式化)

形式化方法起什么作用

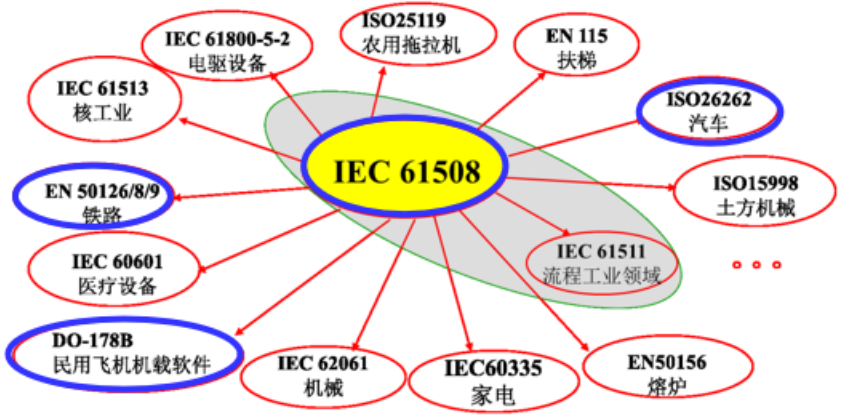
- 基于严格数学基础对计算机软硬件系统进行描述、开发和验证的技术
  - 更精确、更严格、更完备，高级别安全认证 推荐/强制要求使用形式化方法



形式化验证

- 模型检验、定理证明等

安全认证及相关标准



航空/eVTOL	DO-178 B/C, Level A/B/C/D/E, A级要求99.99999999%
轨交/核电	IEC 61508，SIL 1/2/**3/4级**
网络空间安全	网络安全等级保护，一级-五级（**四、五级别**）
航天	A/B/C/D级
金融	数字人民币、区块链智能合约
芯片、安全产品嵌入式软件	**CC EAL 1-7级**
无人汽车、电动汽车	ISO 26262， ASIL A/B/C/D级

高级别安全认证
强烈推荐或强制使用形式化方法

IEC 61508功能安全标准对形式化方法的要求

SIL级别	安全需求规约	软件架构	详细设计	模块测试与集成	软件验证
1	无	无	无	无	无
2	推荐	推荐	推荐	无	推荐
3	推荐	推荐	推荐	推荐	推荐
4	强烈推荐	强烈推荐	强烈推荐	推荐	强烈推荐

DO-178C的DO-333“形式化方法”附件

国际信息技术安全评估标准Common Criteria(CC)

CC级别	需求	功能规约	高层设计	低层设计	代码实现
EAL 1-4	非形式化	非形式化	非形式化	非形式化	非形式化
EAL 5	形式化	部分形式化	部分形式化	非形式化	非形式化
EAL 6	形式化	部分形式化	部分形式化	部分形式化	非形式化
EAL 7	形式化	形式化	形式化	部分形式化	非形式化

国内外OS 安全认证

	操作系统	DO-178B/C	Common Criteria	IEC 61508	ISO 26262	形式化验证程度
工业产品	VxWorks Cert/653/MILS	Level A	EAL 6+	SIL 3		○
	INTEGRITY-178B/RTOS	Level A	EAL 6+	SIL 3		◔
	LynxSecure/LynxOS-178	Level A	EAL 7			◑
	SYSGO PikeOS	Level B		SIL 3		◔
	QNX			SIL 3	ASIL D	○
	ED Separation Kernel		EAL 7			◕
	ProvenCore		EAL 7			◑
开源软件	uC/OS II	Level A				◕
	FreeRTOS/SafeRTOS			SIL 3	ASIL D	○
	Zephyr	Zephyr LTS考虑安全认证：DO-178, Common Criteria, IEC 61508				○
国产产品	翼辉SylixOS			SIL 3	ASIL D	
	睿赛德 RT-Thread			SIL 3	ASIL D	
	东土 Intewell			SIL 3	ASIL D	
	元心 SyberX		EAL 5+			◕

关键的DO-178C和CC EAL 6/7国内空白

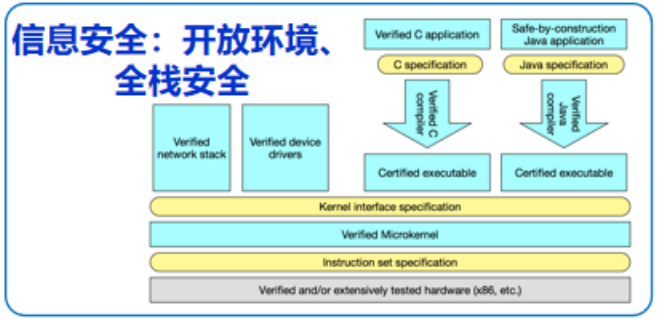
为什么信息安全认证越来越重要?

“网络空间已成为国家继陆、海、空、天四个疆域之后的第五疆域，与其他疆域一样，网络空间也须体现国家主权，保障网络空间安全就是保障国家主权”

—— 中国工程院院士 倪光南

国家战略与政策:

- 十四五与2035远景目标——加快数字化发展
- 《中华人民共和国网络安全法》
- 《中华人民共和国数据安全法》
- 《中华人民共和国个人信息保护法》
- 《关键信息基础设施安全保护条例》



DARPA

SMACCM

REMS

Rigorous Engineering of Mainstream Systems

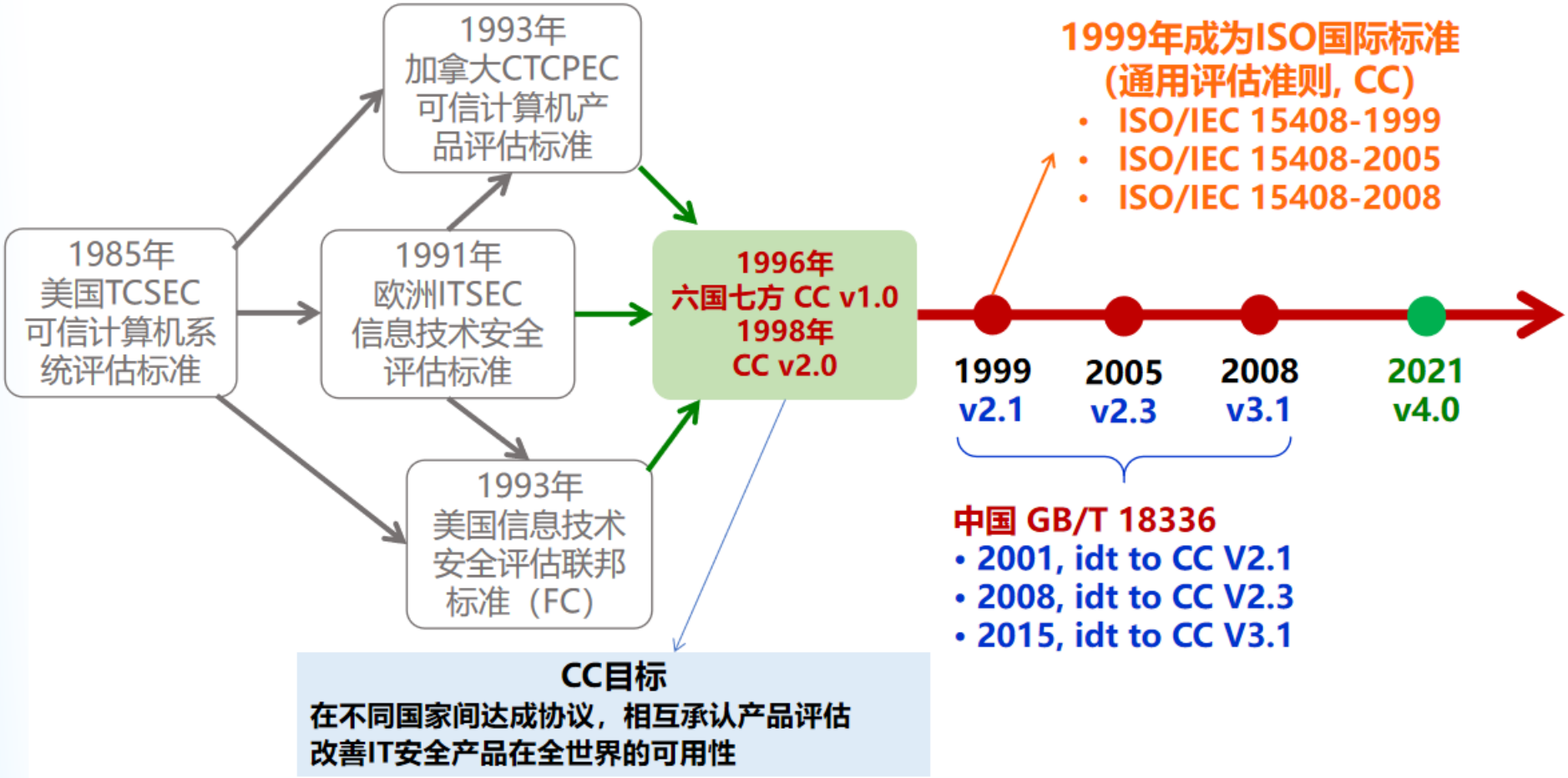
amazon web services

CC信息安全认证现状 (截止2022年12月)

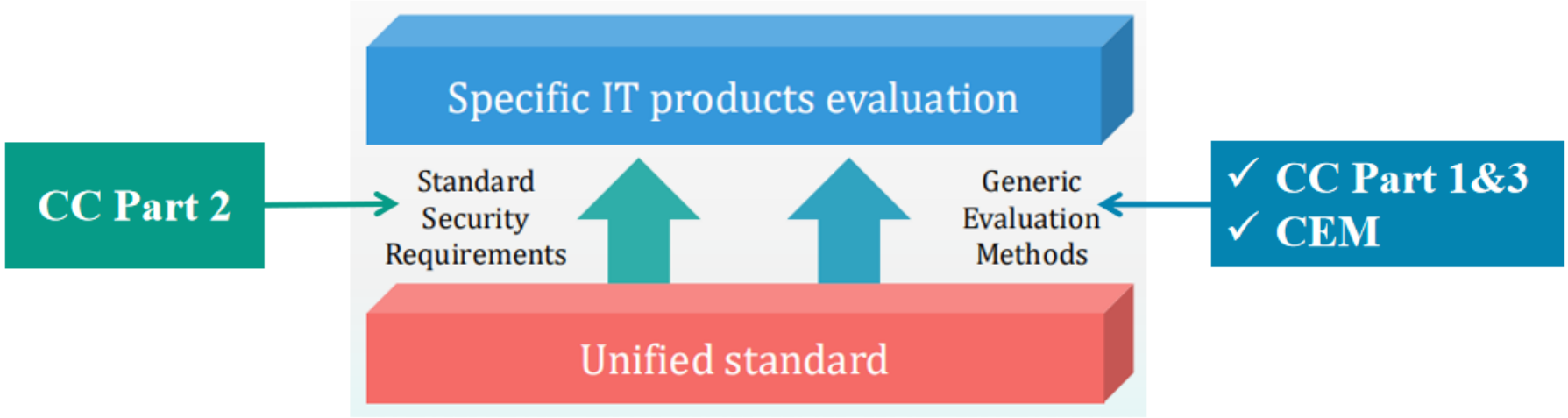
1645 Certified Products by Category *		
Category	**Products**	**Archived**
Access Control Devices and Systems	22	122
Biometric Systems and Devices	0	3
Boundary Protection Devices and Systems	43	198
Data Protection	62	155
Databases	14	78
Detection Devices and Systems	9	67
ICs, Smart Cards and Smart Card-Related Devices and Systems	586	1083
Key Management Systems	10	47
Mobility	29	54
Multi-Function Devices	233	328
Network and Network-Related Devices and Systems	226	493
Operating Systems	51	168
Other Devices and Systems	262	627
Products for Digital Signatures	60	92
Trusted Computing	38	31
Totals:	**1645**	**3546**
Grand Total:		**5191**

Certified Products by Assurance Level and Certification Date														
EAL	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**Total**
Basic	0	0	0	0	0	0	0	0	1	0	1	5	26	33
EAL1	0	0	0	0	0	2	1	2	6	4	3	3	2	23
EAL1+	0	0	0	0	0	1	0	0	1	0	1	0	1	4
EAL2	0	0	0	0	3	3	4	13	13	20	17	39	11	123
EAL2+	0	0	0	0	1	7	4	14	42	32	[illegible]	[illegible]	27	204
EAL3	0	0	0	0	1	2	0	3	6	10	[illegible]	5	0	36
EAL3+	0	0	0	0	1	6	4	1	10	[illegible]	12	18	29	86
EAL4	0	0	0	0	0	0	5	2	[illegible]	[illegible]	5	3	3	34
EAL4+	1	0	1	1	12	8	11	17	[illegible]	48	65	69	65	336
EAL5	0	0	0	0	0	0	2	[illegible]	3	1	2	0	3	12
EAL5+	0	0	0	0	6	5	[illegible]	17	50	47	72	50	27	279
EAL6	0	0	0	0	0	[illegible]	0	0	0	0	0	0	1	1
EAL6+	0	0	0	2	[illegible]	1	0	0	19	22	21	35	27	128
EAL7	0	0	0	[illegible]	0	0	0	0	1	0	1	0	1	3
EAL7+	0	0	[illegible]	0	0	0	0	0	1	0	0	1	0	2
Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	1	0	1	34	61	52	127	65	341
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Totals:	**1**	**0**	**1**	**3**	**25**	**36**	**36**	**71**	**233**	**258**	**303**	**390**	**288**	**1645**

CC标准发展历程


1985年
美国TCSEC
可信计算机系
统评估标准
1991年
欧洲ITSEC
信息技术安全
评估标准
1993年
加拿大CTCPEC
可信计算机产
品评估标准
1993年
美国信息技术
安全评估联邦
标准（FC）
1996年
六国七方 CC v1.0
1998年
CC v2.0
1999年成为ISO国际标准
(通用评估准则, CC)
• ISO/IEC 15408-1999
• ISO/IEC 15408-2005
• ISO/IEC 15408-2008
1999
v2.1
2005
v2.3
2008
v3.1
2021
v4.0
中国 GB/T 18336
• 2001, idt to CC V2.1
• 2008, idt to CC V2.3
• 2015, idt to CC V3.1
CC目标
在不同国家间达成协议，相互承认产品评估
改善IT安全产品在全世界的可用性

CC信息安全认证标准



ISO/IEC 15408
ISO/IEC 18045

Common Criteria

通用评估准则及方法

CC的安全理念

- 安全概念的层次化框架：一套科学的安全分析方法论

01 安全环境 Security environment

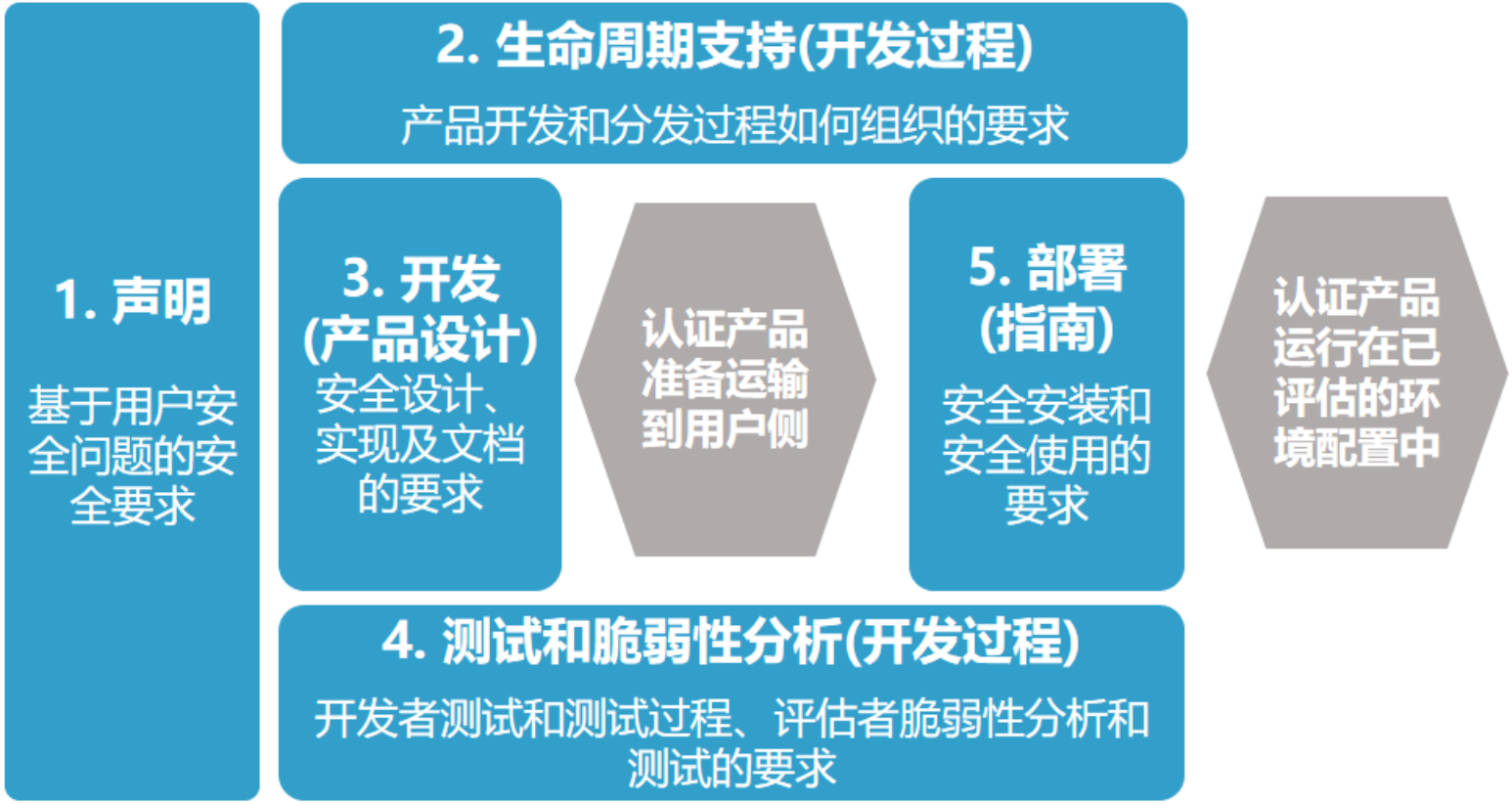
02 安全目的 Security objectives

03 TOE安全要求 security requirements

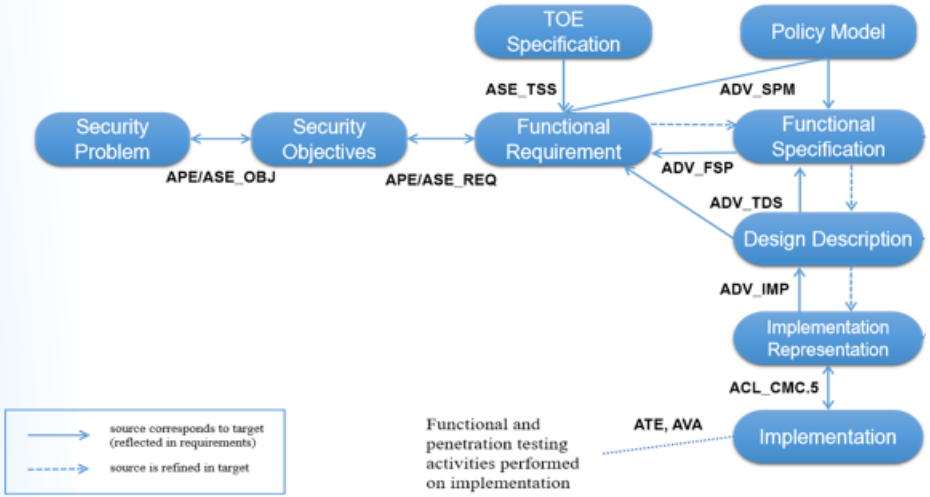
04 TOE安全规范 security specifications

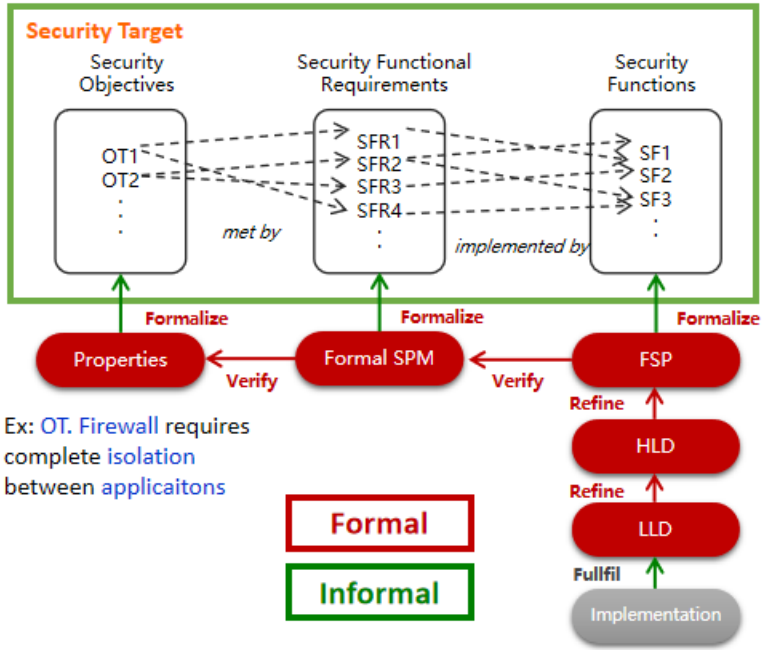
05 TOE实现

CC的5个方面


1. 声明
基于用户安全问题的安全要求
2. 生命周期支持(开发过程)
产品开发和分发过程如何组织的要求
3. 开发(产品设计)
安全设计、实现及文档的要求
认证产品准备运输到用户侧
5. 部署(指南)
安全安装和安全使用的要求
认证产品运行在已评估的环境配置中
4. 测试和脆弱性分析(开发过程)
开发者测试和测试过程、评估者脆弱性分析和测试的要求

EAL5/6/7 形式化要求





Ex: OT. Firewall requires complete isolation between applicaitons

CC信息安全评估的两个难点

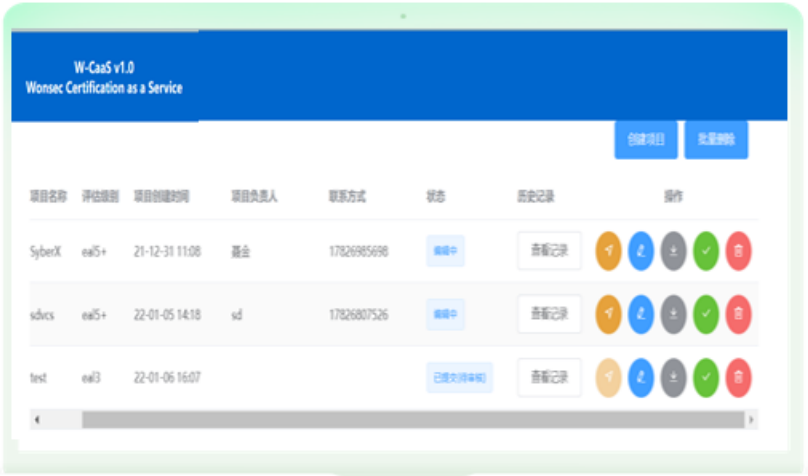
复杂、严格的评估过程
与证据要求

EAL5/6/7形式化
技术要求

CC安全认证云服务平台W-CaaS

- CaaS: Certification as a Service
- 专注于CC认证领域的一站式CC认证项目实施平台
- 可便捷、快速的进行CC认证的实施管理
- 支撑多个国内CC认证项目实施

望安科技 WON SEC



W-CaaS

- 符合ISO 15408、GBT 18336标准
- 覆盖CC EAL 1-7评估全过程
- 集成W-Cert，支持EAL 5-7级形式化

全结构化的评估数据管理

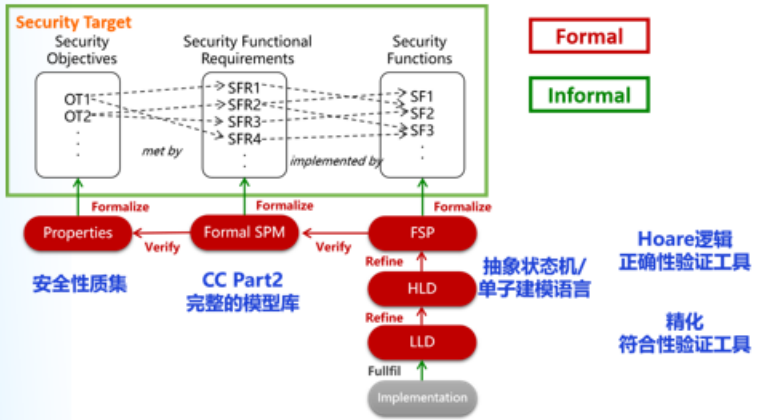
AI增强的自动分析与评估，极大缩短评测机构周期

模板化评估文档自动生成，直接报送国家级评估机构

云服务的线上协作，连通客户、评测机构、发证机构

高安全评估形式化工具W-Cert

- 满足CC标准形式化建模与验证需求的高可信形式化开发工具，有效支持从安全要求、安全策略、安全功能规范到安全设计的形式建模与验证，并提供CC评估所需的形式化证据。
- 开放的IDE，支持插件开发，桌面版与Web版；已应用到多个形式化验证与CC认证项目



望 安 科 技
WON SEC

产品能力

- ✔ 符合CC标准的安全功能要求SFRs形式化模型库
- ✔ 符合CC标准的功能规约FSP的形式化建模与验证
- ✔ 符合CC标准的TOE设计TDS的形式化建模与验证
- ✔ 评估证据自动生成

产品优势

符合标准——符合国际标准ISO/IEC 15408，符合中国国家GB/T 18336

可信、可定制——建模和验证过程完全可信，可进行自动检查；支持客户的定制化开发

提升效率——提高形式化建模、验证复用率；生成符合CC要求的评估证据

功能全面——覆盖CC标准全部形式化建模、验证需求

实施CC评估项目、国内外合作评估机构

元心操作系统EAL5+认证

国产元心安全微内核操作系统的形式化验证与安全认证

获得首个国内最高等级的软件 EAL5+级别证书，与华为鸿蒙OS同安全等级

正在承担的CC认证项目

- CCRC EAL6+项目(国内首个)
- 海微SeawayOS EAL5+认证
- 小米手机基础软件 EAL 4/5+认证
- 中国移动网络摄像机 EAL 3+认证
- 某OS EAL5+认证

中国网络安全审查技术与认证中心
CHINA CYBERSECURITY REVIEW TECHNOLOGY AND CERTIFICATION CENTER

信息产业信息安全测评中心（原信息产业部计算机安全技术检测中心）
中国信息安全测评中心计算机测评中心
国家金卡工程IC卡产品信息安全测评中心

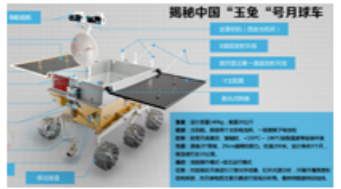
国家金融科技测评中心
National FinTech Evaluation Center
银行卡检测中心
Bank Card Test Center

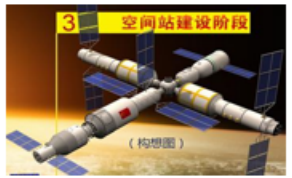
操作系统形式验证

- **采用自研工具，开展国产OS形式验证与认证，覆盖主流的国产RTOS产品**
  - 包括微内核、TEE、RTOS、Hypervisor、分区OS、通用OS等形态
  - 发现并修正了操作系统中大量错误

单位	验证的操作系统（已经完成或正在进行）
XXX	面向智能制造的场景操作系统
XXX	面向工业母机的嵌入式实时操作系统
华为	THEE
小米	MiTEE
元心科技	SyberX
大唐电信	安全微内核
中兴通讯	绿地嵌入式操作系统
军事科学院	无人机群体智能操作系统
航天五院	SpaceOS
……	……
ARINC653	ARINC653操作系统标准
Linux基金会	Zephyr RTOS
Linux基金会	Linux内核安全模块LSM
……	……

国产OS已应用到国家重大行业







参与操作系统与安全认证标准起草

ARINC653标准委员会

BOEING AIRBUS

LOCKHEED MARTIN WIND RIVER

Green Hills SYSGO EMBEDDING INNOVATIONS Rockwell Collins

Honeywell THALES

AEEC

Together "We Set the Standard"

ARINC 653 Meeting

Oct 11-13, 2016

Hosted by Boeing - Renton, WA

Draft Agenda

Tuesday Oct 11th

1. **Welcome, Introductions & Announcements** (AEEC, Boeing, Airbus)
2. **Agenda review** (Airbus)
3. **Status of Action Items** (Boeing)
4. **Response of ARINC 653 paper**
   "Event-based Formalization of Safety-critical Operating System Standards"
5. **Discussions and proposals**
   Multicore support
   a. Multiple concurrent partition execution
   b. Parallel Initialization
   c. Virtualization of processor cores

ARINC委员会专题讨论我们的成果

Common Criteria

Green Hills SOFTWARE, INC.

INTEGRITY-178 OS
CC EAL6+

HarmonyOS

华为鸿蒙OS
CC EAL5+

I am one of the co-chairs of the ARINC 653 Working Group. We are charged with maintenance of the ARINC 653 standards. The subject paper was brought to our attention by Mr. Labreche of CMC Electronics. We held a meeting this week in Seattle and discussed the results of your paper; in particular, the errors identified. We have agreed that the errors are real and we will be resolving them with the next release of the standard. I expect the release will not happen until 2019. We have just released supplement 4, and some of the modifications we are discussing for the next release will take some time.

Thank you for your efforts and thank you for contributing to the betterment of the ARINC 653 standard. If you have any questions please don't hesitate to contact me.

Gordon L. Putsche
Associate Technical Fellow
The Boeing Company
Phone 425-237-7698
e-mail: gordon.l.putsche@boeing.com

委员会主席、波音公司的Fellow给本人发来致谢邮件，认可我们的成果，并修订标准

Dear Prof. Zhao,

CC发来邀请邮件

I'm working at the German company SYSGO, and the same as us, you are active in separation kernels (we had email exchange once in 2016 about MCISK). As you know the security and safety assurance for separation kernels, especially in the multicore era, can be a quite challenging task and we think it would be a good idea to work out some security protection profile at the Common Criteria Users' Forum / CCUF (http://www.ccusersforum.org/). In particular the Common Criteria since its version 3.1 revision 5 allow to develop modular protection profiles, which allows to encapsulate disputed functionality into optional modules, and should facilitate agreement on the basic functionality (base PP).

Hereby, we'd welcome you to join the CCUF working group in foundation on separation kernel and similar devices, and to follow the attached instructions (PDF). If there is any question, please do not hesitate to ask me.

- 应邀加入ARINC653标准委员会
- 参与起草多核调度、安全服务等

- 应邀加入CC操作系统内核技术委员会(SK TC)
- 参与Security Protection Profile起草

发起操作系统国家标准研制工作

- 2021年与中国电子技术标准化研究院 联合主办**嵌入式操作系统标准研讨会**
- 2022年，参与发起成立全国信标委 操作系统标准工作组

中国电子技术标准化研究院

关于召开嵌入式操作系统标准研讨会的通知

各有关单位：

操作系统受到国内产业界、学术研究机构和政府部门高度重视。嵌入式操作系统作为数字基础设施的灵魂，是支撑数字变革的核心力量，伴随着人工智能、物联网、工业互联网、无人车、航空航天装备等产业迅猛发展，国内嵌入式操作系统发展步入快车道，标准化需求强烈。

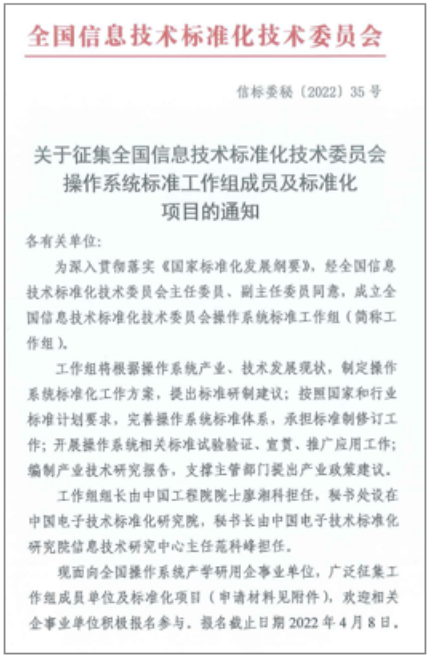
为推动产业协同发展，加快国内嵌入式操作系统标准化进程，中国电子技术标准化研究院和浙江大学联合主办嵌入式操作系统标准线上研讨会，诚邀参会！

会议时间：2021 年 12 月 6 日 星期一 13:30-17:00

会议报名：12 月 3 日前发送报名回执至 macq0804@163.com

联 系 人：马承青 13810203049

中国电子技术标准化研究院
信息技术研究中心
2021 年 11 月 26 日



全国信息技术标准化技术委员会

信标委秘〔2022〕35 号

关于征集全国信息技术标准化技术委员会操作系统标准工作组成员及标准化项目的通知

各有关单位：

为深入贯彻落实《国家标准化发展纲要》，经全国信息技术标准化技术委员会主任委员、副主任委员同意，成立全国信息技术标准化技术委员会操作系统标准工作组（简称工作组）。

工作组将根据操作系统产业、技术发展现状，制定操作系统标准化工作方案，提出标准研制建议；按照国家和行业标准计划要求，完善操作系统标准体系，承担标准制修订工作；开展操作系统相关标准试验验证、宣贯、推广应用工作；编制产业技术研究报告，支撑主管部门提出产业政策建议。

工作组组长由中国工程院院士廖湘科担任，秘书处设在中国电子技术标准化研究院，秘书长由中国电子技术标准化研究院信息技术研究中心主任范科峰担任。

现面向全国操作系统产学研用企事业单位，广泛征集工作组成员单位及标准化项目（申请材料见附件），欢迎相关企事业单位积极报名参与。报名截止日期 2022 年 4 月 8 日。

谢谢
请批评指正