中国IT产品信息安全认证体系与实践

中国信息安全认证中心

CHINA INFORMATION SECURITY CERTIFICATION CENTER

目 录

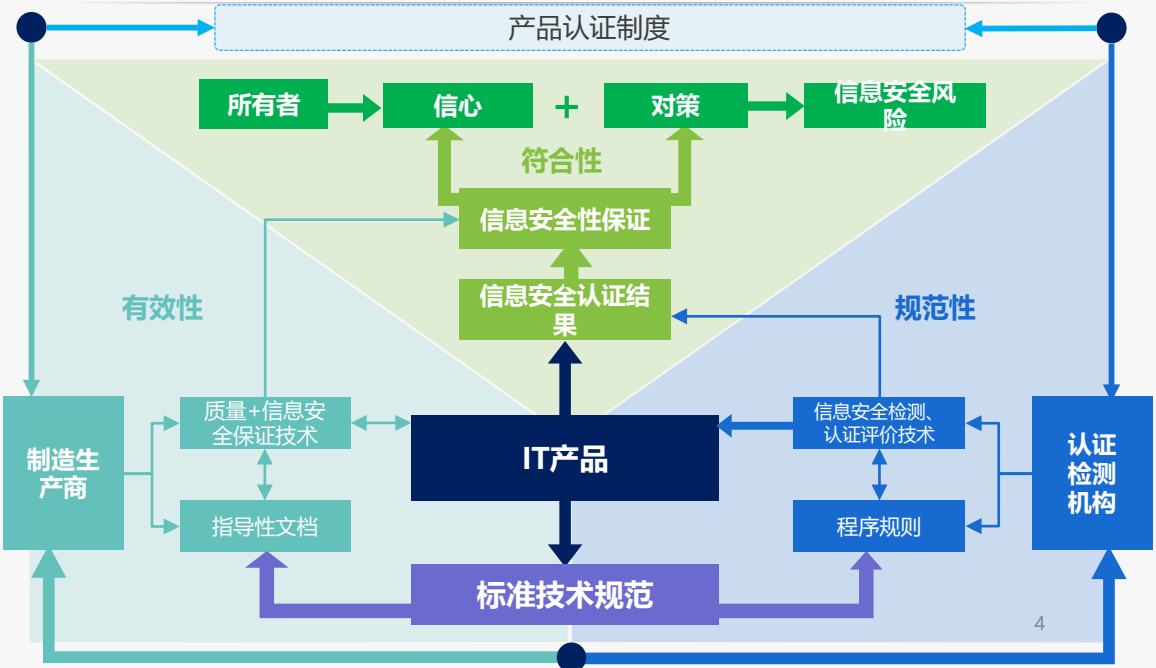
IT产品信息安全认证设立背景

IT产品信息安全认证建立背景

IT产品是组成基础网络、重要信息系统和工业控制系统等关键信息基础设施的基本单位，其信息安全重要性日益凸显。

IT产品自身信息安全漏洞风险日益严峻，使得相关网络和系统，面临着敏感信息泄露、系统停运等重大安全事件的安全风险。

认证的目的和意义


产品认证制度
所有者
信心
+
对策
信息安全风险
符合性
信息安全性保证
信息安全认证结果
有效性
规范性
制造生产商
质量+信息安全保证技术
指导性文档
IT产品
信息安全检测、认证评价技术
程序规则
认证检测机构
标准技术规范

认证制度体系

法律法规

《中华人民共和国认证认可条例》

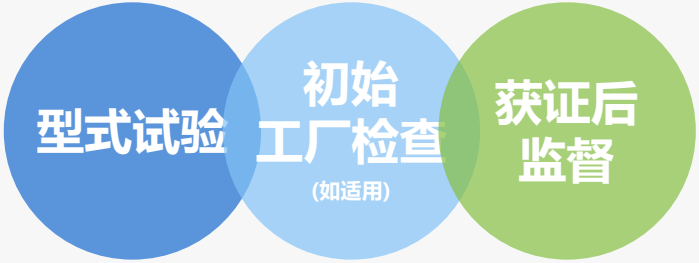
政策规章

国家部门发布的通知、公告，及部门管理规章等

规范性文件

- 技术规范
- 程序规则
- 管理要求

认证模式



认证证书的保持：证书的有效期三年

认证产品的变更

- 生产厂、证书持有者或相关地址等发生变化时，应向认证机构提出变更申请
- 其他证书变更情况依据有关实施规则规定执行；
- 认证证书到期后，如需要延续证书，应重新进行申请。

认证证书覆盖产品的扩展

- 增加与已经获得认证产品的认证范围时，应向认证机构提出扩展申请

认证实施规则

认证规则主要内容

适用范围	适用的产品范围
认证依据	适用的产品所对应的国家、行业标准和技术要求
认证模式	认证模式
认证申请及受理	申请单元划分原则或者规定
规范性文件	抽样和送样要求 关键元器件或者原材料的确认要求（需要时） 检测标准的要求（需要时）
工厂检查	工厂检查的要求
获证后监督	获证后跟踪检查的要求
认证证书	认证证书有效期的要求
标志的使用	获证产品标注认证标志的要求

规定具体产品认证要求
指导认证活动实施

标准和规范（GB/T 18336）

标准和规范（GB/T 18336）

- 我国信息安全认证工作开展的重要技术依据之一，是信息安全产品认证的通用标准；
- 是相关产品安全技术要求/国标/行标的引用和参考标准。

标准和规范

安全技术标准

GB/T 18336

信息安全产品	集成安全功能的IT产品	新技术新应用IT产品
IDS、IPS、UTM、安全审计产品...	智能卡、交换机、操作系统IT产品..	云计算、**工业控制**、物联网...

测试评估方法

安全保障评估：开发类文档、生命周期支持、指导性文档、测试文档

安全检测：独立性测试、穿透性测试、安全保障评估

检测结果：型式试验报告、评估技术报告

工厂检查要求

信息安全保障能力、质量保证能力核产品一致性核查

认证业务进展

技术规范 70项

- 边界访问控制产品、数据安全产品、身份鉴别和访问控制产品
- 入侵监测产品、基础平台产品、应用安全产品、安全管理产品
- 智能卡产品、集成安全功能的IT产品
- 工业控制专用产品、物联网专用产品

检测实验室 9家

中国电科第十五研究所、北京信息安全测评中心、上海市信息安全测评认证中心、中国电力科学研究院信息安全实验室、辽宁省信息安全与软件测评认证中心、公安部一所、中金金融认证中心有限公司、公安部三所、中国电子信息产业集团有限公司第六研究

认证证书

累计颁证366张，有效证书243张

目 录

工控网络面临的安全挑战

随着“中国制造 2025”、“互联网+”等国家战略的提出，工业企业信息安全建设也被提上日程，工业控制网络安全面临更大的挑战 。

控制安全	控制环境开放化使外部互联网威胁渗透到工厂控制环境
网络安全	网络IP化、无线化以及组网灵活化给工厂网络带来更大的安全风险
数据安全	流动和共享使数据和隐私保护面临前所未有的挑战
设备安全	设备智能化使生产装备和产品暴露在网络攻击之下

工控网络面临的安全风险

工控安全管理要求

法律、法规	《国网络安全法》	《关键信息基础设施安全保护条例》				
制度、工作机制	产品检测认证	关键基础设施保护	专项安全检查	… …		
部门管理要求	中央网信办	国家发改委	工业和信息部	公安部	国家能源局	… …
重点行业	轨道交通、电力交通、石化行业、航空航天装备 … …					
联盟、协会	工业控制信息安全产业联盟、工业互联网产业联盟、关键基础设施保护工作委员会……					

工控安全技术标准（国家）

全国信息安全标准化技术委员会（SAC/TC260）

- GB/T 32919-2016《信息安全技术 工业控制系统安全控制应用指南》
- GB/T 33007-2016《工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序》
- GB/T 33008.1-2016《工业自动化和控制系统网络安全 可编程序控制器（PLC）》
- GB/T 33009.2-2016《工业自动化和控制系统网络安全 集散控制系统（DCS）》

全国工业过程测量和控制标准化技员会（SAC/TC124）

- GB/T 30976.1-2014《工业控制系统信息安全》

全国电力系统管理及其信息交换标准化技术委员会（SAC /TC 82）

- GB/Z 25320《电力系统管理及其信息交换数据和通信安全》

全国电力监管标准化技术委员会（SAC/TC 296）

- 《电力二次系统安全防护标准（强制）》
- 《电力信息系统安全检查规范（强制）》
- 《电力行业信息安全水平评价指标（推荐）》

全国核仪器仪表标准化技术委员会（SAC/TC 30）

- GB/T 13284.1-2008《核电厂安全系统 第1 部分 设计准则》
- GB/T 13629-2008《核电厂安全系统中数字计算机的适用准则》

工控安全技术标准（行业）

机械行业标准

- JB/T 11960-2014《工业过程测量和控制安全网络和系统安全》（IEC/TR 62443-3：2008）
- JB/T 11961-2014《工业通信网络 网络和系统安全术语、概念和模型》（IEC/TS 62443-1-1：2009）
- JB/T 11962-2014《工业通信网络 网络和信息系统 工业自动化和控制系统信息安全技术》（IEC/TR 62443-3-1：2009）

核工业标准

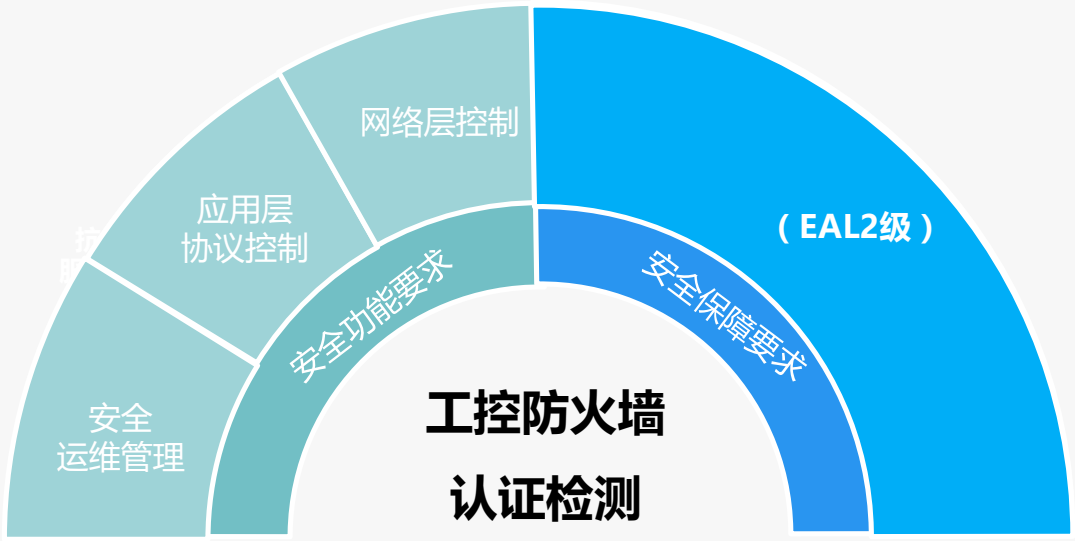
- HAD102-16《核电厂基于计算机的安全重要系统软件》

工控安全产品认证

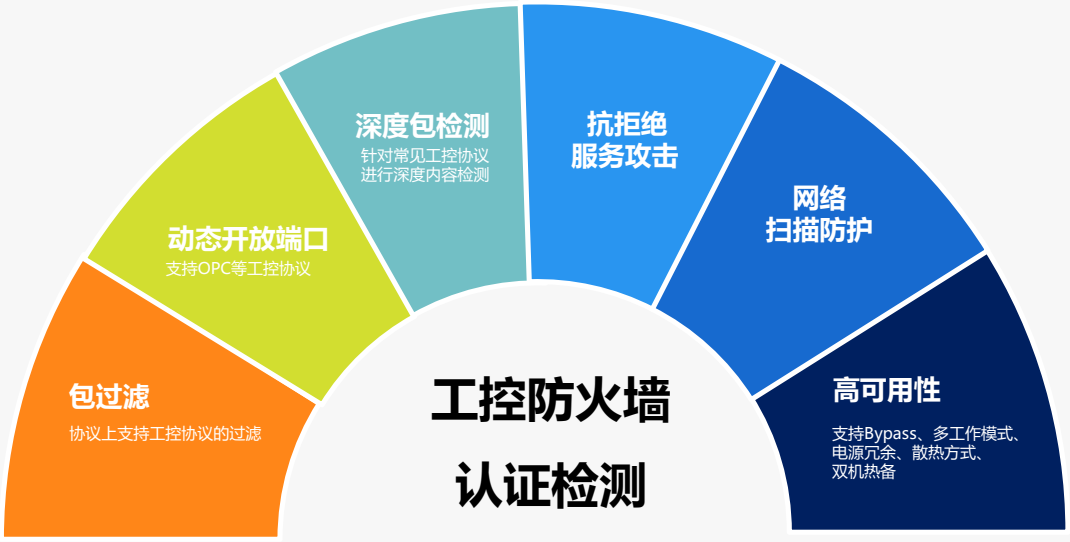
基于IT产品信息安全认证，ISCCC及合作实验室开展了工控产品检测认证，包括：工控防火墙产品、工控网闸产品、工控安全审计产品等。

相关实验室开展了PLC、DCS等设备的安全技术规范验证测试。

认证案例：工控防火墙



认证案例：工控防火墙


深度包检测
针对常见工控协议
进行深度内容检测
抗拒绝
服务攻击
网络
扫描防护
动态开放端口
支持OPC等工控协议
包过滤
协议上支持工控协议的过滤
工控防火墙
认证检测
高可用性
支持Bypass、多工作模式、
电源冗余、散热方式、
双机热备

认证案例：工控防火墙

	检测项	传统防火墙	工控防火墙
1	包过滤	基于MAC地址、IP地址、端口、协议类型和时间等的过滤	协议上支持工控协议的过滤
2	NAT	支持SNAT、DNAT	可选，部署在控制层通常透明部署
3	策略路由	支持相关策略路由功能	无相关要求
4	动态开放端口	支持FTP等协议	要求支持OPC等工控协议
5	深度包检测	针对一些常见协议（http、smtp等）	针对常见的工控协议进行深度内容检测
6	高可用性	双机热备	Bypass、工作模式、电源冗余、散热方式、双机热备

谢 谢！

布宁
中国信息安全认证中心/ISCCC
buning@isccc.gov.cn
www.isccc.gov.cn