



国内外工业控制系统 信息安全标准及政策法规介绍

全国信息安全标准化技术委员会秘书处 (TC)

2012年11月

提纲



工业控制系统概述

国外工业控制系统信息安全标准

我国工业控制系统信息安全标准

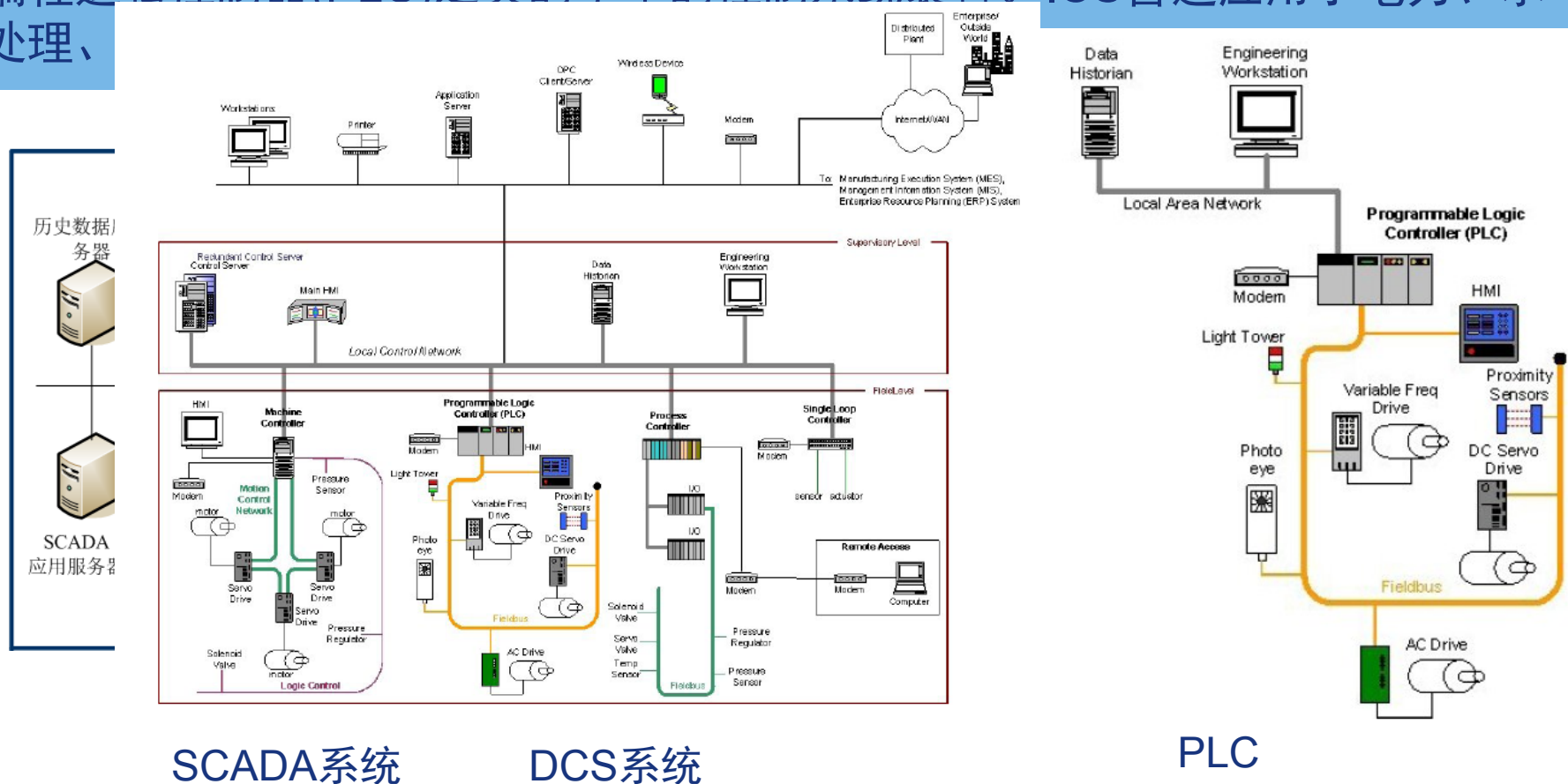
相关政策法规

结论与展望

工控系统概述

ICS

工业控制系统(ICS)是对多种控制系统的总称，典型形态包括 监控和数据采集(SCADA)系统、分布式控制系统 (DCS)，以及可编程逻辑控制器(PLC)之类的小型控制系统装置。ICS普遍应用于电力、水处理、





工控系统概述

工业控制系统与IT系统的差别：

网络边缘不同

工控系统在地域上分布广阔，其边缘部分是智能程度不高的含传感和控制功能的远动装置，而不是IT系统边缘的通用计算机，两者之间在物理安全需求上差异很大。

体系结构不同

工控系统结构纵向高度集成，主站节点和终端节点之间是主从关系，IT系统则是扁平的对等关系，两者之间在脆弱节点分布上差异很大。

传输内容不同

工控系统传输的是工业设备的“四遥信息”，安全问题大多集中于物理层面，安全防护要延伸到物理层并防止复杂的控制关系所产生的骨牌效应。

工控系统概述

工控系统面临的威胁

敌对政府、恐怖主义组织

偶然事件

恶意入侵

自然灾害

内部人员的恶意或无意
行为

工控系统存在的漏洞

策略和程序漏洞

平台漏洞

网络漏洞

工控系统相关安全事件

Cyber Storm

美国国土安全部分别在2006年2月6日、2008年3月10日和2010年9月27日共举办了三次网络风暴演习。三次演习都涉及多个政府部门、私人企业和厂商。演习目的在于检验包括电力、水源和银行在内的美国重要部门遭大规模网络攻击时的协同应对能力。

Aurora 测试

美国国家能源实验室于2007年3月进行了“极光发电机测试”，摄制的视频录像中显示了黑客通过攻击汽轮机导致汽轮机失控和电力中断。“极光”事件之后，美国政府全面加大了针对工业控制系统信息安全防护的力度，国会在2008年5月举办了电网安全听证会。

污水泄漏

2001年，在澳大利亚昆士兰，一名被解雇的工程师通过无线网络侵入水厂控制系统，造成水处理厂发生46次控制设备功能异常事件，导致数百万公升污水进入地区供水系统。

天然气爆炸

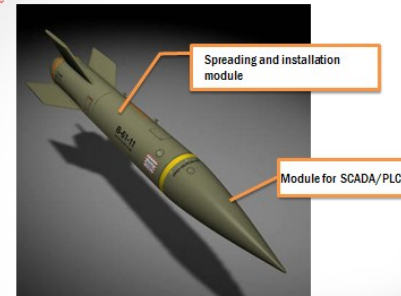
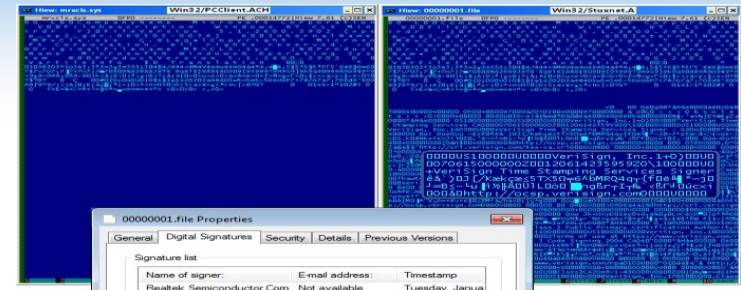
1982年6月，美国中央情报局通过利用SCADA系统的缺陷，对前苏联天然气管线进行了远程攻击，导致了有史以来最大的非核爆炸。



工控系统相关安全事件

Duqu 蠕虫

2011年9月，一种与Stuxnet具有相似结构的恶意代码Duqu出现在欧洲多个国家。Duqu的主要作用是 侦查和搜集资料。虽然Duqu不像Stuxnet一样直接攻击现场设备，但是可以随时根据攻击对象安装不同的攻击工具包，Duqu可能会成为寄居在基础设施内的定时炸弹。



Luigi Auriemma

2011年3月21日意大利黑客在主页上披露Siemens、Iconics、7-Technologies、RealFlex Technologies等公司产品存在34个漏洞，3月23日披露BroadWin公司产品存在2个漏洞。

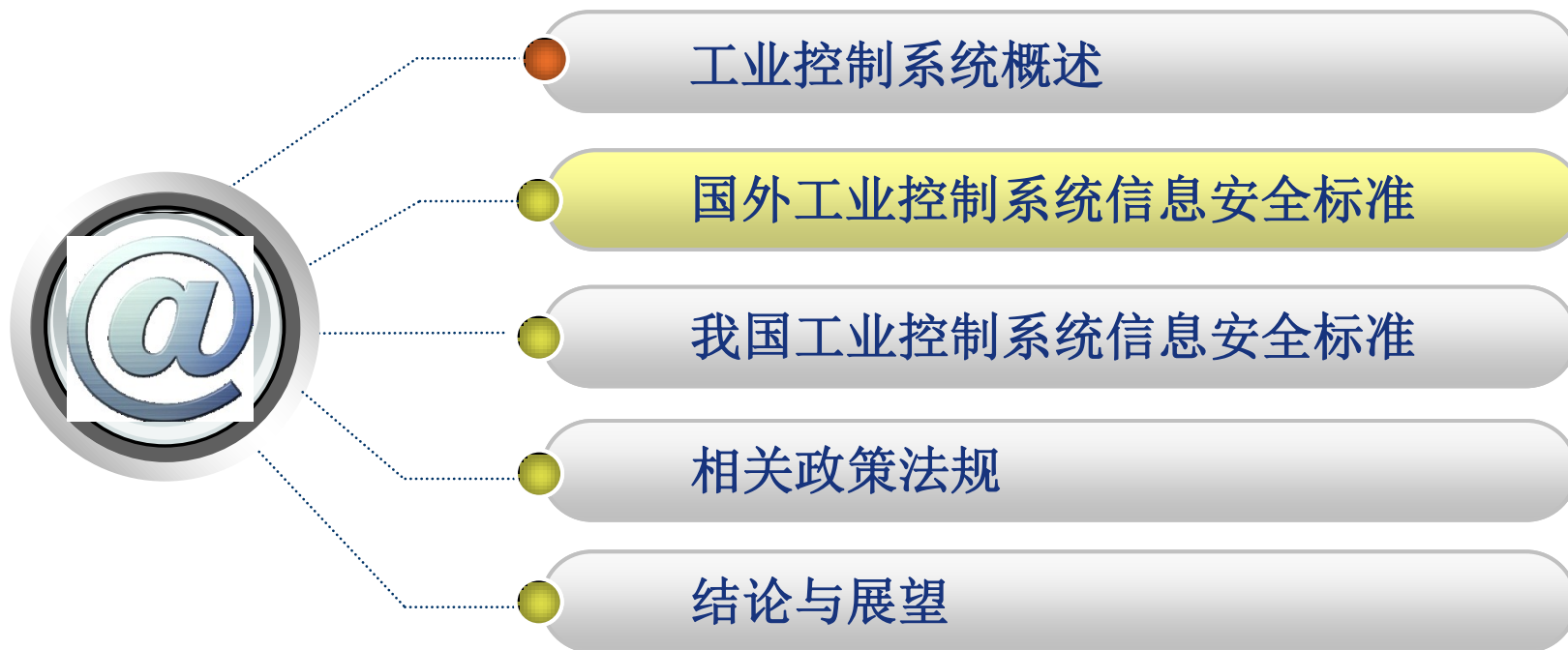
Dillon Beresford

2011年5月开始，美国NSS实验室持续报告出大量工控系统的安全漏洞，包括中国的力控软件和国外的Siemens在内。8月份的黑帽大会上，他为大家演示了如何入侵一台西门子S7 PLC，包括获取内存读写权限、盗取数据、运行指令以及关闭整台计算机。

McCorkle & Rios

2011年10月，美国DerbyCon会议上，Terry McCorkle和Billy Rios在报告中提到他们发现了存在于工控系统中的665个漏洞，其中75个漏洞位于网上可以免费下载的工控系统软件和HMI中。

提纲






国外工业控制系统信息安全标准

国际上，研究工控系统安全的标准化组织如下：

1. 国际电工委员会
(IEC, International Electro Technical Commission)
2. 国际自动化协会
(ISA, the International Society of Automation)
3. 美国国家标准技术研究院
(NIST , National Institute of Standards and Technology)



国外工业控制系统信息安全标准

IEC 62443标准

- IEC/TC65（工业过程测量、控制和自动化）下的网络和系统信息安全工作组WG10与国际自动化协会ISA 99委员会的专家成立联合工作组，共同制定IEC 62443《工业过程测量、控制和自动化 网络与系统信息安全》系列标准。
- 目标是定义一个通用的、最小要求集以达到各级SALS（Security Assurances Levels, SAL）的安全保障需求。
- IEC 62443一共分为了四个部分，第一部分是通用标准，第二部分是策略和规程，第三部分提出系统级的措施，第四部分提出组件级的措施。



国外工业控制系统信息安全标准

SP800-82 《工业控制系统(ICS)安全指南》

- SP800-82于2010年10月发布，是NIST依据2002年《联邦信息安全管理法》、2003年国土安全总统令HSPD-7等编制而成。它遵循《OMB手册》的要求“保障机构信息系统”，为联邦机构使用，同时允许非政府组织资源使用。

- 该指南概述了ICS和典型的系统拓扑结构，指出了对于这些系统的典型威胁和脆弱点所在，为消减相关风险提供了建议性的安全对策。同时，根据ICS的潜在风险和影响水平的不同，指出了保障的不同方法和技术手段。

- 该指南适用于电力、水利、石化、交通、化工、制药等行业的ICS系统。



我国工业控制系统信息安全标准

	组织名称	国际对口	挂靠单位
1	全国信息安全标准化技术委员会 (TC260)	ISO/IEC JTC1 SC27	中国电子技术标准化研究院
2	全国电力系统管理及其信息交换标准化技术委员会 (TC82)	IEC TC 57 (电力系统管理与相关信息交换委员会)	国网电力科学研究院
3	全国工业过程测量和控制标准化技术委员会 (TC124)	IEC/TC65 (工业过程测量、控制与自动化委员会)	机械工业仪器仪表综合技术经济研究所
4	全国电力监管标准化技术委员会 (TC 296)		电监会 输电监管部

全国信息安全标准化技术委员会 (TC260)

- ❖ 2002年4月 国标委发文正式成立，由国家标准委直接领导；
 - 国 际：ISO/IEC JTC1/SC27；
 - 秘书处：中国电子技术标准化研究院；
 - 组 成：由30多个部门和单位的49名领导和专家组成；共有工作组成员单位165家，其中企业120家；
 - 标 准：已发布国标 102项，正在制定中的125项
 - 联系人：罗锋盈 15901234287 luofy@cesi.ac.cn

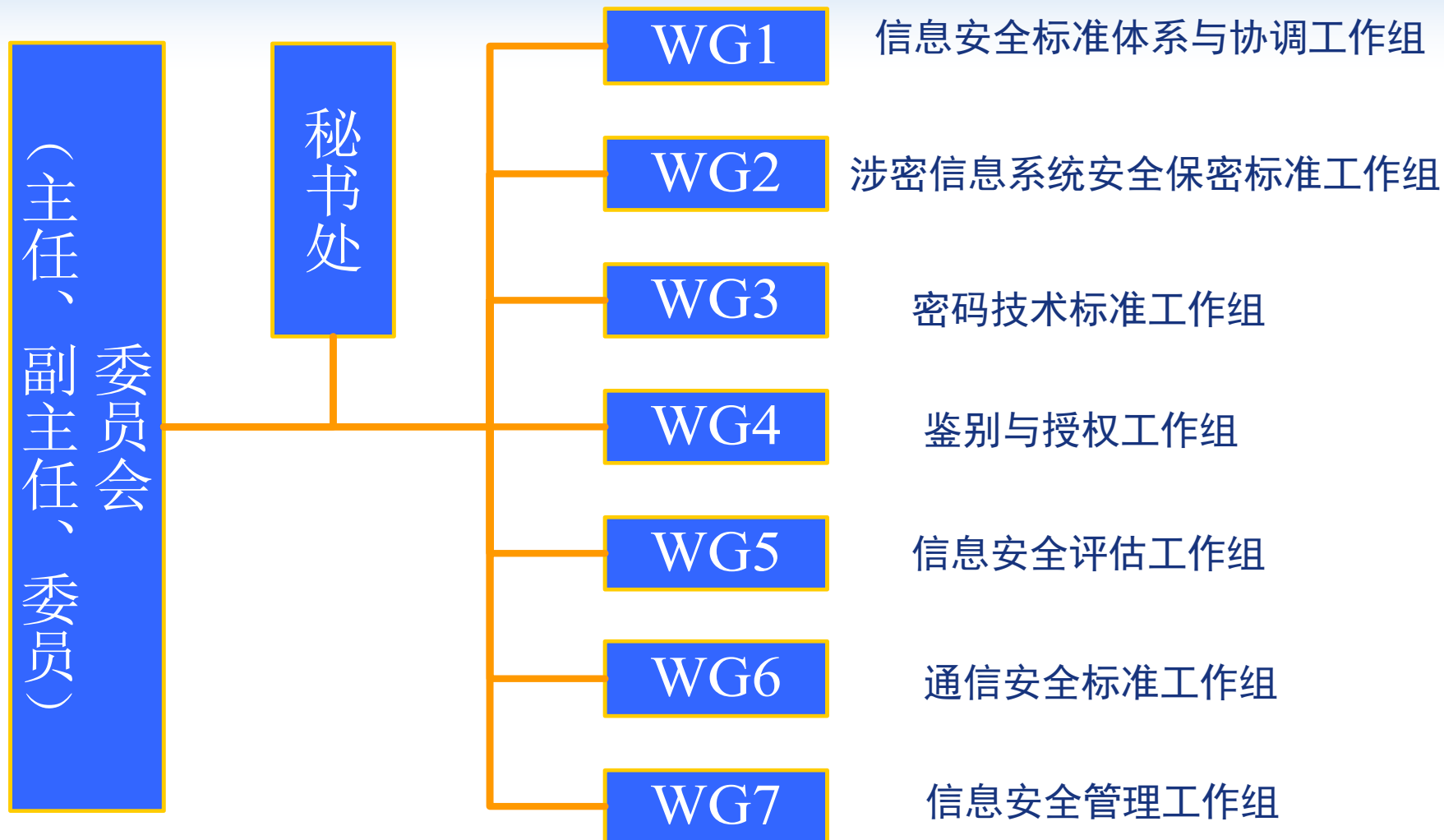
全国信息安全标准化技术委员会 (TC260)

“自2004年1月起，各有关部门在申报信息安全国家标准计划项目时，必须经信息安全标委会提出工作意见，协调一致后由信息安全标委会组织申报；在国家标准制定过程中，标准工作组或主要起草单位要与信息安全标委会积极合作，并由信息安全标委会完成国家标准送审、报批工作。”

(国标委高新函[2004]1号文)



TC260 组织结构图





国标制定情况

工作重点

信息安全等级保护
网络信任体系建设
信息安全应急处理
信息安全测评
信息安全管理
...

16个领域的标准制定

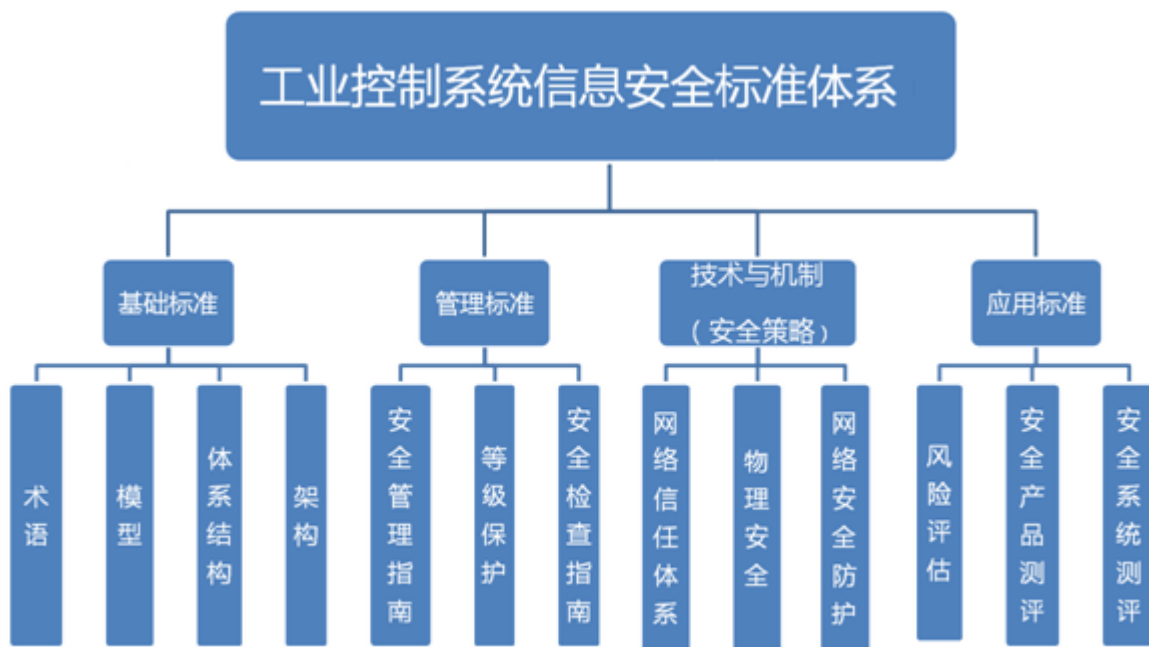
标准成果

提出227项国标计划
发布102项国家标准
在研125项

我国工业控制系统信息安全标准

全国信息安全标准化技术委员会 (TC260)

工控系统信息安全标准体系研究





我国工业控制系统信息安全标准

全国信息安全标准化技术委员会（TC260）

1) 在编标准：

《信息安全技术 SCADA系统安全控制指南》

《信息安全技术 安全可控信息系统（电力系统）安全指标体系》

2) 计划制定

《信息安全技术 工业控制系统安全管理基本要求》

《信息安全技术 工业控制系统安全检查指南》

《信息安全技术 工业控制系统测控终端安全要求》

《信息安全技术 工业控制系统安全防护技术要求和测评方法》

《信息安全技术 工业控制系统安全分级指南》

.....



全国电力系统管理及其信息交换标准化技术委员会 TC82

已发布标准

《电力系统管理及其信息交换 数据和通信安全 第1部分：通信网络和系统安全 安全问题介绍》（GB/Z 25320.1-2010）

《电力系统管理及其信息交换 数据和通信安全 第3部分：通信网络和系统安全 包括TCP/IP的协议集》（GB/Z 25320.3-2010）

《电力系统管理及其信息交换 数据和通信安全 第4部分：包含MMS的协议集》（GB/Z 25320.4-2010）

《电力系统管理及其信息交换 数据和通信安全 第6部分：IEC 61850的安全》（GB/Z 25320.6-2011）



全国工业过程测量和控制标准化技术委员会TC124

1) 在编标准

《工业控制计算机系统 通用规范 第2部分：工业控制计算机的安全要求》

2) 计划制定

《工业通信网络-网络和系统安全-第2-1部分：建立工业自动化和控制系统信息安全程序》，等同采用 IEC 62443-2-1:2010

《工业控制系统信息安全 第1部分：评估规范》

《工业控制系统信息安全 第2部分：验收规范》



全国电力监管标准化技术委员会（TC 296）

在编标准：

《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）

提纲



工业控制系统概述

国外工业控制系统信息安全标准

我国工业控制系统信息安全标准

相关政策法规

结论与展望

国家政府方面

2012年6月28日国务院《关于大力推进信息化发展和切实保障信息安全的若干意见（国发〔2012〕23号）》明确要求：保障工业控制系统安全。加强核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要领域工业控制系统，定期开展安全检查和风险评估。

重点对可能危及生命和公共财产安全的工业控制系统加强监管。对重点领域使用的关键产品开展安全测评，实行安全风险和漏洞通报制度。

国家政府方面

工业和信息化部2011年9月发布《关于加强工业控制系统信息安全管理的通知》（[2011]451号），通知明确了工业控制系统信息安全的组织领导、技术保障、规章制度等方面的要求。并在工业控制系统的连接、组网、配置、设备选择与升级、数据、应急管理等方面提出了明确的具体要求。

文中明确指出：“**全国信息安全标准化技术委员会抓紧制定工业控制系统关键设备信息安全规范和技术标准，明确设备安全技术要求。**”

行业方面

电力行业已陆续发布《电力二次系统安全防护规定》、《电力二次系统安全防护总体要求》等一系列文件。

交通铁路系统也发布了TB10117—98《铁路电力牵引供电远动系统技术规范》，TB10064—2002《电力系统综合设计》和《铁路供电水电调度规则》、《关于强化铁路牵引供电和电力远动系统若干要求》等文件。



结论与展望

小结

工业控制系统是国家重要基础设施（如电力、交通、能源、通信、水利、金融等）的“大脑”和“中枢神经”，是基础的基础、核心的核心。

从总体上看，我国工控系统信息安全防护体系建设明显滞后于工控系统建设，在防护意识、防护策略、防护机制、法规标准、防护检测等方面都存在不少问题，涉及工控系统的信息安全工作尚在起步阶段。

我国工业控制系统信息安全标准尚不健全，尚在发展初期。



结论与展望

下一步工作安排

分析工业控制系统信息安全保障体系建设需求，基于国家信息安全标准体系框架，建立工业控制系统信息安全标准体系总体框架。

在标准体系框架内梳理现有信息安全标准在工业控制系统建设中的应用关系，确定工业控制系统信息安全标准体系中强制使用和推荐使用的标准目录。

开展重点标准的研制规划，逐步丰富完善标准体系。



感谢您的聆听！

