



工控安全标准解读与标准评估



科学、公正、诚信、服务

工业和信息化部电子工业标准化研究院
全国信息安全标准化技术委员会秘书处
2016年11月2日

目 录

- 1. 《工业控制系统安全控制应用指南》解读**
- 2. 工业控制系统关键标准评估**

目 录

- 1. 《工业控制系统安全控制应用指南》解读**
- 2. 工业控制系统关键标准评估**

一、工业控制系统安全控制应用指南



➤ 标准发布背景

✓2016年8月29日，全国信息安全标准化技术委员会归口的《信息安全技术 工业控制系统安全控制应用指南》、《信息安全技术 信息技术产品供应方行为安全准则》、《信息技术 安全技术 信息安全控制实践指南》等24项国家标准正式发布。

✓该标准将于2017年3月1日正式实施，可指导工业控制系统建设、运行、使用、管理等相关方开展工业控制系统安全的规划和落地，也可供工业控制系统安全测评与安全检查工作作为参考依据

✓2016年9月，在北京工业控制系统信息安全峰会上，部分解读了该标准的主要内容。



一、工业控制系统安全控制应用指南



➤ 目录

A decorative graphic on the left side of the page features a central large orange circle with the text '目录' (Table of Contents) and 'CONTENTS' below it. Surrounding this central circle are several smaller circles in various colors: purple, green, red, yellow, blue, and brown.

目录

CONTENTS

1

前言与引言

2

范围、规范性引用文件、
术语和定义、缩略语

3

安全控制概述、基线及其设计、
选择与规约、选择过程应用

4

工业控制系统面临的安全风险

5

工业控制系统安全控制列表

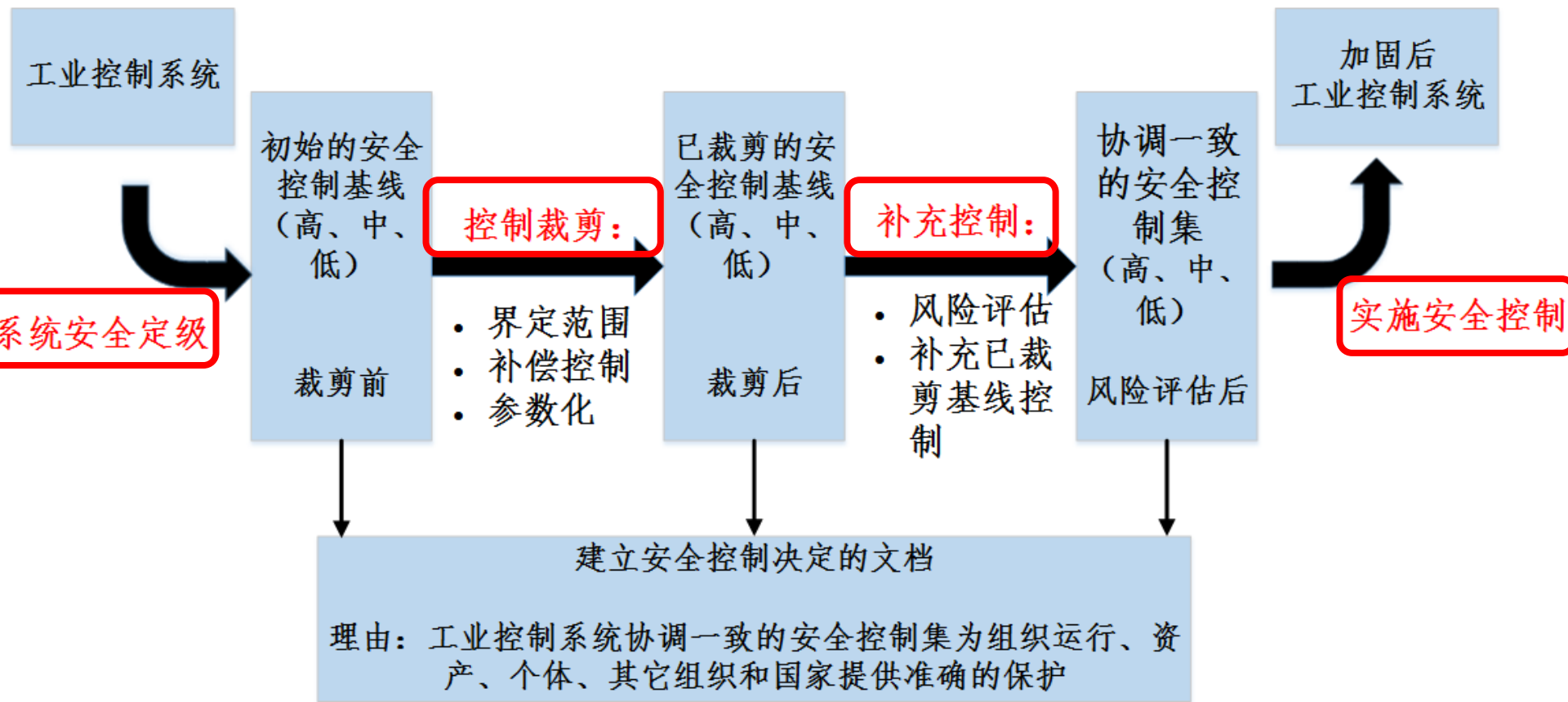
6

工业控制系统安全控制基线

一、工业控制系统安全控制应用指南



➤ 安全控制选择与规约



- 针对工业控制系统存在的脆弱性，分析面临的威胁，评估风险发生的可能性以及风险发生可能造成的影响和危害，制定风险处置原则和处置计划，**将工业控制系统安全风险控制在可接受的水平。**

一、工业控制系统安全控制应用指南



➤ 附录B 工业控制系统安全控制

技术

包含4个族，58个安全控制项
涉及访问控制、系统和通讯
保护、标识和鉴别

管理

包含5个族，42安全控制项
涉及安全评估与授权、规划、
系统和服务获取等



运维

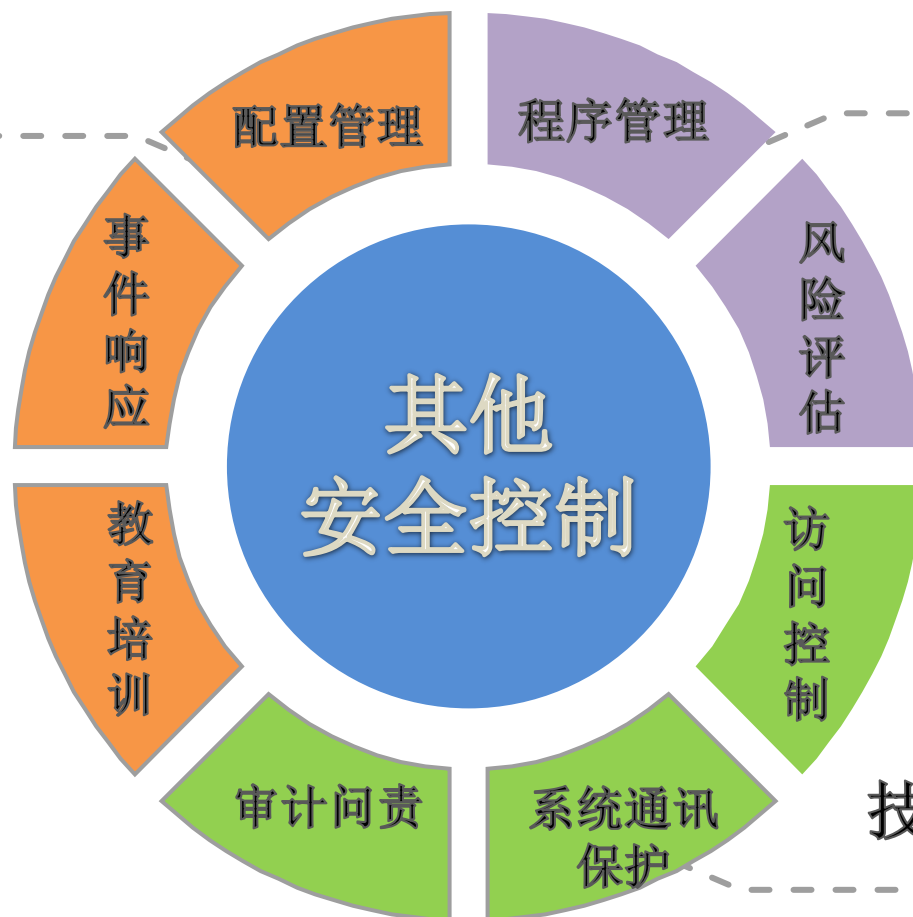
包含9个族，86个安全控制项
涉及人员安全、介质保护、事件响应、
应急计划等。

一、工业控制系统安全控制应用指南



运 维

管 理



一、工业控制系统安全控制应用指南



B.3风险评估

策略与规程

需结合组织自身实际情况，制定风险评估策略与规程，定期评审更新

风险评估

组织应定期开展风险评估，评审评估结果，并在需要时对风险评估进行调整

安全分类

依据相关规定，对ICS进行分类，并对结果进行审核确认

脆弱性扫描

定期对系统和主机进行脆弱性扫描，分析扫描结果，依据风险评估，修补脆弱性。

一、工业控制系统安全控制应用指南



B.4 系统与服务获取

相关政策



- ☐ 系统与服务获取策略和规程
- ☐ 资源分配
- ☐ 安全工程原则

相关系统获取



- ☐ 生存周期支持
- ☐ 系统文档
- ☐ 用户安装软件
- ☐ 软件使用限制
- ☐ 可信赖性
- ☐ 关键系统部件

相关服务获取



- ☐ 服务获取
- ☐ 外部系统服务
- ☐ 供应链保护

一、工业控制系统安全控制应用指南



B.8 应急计划(CP)



测试和演练工
业控制系统的
应急计划

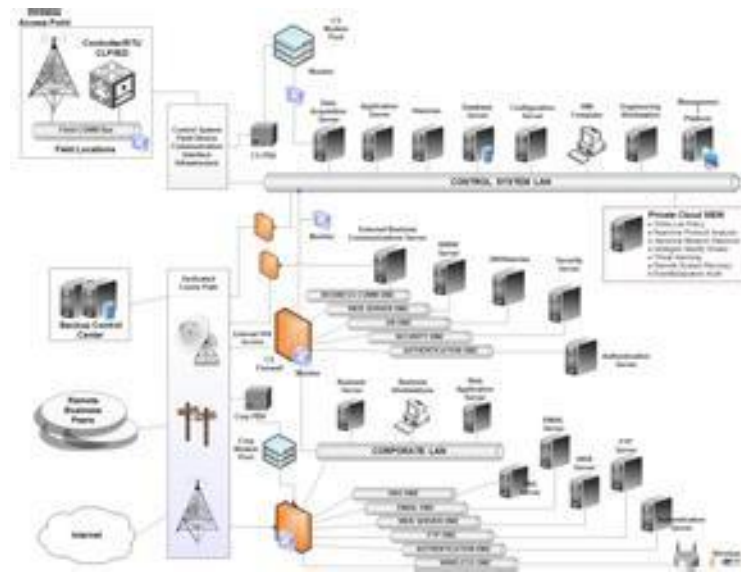


制定应急培训计划，
并对相关人员进行
培训



制定并发布ICS
应急计划和ICS
灾难恢复计划

制定并发布正
式的应急策略



一、工业控制系统安全控制应用指南



B.9 配置管理(CM)

配置管理策略和规程

- 制定并发布正式的配置管理策略和规程
- 定时对配置管理方针策略及规程进行评审和更新

配置管理计划

- 开发ICS的配置管理计划，建立相应的文档并实现该计划

基线配置

- 制定并维护ICS当前的配置基线
- 定时或在系统发生重大变更后，对基线配置进行评审和更新
- 保留旧版本ICS基线配置，以便必要时恢复配置

配置监控

- 实施工业控制系统中所使用产品的配置
- 评估ICS组件与已设配置存在的偏差
- 监控配置设置项的变更
- 对配置设置进行集中管理、应用和验证
- 对被检测事件的追踪、监视、纠正

一、工业控制系统安全控制应用指南



➤ B.13 事件响应(IR)

事件响
应策略
和章程

- 建立并有效实施事件响应策略与规程

事件响
应培训

- 信息系统变更时或按照一定的频率向人员或角色提供应急响应培训

事件响
应与演
练

- 按定义时间进行测试确保应急响应计划的有效性并确定该计划潜在的弱点
- 对演练进行记录

事件响
应支持

- 提供信息帮助台、援助团体、并在需要时获得证据方面的支持服务

事件响应
计划

- 制定、审批事件响应计划
- 按一定时间间隔或系统变更更新计划
- 保证计划的受控性

一、工业控制系统安全控制应用指南



➤ B.14 教育培训(AT)

教育培训策略和规程

- 规定了人员的安全教育培训

安全意识培训

- 培训人员包括管理员、ICS操作员、高级管理层、承包商
- 内容主要为信息安全方面安全事件处理技术如攻击防御、威胁识别

基于角色的安全培训

- 安排在ICS授权、新用户培训和按一定时间进行
- 根据个人的安全角色和安全责任进行培训，内容包括ICS特定安全方针策略，安全操作程序，ICS安全趋势和安全漏洞

安全培训记录

- 对安全培训记录，按规定时限保存记录

B.16 访问控制(AC)



一、工业控制系统安全控制应用指南



B.18 系统及通讯保护(SC)

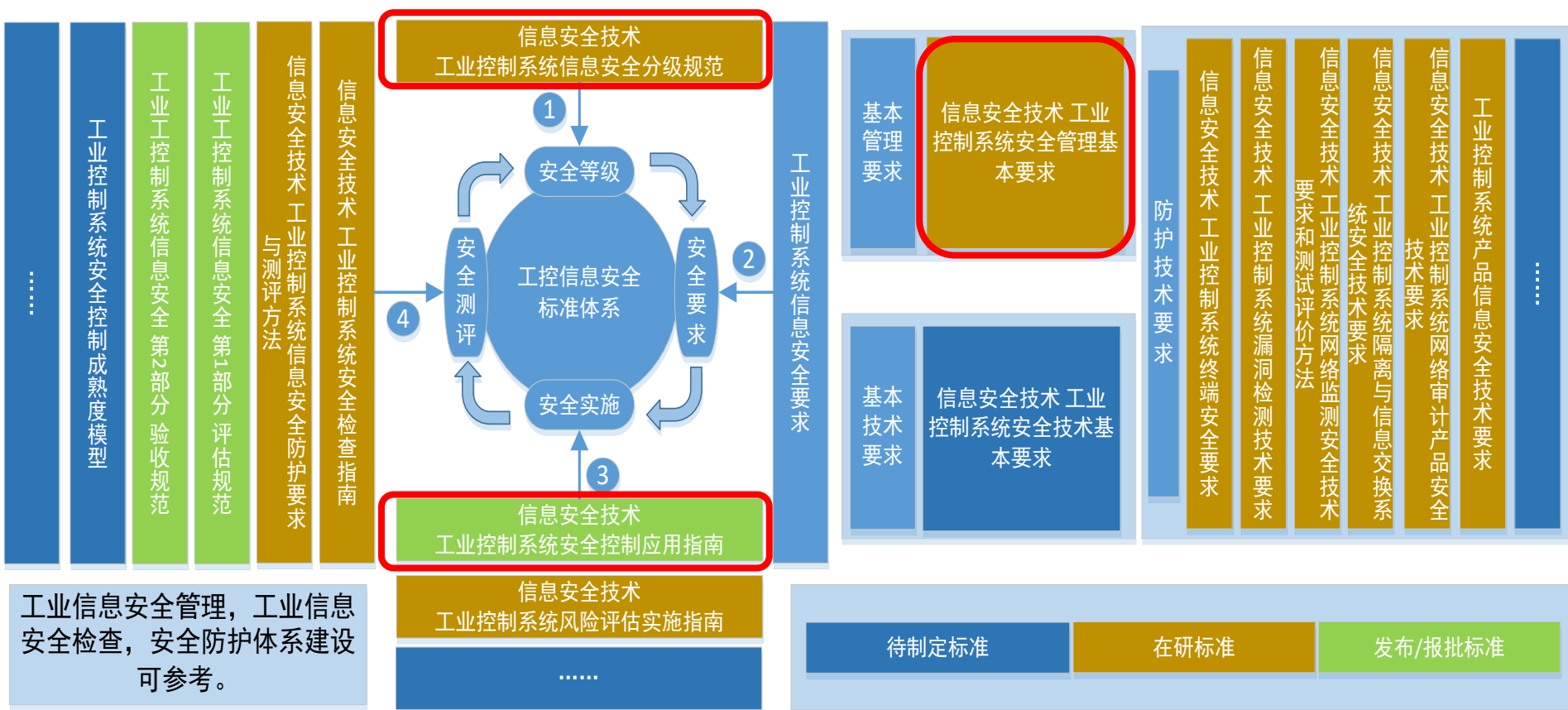


目 录

- 1. 《工业控制系统安全控制应用指南》解读**
- 2. 工业控制系统关键标准评估**

二、工业控制系统关键标准评估

➤ 工业控制系统信息安全标准体系



二、工业控制系统关键标准评估



➤ 工业控制系统信息安全标准符合性评估系统

- 《工业控制系统信息安全分级规范》
- 《工业控制系统信息安全管理基本要求》
- 《工业控制系统安全控制应用指南》 (GB/T32919-2016)



➤ 建立工业信息安全保障体系

- **安全管理：** 包括企业制度建立及落实、人员安全管理、资产安全管理、供应链安全管理等方面。
- **安全技术：** 包括物理环境安全防护、信息安全防护、网络设备安全防护、安全设备安全防护、重要数据安全防护等方面。
- **安全服务/运维：** 包括业务连续性管理制度、信息安全事件应急预案、信息安全事件应急技术支撑、灾难备份恢复、重大信息安全事件处置等方面。
- **共计186项安全控制措施。**

➤ 标准实施应用工作服务单位：

- 台州第二发电厂
- 中车株洲电力机车有限公司
- 沈机昆明机床股份有限公司
- 太原钢铁集团

➤ 对企业工业信息安全保障体系开展标准符合性评估：

- **评估手段：** 标准符合性在线评估，现场证据核查、人员访谈、系统/设备安全检测；
- **评估内容：** 企业工业信息安全管理、安全技术防护、安全运维的标准符合性。
- **评估效果：** 提升了企业**漏洞发现、隐患防范和风险评估能力，有效抵御90%以上的攻击。**

二、工业控制系统关键标准评估



➤ 工业控制系统信息安全标准符合性评估系统

中国电子技术标准化研究院
China Electronics Standardization Institute


继续上一次任务


点击新建任务

最近3次任务：

任务名称	创建时间	上次开始时间	操作
冶金业工控系统安全评估	2016-10-24 20:46:17	2016-10-24 20:46:17	继续评估 删除
电厂工控系统安全评估	2016-10-21 10:09:56	2016-10-21 13:46:23	继续评估 删除

➤ 分任务管理安全评估项目

- **多用户：**以多用户方式开展评估业务，确保不同用户之前数据和业务的独立性。
- **多任务：**依据用户实际需要，针对同一用户多套工控系统开展评估任务，并对不同任务开展持续跟踪处理。
- **数据安全：**系统上线前开展全面的安全防护测试，确保用户数据安全。

➤ 三种评估模式

- **脆弱性评估：**依据工控系统设备信息和网络拓扑架构，智能分析、评测工控系统的脆弱性。
- **标准评估：**依据工控安全分级、基本要求和控制应用指南等标准，对工控系统进行标准符合性评估。
- **全面评估：**综合工控系统资产信息、网络拓扑信息，结合工控安全相关标准和文件，对工控系统开展全面评估。

中国电子技术标准化研究院
China Electronics Standardization Institute


脆弱性评估
Vulnerability Assessment
为生产企业了解企业内工业控制系统的漏洞情况，并提供漏洞信息的优先解决方案。
[开始脆弱性评估](#)


标准符合性评估
Standard Assessment
为生产企业快速进行工业控制系统的安全自查，并提供自查的安全评估报告。
[开始标准评估](#)

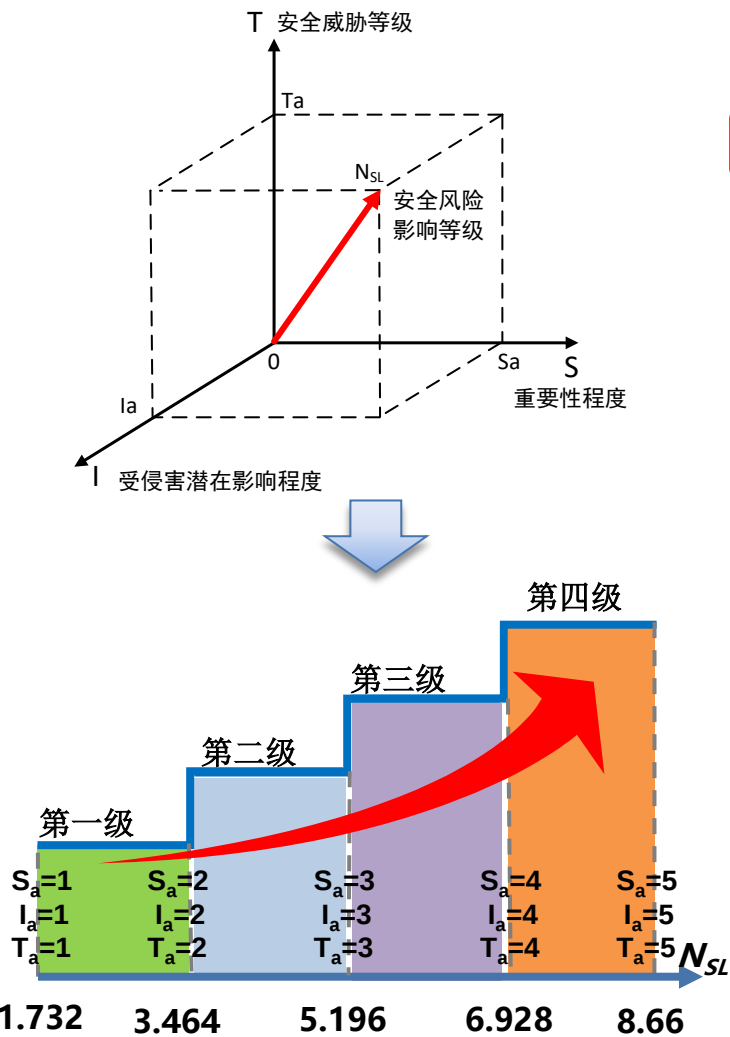

完整评估
Complete Assessment
为生产企业提供完善的工业控制系统安全评估和脆弱性评估，并提供安全评估和脆弱性评估报告。
[开始完整评估](#)

中国电子技术标准化研究院
China Electronics Standardization Institute

[Home](#) | [About Us](#) | [Services](#) | [Clients](#) | [Contacts](#)

二、工业控制系统关键标准评估

➤ 系统定级



定级对应表:

重要性程度 特征值	影响程度特 征值	信息安全威胁等级				
		1	2	3	4	5
1	1	第一级	第一级	第一级	第二级	第三级
1	2	第一级	第一级	第二级	第二级	第三级
1	3	第一级	第二级	第二级	第二级	第三级
1	4	第二级	第二级	第二级	第三级	第三级
1	5	第三级	第三级	第三级	第三级	第四级
2	1	第一级	第一级	第二级	第二级	第三级
2	2	第一级	第二级	第二级	第二级	第三级
2	3	第二级	第二级	第二级	第三级	第三级
2	4	第二级	第二级	第三级	第三级	第三级
2	5	第三级	第三级	第三级	第三级	第四级
3	1	第一级	第二级	第二级	第二级	第三级
3	2	第二级	第二级	第二级	第三级	第三级
3	3	第二级	第二级	第三级	第三级	第三级
3	4	第二级	第三级	第三级	第三级	第四级
3	5	第三级	第三级	第三级	第四级	第四级
4	1	第二级	第二级	第二级	第三级	第三级
4	2	第二级	第二级	第三级	第三级	第三级
4	3	第二级	第三级	第三级	第三级	第四级
4	4	第三级	第三级	第三级	第四级	第四级
4	5	第三级	第三级	第四级	第四级	第四级
5	1	第三级	第三级	第三级	第三级	第四级
5	2	第三级	第三级	第三级	第三级	第四级
5	3	第三级	第三级	第三级	第四级	第四级
5	4	第三级	第三级	第四级	第四级	第四级
5	5	第四级	第四级	第四级	第四级	第四级

二、工业控制系统关键标准评估



➤ 工业控制系统信息安全标准符合性评估系统

明确目标资产，梳理评估对象

拓扑管理

资产管理

报告管理

企业中心

公告栏

➤ 资产管理

全区域

中国

河南

北京

上海

浙江

辽宁

区域管理

中国

新增区域设备

修改删除	资产IP	资产名	资产厂商	资产系列名	资产区域	资产重要性
☐	sahfk	路由器	紫金桥	Realinfo	中国	非常重要
☐	192.168.1.3	HMI	施耐德	ETG3000 FactoryCast HMI	河南	非常重要
☐	192.168.2.7	MES	浙大中控	控制软件	河南	非常重要
☐	192.168.3.3	SCADA	国电智深	EDPF-SCADA	河南	非常重要
☐	192.168.5.77	DCS	honeywell	Experion PKS	河南	非常重要
☐	192.168.4.5	SCADA	亚控	Kingview	北京	非常重要
☐	192.168.8.123	DCS	honeywell	Experion PKS	北京	非常重要
☐	192.168.5.33	PLC	施耐德	Modicon M340	北京	非常重要
☐	192.145.3.44	工业交换机	Qualys Security	Magnum MNS-6K	北京	非常重要
☐	192.178.3.2	HMI	施耐德	ETG3000 FactoryCast HMI	北京	非常重要
☐	192.168.4.23	MES	浙大中控	控制软件	北京	非常重要
☐	192.168.7.45	远程IO模块	MOXA	ioLogik Series	北京	非常重要
☐	192.168.9.156	仪器仪表	横河	HART Device DTM	北京	非常重要
☐	192.168.113.45	工业网关	Sierra Wireless	AirLink Raven X EV-DO	北京	非常重要
☐	10.1.34.55	RTU	施耐德	Telvent	北京	非常重要
☐	10.1.3.55	工业安全路由器	MOXA	EDR Series	北京	非常重要
☐	192.168.56.44	杀毒软件	ClamAV	系统杀毒软件	北京	非常重要
☐	192.168.1.123	无线路由器	Tropos Networks	Mesh OS	北京	非常重要

➤ 总览

当前区域：中国

设备数量：21

负责人：XX

重要性：非常重要

区域评估定级-中国

二、工业控制系统关键标准评估

➤ 工业控制系统信息安全标准符合性评估系统

中国电子技术标准化研究院
China Electronics Standardization Institute

国际选择

标准一：《工业控制系统信息安全分级规范》	☒
标准二：《工业控制系统信息安全管理基本要求》	☒
标准三：《工业控制系统安全控制应用指南》	☒
标准四：《工业控制系统信息安全防护指南》	☒

安全定级

危险等级:	低	中	高	极高
定级方式:	快速定级	影响定级	国际定级	
保密性:	低	中	高	极高
完整性:	低	中	高	极高
可获得性:	低	中	高	极高

总览

当前类型: 评估类型: 标准评估

国标: 安全分级规范、管理基本要求、控制应用指南、安全防护指南

危险等级: 极高

中国电子技术标准化研究院
China Electronics Standardization Institute

国际选择

标准一：《工业控制系统信息安全分级规范》	☒
标准二：《工业控制系统信息安全管理基本要求》	☒
标准三：《工业控制系统安全控制应用指南》	☒
标准四：《工业控制系统信息安全防护指南》	☒

安全定级

危险等级:	低	中	高	极高
定级方式:	快速定级	影响定级	国际定级	
死亡人数:	<input type="range"/>			34 人
重伤个数:	<input type="range"/>			329 人
直接经济损失:	<input type="range"/>			48446 万元

信息安全威胁程度

物理破坏

拒绝服务

欺骗与假冒

回放攻击

数据库注入

通信攻击等

资产价值

业务使命

行业领域

资产重要程度

受侵害的对象

受侵害的程度

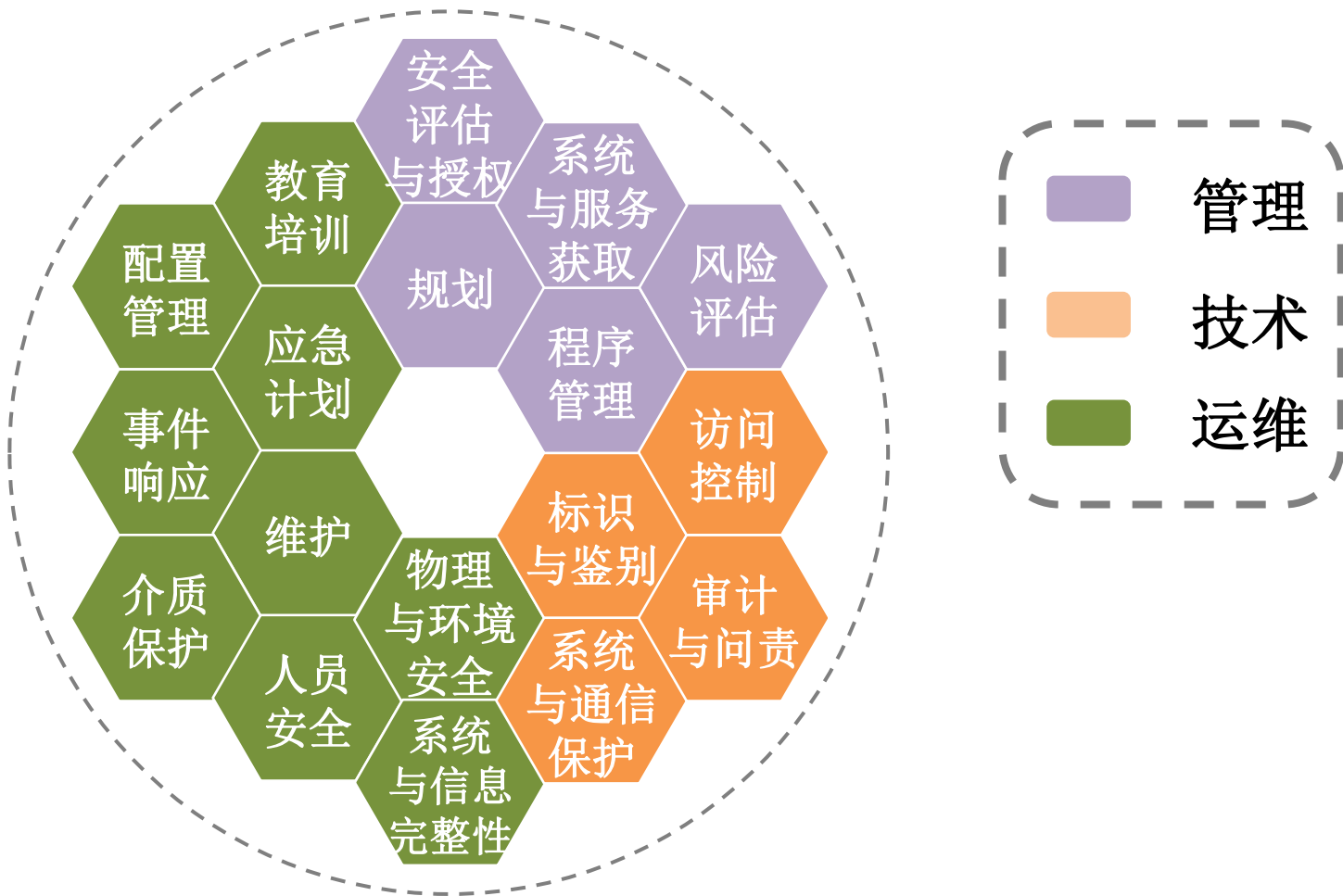
工业生产运行安全

潜在影响程度

有效指导企业对工控系统资产进行快速定级，为后续提出安全要求，实施安全控制措施提供基础。

二、工业控制系统关键标准评估

➤ 附录B 工业控制系统安全控制



本标准从**管理、运维、技术**三个维度提出了**18个族**，**186项**安全控制措施，范围涵盖访问控制、安全评估、系统与服务获取、风险评估、运维等。

二、工业控制系统关键标准评估



➤ 工业控制系统信息安全标准符合性评估系统

拓扑管理

资产管理

安全定级

问卷调查

报告管理

企业中心

公告栏

问题分类

所有标准

教育培训

审计与问表

安全评估与授权

配置管理

应急计划

标识与鉴别

事件响应

维护

介质保护

物理与环境安全

是 ☐ 否 ☐ 未回答 ☐

不适用 ☐ 不涉及 ☐

已标记 ☐ 未标记 ☐

完成率：

19.02%

配置管理

3. 系统目前是否已经有一个完善的、可备份的、用于维护系统的配置基线？

☐ 是 ☐ 否 ☐ 不适用 ☐ 不涉及

4. 在系统发生重大变更后，对基线配置是否进行评审和更新？

☐ 是 ☐ 否 ☐ 不适用 ☐ 不涉及

5. 旧版本基线配置是否保留，以便必要时恢复配置？

☐ 是 ☐ 否 ☐ 不适用 ☐ 不涉及

6. 是否采用自动化机制用于维护一个最新的、完整的、准确的、并就绪可用的基线配置？

☐ 是 ☐ 否 ☐ 不适用 ☐ 不涉及

7. 是否为开发和测试环境配置一条基线，该基线与操作基线实质分离，单独维护和管理？

查看分析结果

问题描述

备注

详情

控制：

- a) 应制定并维护ICS当前的配置基线；
- b) 应按【赋值：组织定义的时间间隔】或在系统发生重大变更后，对基线配置进行评审和更新；
- c) 应保留旧版本ICS基线配置，以便必要时恢复配置。

补充指导：

- a) 应为ICS及与ICS通讯和连接的部件，建立了一个基线配置；
- b) 该基线配置提供了有关ICS的信息，如：为工作台、服务器、网络部件或移动设备所装载的标准软件；提供了有关网络拓扑以及系统体系结构中的逻辑地点等信息；
- c) 该基线配置是对所构造ICS的最近的规格说明；
- d) 维护该基线配置，涉及当该ICS改变时，及时创建新的基线；
- e) ICS的基线配置与组织的业务体系结构是一致的。
- f) 相关安全控制：CM-3、CM-6、CM-8。

针对18个族，186个安全控制项，设计1000余个问题，帮助企业开展安全控制措施的符合性评估。

二、工业控制系统关键标准评估



➤ 工业控制系统信息安全标准符合性评估系统

中国电子技术标准化研究院
China Electronics Standardization Institute

Q OK 退出

拓扑管理

资产管理

安全定级

问卷调查

报告管理

企业中心

公告栏

报告管理

综合分析结果

安全评估报告

风险评估报告

导出报告

标准评估

脆弱性评估

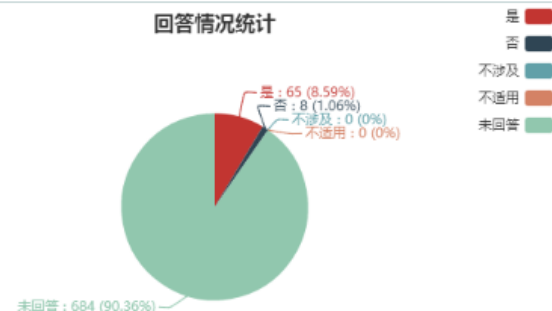
完整评估

标准符合度



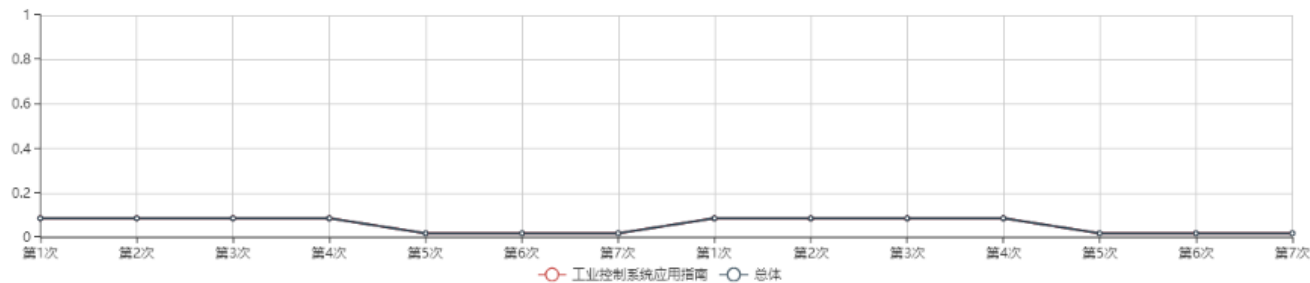
标准符合度

回答情况统计



问题回答统计

标准符合度趋势



标准符合度趋势图

标准协议集符合概况图

下一步设想

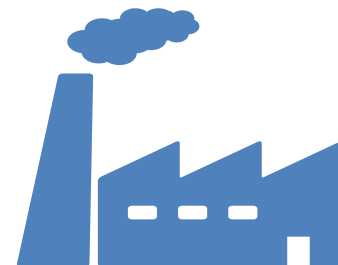


1. 开展工控安全体系标准评估：

- 根据《信息安全技术 工业控制系统安全控制应用指南》（GB/T 32919-2016）国家标准，开展标准评估工作，帮助企业做好工控安全管理和技术防护体系建设。

2. 开展工控安全防护体系建设：

- 根据工信部等行业主管部门相关政策文件，开展针对文件的评估工作，及时发现安全隐患，形成工控安全有效解决方案，指导企业提高工控安全保障水平。



谢谢!

