



# 工业控制系统 信息安全防护能力评估介绍



科学、公正、诚信、介绍

中国电子技术标准化研究院**CESI**  
工业控制系统安全标准与测评**MIIT**重点实验室  
工业控制系统信息安全产业联盟秘书处**ICISIS**  
全国信息安全标准化技术委员会秘书处**SAC/TC260**

# 目 录

**1. 必要性**

**2. ICS安全防护能力评估**

**3. 合作**

# 必要性



## 工业4.0、工业互联网、中国制造2025

云、大数据、物联网等新技术、新应用的使用

自成体系且封闭独立的系统

开放式

数据共享，  
数据流通。

信息安全形势更加严峻

IT系统信息安全基本特征

工控系统信息安全基本特征

保密性—完整性—可用性

可用性—完整性—保密性

新的信息  
安全需求



## 两化深度融合 智能制造 互联网+制造业

➤ 为切实做好工业信息安全保障工作，主管部门发布系列政策文件和法规：

- 《关于加强工业控制系统信息安全管理的通知》（工信部协〔2011〕451号）；
- 《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）
- 《关于开展2015年智能制造试点示范专项行动的通知》（工信部装〔2015〕72号）；
- 《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号）；
- 《关于加强国家网络安全标准化工作的若干意见》（中网办发文〔2016〕5号）；
- 《中华人民共和国网络安全法》（2016.11）
- 《工业控制系统信息安全防护指南》（工信软函[2016]338号）

● 2016年5月26日，在第20届中国国际软件博览会上，苗部长指出：“要提高工业信息系统安全水平。制定实施工业控制系统信息安全防护指南，完善标准体系”。

- 从国内外形势和产业发展看出，工业信息安全防护工作极端重要。
- 标准作为政策规划落实的重要抓手，为工业信息安全防护工作提供重要支撑。
- 测评是标准落地的有效手段，提升工业企业安全防护能力，提高工业行业整体信息安全保障水平。

# 必要性

## 工控安全保障体系建设

安全技术体系

安全管理体系!

安全产品

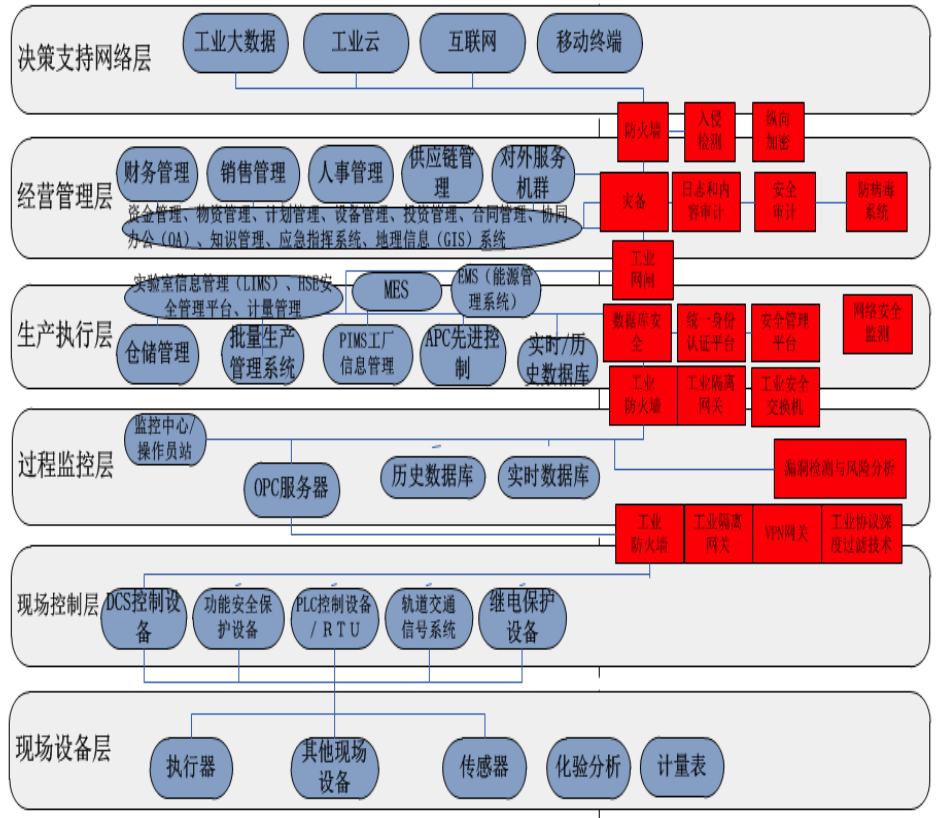
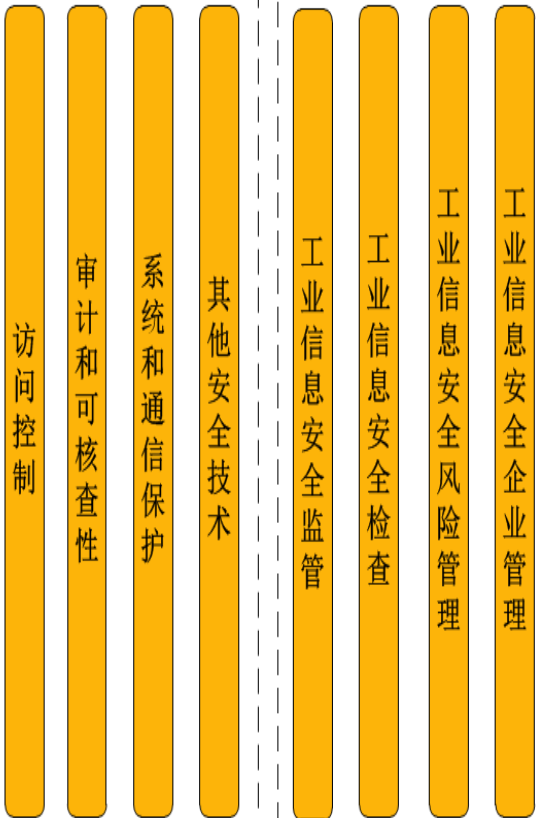
安全运维体系

工业信息安全技术

工业信息安全管理

工业信息安全技术产品

工业信息安全服务



重点领域

- 石化
- 汽车
- 轨道交通
- 船舶
- 冶金
- 电力
- 市政
- 水利
- 烟草
- 智能制造
- 食品
- 医疗
- 煤炭
- 军工
- 核电
- 纺织
- 新能源
- 其他

# 目 录

**1. 必要性**

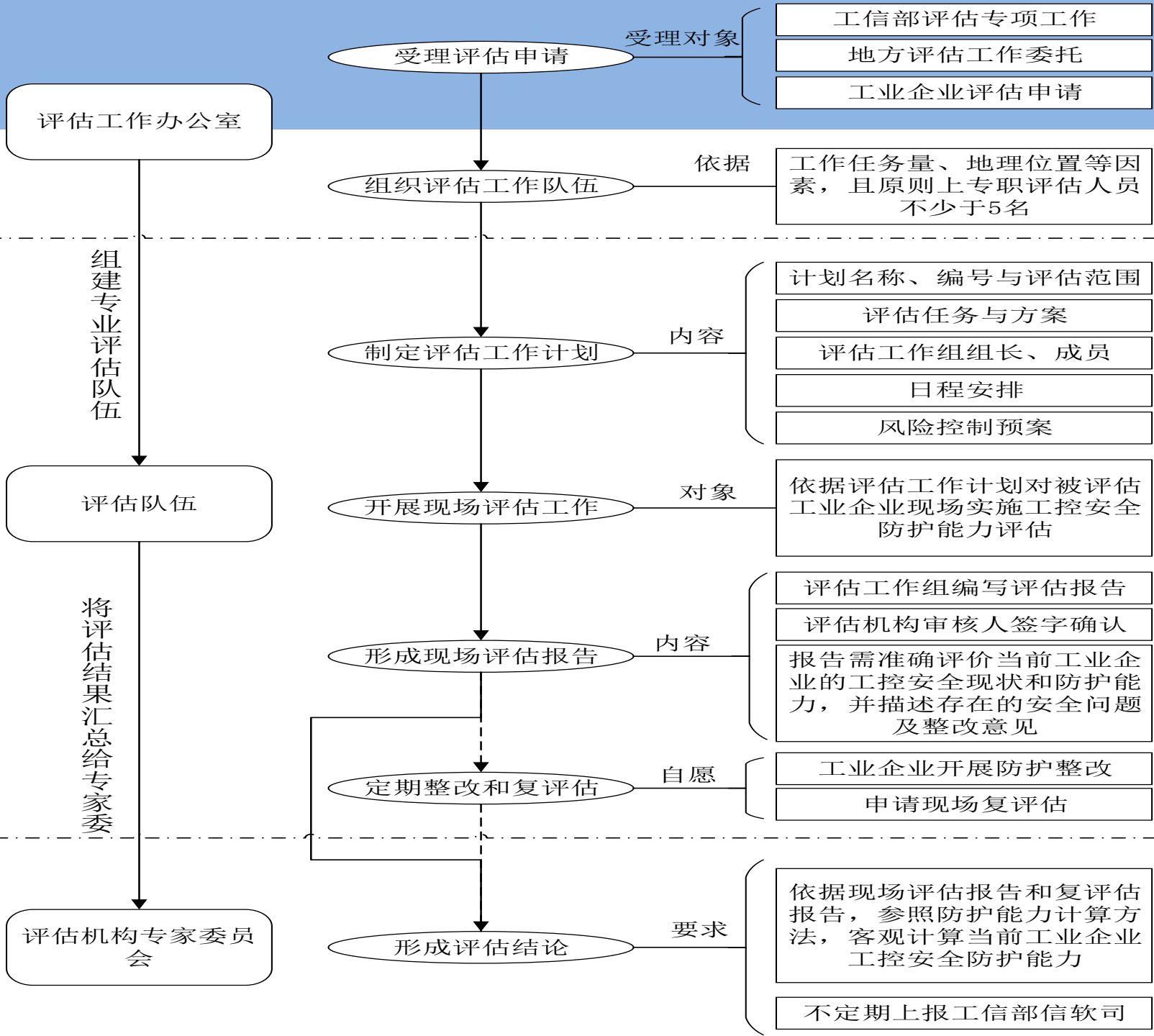
**2. ICS安全防护能力评估介绍**

**3. 合作**



## ➤ 评估工作流程

工业控制系统信息安全防护能力评估工作程序如图1所示。主要包括受理评估申请、组建评估工作队伍、制定评估工作计划、开展现场评估工作、形成现场评估报告和形成评估结论六个部分，并且工业企业可自愿依据现场评估报告开展工控安全防护整改后申请现场复评估。

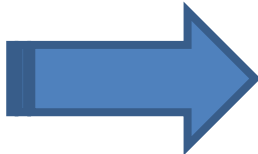




## ➤ 现场评估工作内容

### ✓ 1 安全软件选择与管理防护评估

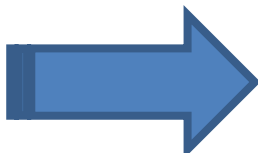
在工业主机上采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件，只允许经过工业企业自身授权和安全评估的软件运行。



a) 工业企业应在工业主机上安装防病毒软件或应用程序白名单软件，确保有效防护病毒、木马等恶意软件及未授权应用程序和介绍；

b) 工业企业工业主机上安装防病毒软件或应用程序白名单软件，应在离线环境中充分验证测试，确保其不会对工业控制系统的正常运行造成影响。

建立防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采取病毒查杀等安全预防措施。



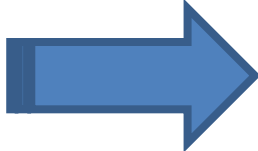
a) 工业企业应建立防病毒和恶意软件入侵管理机制，确保该管理机制可有效规范防病毒和恶意软件入侵管理工作；

b) 工业企业应定期针对工业控制系统及临时接入的设备开展查杀，并做详细查杀记录。

## ➤ 现场评估工作内容

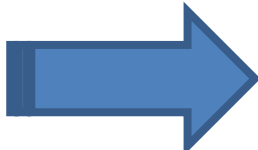
### ✓ 2 配置和补丁升级防护评估

做好工业控制网络、工业主机和工业控制设备的安全配置，建立工业控制系统配置清单，定期进行配置审计。



- a) 工业企业应做好工业控制网络、工业主机和工业控制设备的安全配置，确保工业控制系统相关安全配置的有效性；
- b) 工业企业应建立工业控制系统配置清单，确保该清单满足企业工业控制系统安全可靠运行的需要；
- c) 工业企业应定期对工业控制系统配置进行核查审计，确保系统实际配置与配置清单的一致性。

对重大配置变更制定变更计划并进行影响分析，配置变更实施前进行严格安全测试。

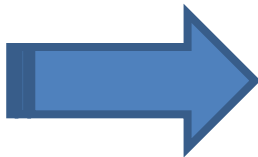


- a) 工业企业应在发生重大配置变更时，制定配置变更计划，进行影响分析，确保该重大配置变更不会引入重大安全风险；
- b) 工业企业应在配置变更实施前进行严格安全测试，必要时应在离线环境中进行安全验证，以确保配置变更不会影响工业控制系统正常运行。

## ➤ 现场评估工作内容

### ✓ 2 配置和补丁升级防护评估

**密切关注重大工控安全漏洞及其补丁发布，及时采取补丁升级措施。在补丁安装前，需对补丁进行严格的安全评估和测试验证。**

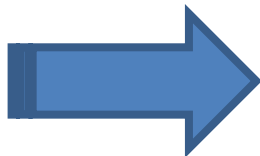


- a) 工业企业应密切关注重大工控安全漏洞及补丁发布，并一定时间内（原则上不超过**180**天）及时开展补丁升级，确保工业控制系统及时针对已知安全漏洞采取安全防护措施；
- b) 工业企业应在补丁安装前，针对补丁进行安全评估测试，必要时进行离线评估，确保补丁安装后工业控制系统的正常运行。

## ➤ 现场评估工作内容

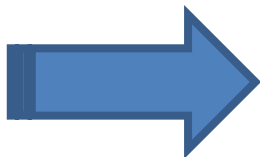
### ✓ 3 边界安全防护评估

分离工业控制系统的开发、测试和生产环境。



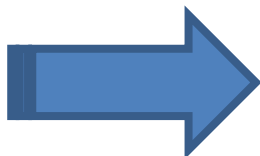
a) 工业企业应针对工业控制系统的开发、测试和生产分别提供独立环境，避免开发、测试环境中的安全风险引入生产系统。

通过工业控制网络边界防护设备对工业控制网络与企业网或互联网之间的边界进行安全防护，禁止没有防护的工业控制网络与互联网连接。



a) 工业企业应在工业控制网络与企业网边界部署安全防护设备，以避免企业网的安全风险引入工业控制网络；  
b) 工业企业应禁止没有防护的工业控制网络与互联网连接，以确保互联网的安全风险不被引入工业控制网络。

通过工业防火墙、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护。

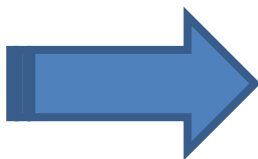


a) 工业企业应根据区域重要性和业务需求对工业控制系统网络进行安全区域划分，以确保安全风险的区域隔离；  
b) 工业企业应采用工业防火墙、网闸等防护设备，对工业控制网络安全区域实施逻辑隔离安全防护。

## ➤ 现场评估工作内容

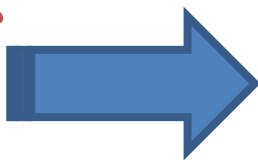
### ✓ 4 物理和环境安全防护评估

对重要工程师站、数据库、介绍器等核心工业控制软硬件所在区域采取访问控制、视频监控、专人值守等物理安全防护措施。



- a) 工业企业应基于重要工程师站、数据库、介绍器等核心工业控制软硬件明确重点物理安全防护区域；
- b) 工业企业应对重点物理安全防护区域采取物理隔离、访问控制、视频监控、专人值守等物理安全防护措施。

拆除或封闭工业主机上不必要的USB、光驱、无线等接口。若确需使用，通过主机外设安全管理技术手段实施严格访问控制。

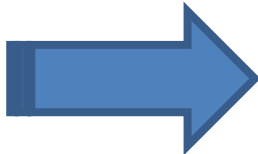


- a) 工业企业应拆除或封闭工业主机上不必要的**USB**、光驱、无线等接口，以防止病毒、木马、蠕虫等恶意代码入侵，并避免数据泄露；
- b) 在确需使用工业主机外设接口时，工业企业应建立主机外设接口管理制度，并通过主机外设安全管理技术手段实施访问控制，以避免未经授权的外设终端接入。

## ➤ 现场评估工作内容

### ✓ 5 身份认证防护评估

在工业主机登录、应用介绍资源访问、工业云平台访问等过程中使用身份认证管理。对于关键设备、系统和平台的访问采用多因素认证。



a) 工业企业应在工业主机登录、应用介绍资源访问、工业云平台访问等过程中使用身份认证管理技术（如口令密码、**USB-key**、智能卡、生物指纹、虹膜等），以确保访问过程安全可控；

b) 工业企业宜根据自身实际情况，明确关键设备、系统和平台，并在访问过程中，采用两种或两种以上因素认证方式，以避免非法登录等安全隐患。

合理分类设置账户权限，以最小特权原则分配账户权限。



a) 工业企业应根据不同业务需求、岗位职责等，合理分类设置账户；

b) 工业企业应以满足工作要求的最小特权原则来进行系统账户权限分配，降低因事故、错误、篡改等原因造成损失的可能性；

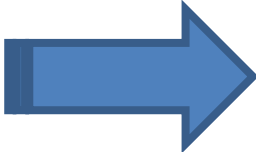
c) 工业企业需定期审计分配的账户权限是否超出工作需要，确保超出工作需要的账户权限及时调整。



## ➤ 现场评估工作内容

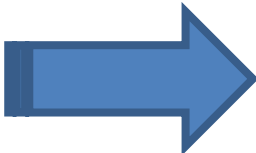
### ✓ 5 身份认证防护评估

强化工业控制设备、SCADA软件、工业通信设备等的登录账户及密码，避免使用默认口令或弱口令，定期更新口令。



- a) 工业企业应为工业控制设备、SCADA软件、工业通信设备等的登录账户设定足够强度的登录密码，采取措施避免使用默认口令或弱口令，并妥善管理，以降低对设备未授权登录和操作的可能性；
- b) 工业企业应定期更新口令。

加强对身份认证证书信息保护力度，禁止在不同系统和网络环境下共享。

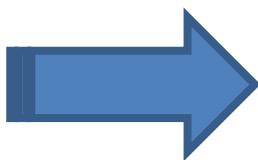


- a) 适用时，工业企业应确保其身份认证证书传输、存储的安全可靠，避免证书的未授权使用。

## ➤ 现场评估工作内容

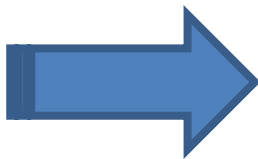
### ✓ 6 远程访问安全防护评估

原则上严格禁止工业控制系统面向互联网开通HTTP、FTP、Telnet等高风险通用网络介绍。



a) 适用时，工业企业应制定规章制度，原则上严格禁止工业控制系统面向互联网开通HTTP、FTP、Telnet等高风险通用网络介绍。

确需远程访问的，采用数据单向访问控制等策略进行安全加固，对访问时限进行控制，并采用加标锁定策略。

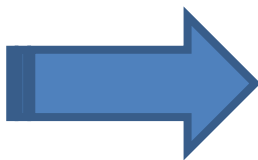


a) 工业企业应采用数据单向访问控制等策略对远程访问进行安全加固，确保数据传输安全，避免未授权操作；  
b) 工业企业应对远程访问进行时限控制，并采用加标锁定策略，确保组织对远程访问的可控性。

## ➤ 现场评估工作内容

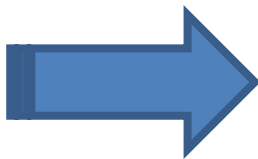
### ✓ 6 远程访问安全防护评估

**确需远程维护的，采用虚拟专用网络（VPN）等远程接入方式进行。**



- a) 适用时，工业企业应对远程维护采用虚拟专用网络（VPN）等远程接入方式，以确保远程维护安全可信；
- b) 工业企业应制定远程接入账户管理制度，规范账户申请、使用、收回等流程。

**保留工业控制系统的相关访问日志，并对操作过程进行安全审计。**

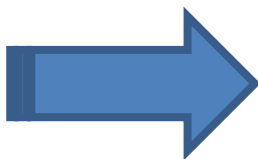


- a) 工业企业应保留工业控制系统相关访问日志（如人员账户、访问时间、操作内容等），并定期进行备份，以确保安全审计的有效开展；
- b) 工业企业制定审计制度，通过审计相关日志信息，及时发现异常访问行为。

## ➤ 现场评估工作内容

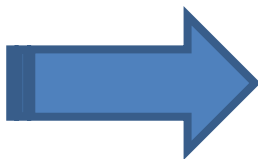
### ✓ 7 安全监测和应急预案演练防护评估

**在工业控制网络部署网络安全监测设备，及时发现、报告并处理网络攻击或异常行为。**



a) 工业企业应部署具备对工业控制系统与网络进行状态监测、日志采集与事件管理、流量采集与行为分析、异常告警及关联分析等功能的网络安全监测设备，及时发现、报告并处理包括设备状态异常、恶意软件传播、异常流量、异常诊断日志、端口扫描、暴力破解等网络攻击或异常行为。

**在重要工业控制设备前端部署具备工业协议深度包检测功能的防护设备，限制违法操作。**

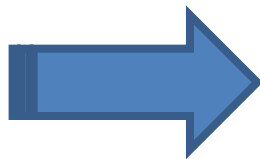


a) 工业企业应明确重要工业控制设备清单；  
b) 工业企业应在重要工业控制设备前端部署可对所使用的工业控制系统协议进行深度包分析和检测过滤的防护设备，具备检测或阻断不符合协议标准结构的数据包、不符合正常生产业务范围的数据内容等功能，限制违法操作。

## ➤ 现场评估工作内容

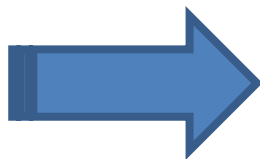
### ✓ 7 安全监测和应急预案演练防护评估

**制定工控安全事件应急响应预案，当遭受安全威胁导致工业控制系统出现异常或故障时，应立即采取紧急防护措施，防止事态扩大，并逐级报送直至属地省级工业和信息化主管部门，同时注意保护现场，以便进行调查取证。**



- a) 工业企业应制定工控安全事件应急响应预案，确保工业企业正确应对安全事件；
- b) 当工业企业工业控制系统因信息安全威胁出现异常或故障时，应按应急响应预案做好应急响应工作，采取紧急防护措施，防止事态扩大，并逐级报送直至属地省级工业和信息化主管部门，同时注意保护现场，以便进行调查取证。

**定期对工业控制系统的应急响应预案进行演练，必要时对应急响应预案进行修订。**

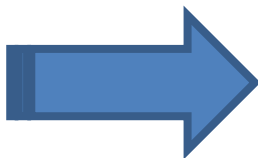


- a) 工业企业应定期组织工业控制系统相关人员开展应急响应预案演练，确保安全事件发生时应急预案被有效执行；
- b) 工业企业应根据实际情况对应急响应预案进行评审和修订，确保应急响应预案的适宜性。

## ➤ 现场评估工作内容

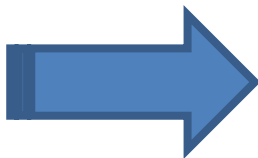
### ✓ 8 资产安全防护评估

**建设工业控制系统资产清单，明确资产责任人，以及资产使用及处置规则。**



- a) 工业企业应建立工业控制系统资产清单（包括软件资产、硬件资产、数据资产等），确保工业控制系统资产信息可核查、可追溯；
- b) 工业企业应明确资产责任人并建立资产使用处置规则，以在资产生命周期内对其进行适当管理。

**对关键主机设备、网络设备、控制组件等进行冗余配置。**



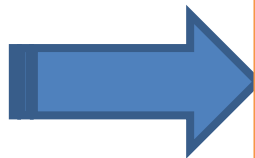
- a) 工业企业应根据业务需求，制定关键主机设备、网络设备、控制组件清单；
- b) 工业企业应针对关键主机设备、网络设备、控制组件等进行冗余配置，确保突发事件（如停电、设备损坏、网络攻击等）不会影响工业控制系统正常运行。



## ➤ 现场评估工作内容

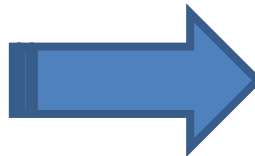
### ✓ 9 数据安全防护评估

对静态存储和动态传输过程中的重要工业数据进行保护，根据风险评估结果对数据信息进行分级分类管理。



- a) 工业企业应明确识别重要工业数据清单；
- b) 工业企业应对静态存储的重要工业数据进行加密存储或隔离保护，设置访问控制功能，确保静态存储的重要工业数据不被非法访问、删除、修改；
- c) 工业企业应对动态传输重要工业数据进行加密传输或使用VPN等方式进行保护，确保动态传输过程中重要工业数据的安全性；
- d) 工业企业应根据风险评估结果建立数据分级分类管理制度，确保工业数据的防护方式合理。

定期备份关键业务数据。

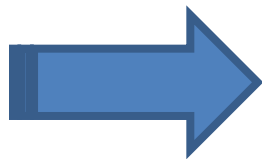


- a) 工业企业应建立关键业务数据清单；
- b) 工业企业应对关键业务数据进行定期备份，确保在工业控制系统关键业务数据丢失时可以及时恢复数据；
- c) 工业企业应定期对所备份的关键业务数据进行恢复测试，确保备份数据的可用性。

## ➤ 现场评估工作内容

### ✓ 9 数据安全防护评估

**对测试数据进行保护。**

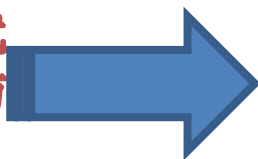


- a) 工业企业应对测试过程中产生的数据进行保护，以确保工业企业测试数据的安全；
- b) 工业企业应避免使用实际生产数据等敏感数据进行测试，在必要情况下，应提供去除所有敏感细节和内容的数据进行测试。

## ➤ 现场评估工作内容

### ✓ 10 供应链安全防护评估

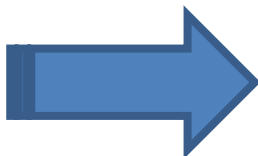
**在选择工业控制系统规划、设计、建设、运维或评估等介绍商时，优先考虑具备工控安全防护经验的企事业单位，以合同等方式明确介绍商应承担的信息安全责任和义务。**



a) 工业企业应以合同等方式明确工业控制系统产品和介绍提供商承担的信息安全责任和义务，确保提供的产品和介绍满足信息安全要求；

b) 工业企业在选择工业控制系统规划、设计、建设、运维或评估介绍商时，应优先考虑具备工控安全防护经验的企事业单位。

**以保密协议的方式要求介绍商做好保密工作，防范敏感信息外泄。**

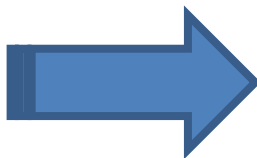


a) 工业企业应与介绍商签订保密协议，确保敏感信息不外泄。

## ➤ 现场评估工作内容

### ✓ 11 落实责任防护评估

**通过建立工控安全管理机制、成立信息安全协调小组等方式，明确工控安全管理责任人，落实工控安全责任制，部署工控安全防护措施。**



a) 工业企业应通过建立工业控制系统安全管理机制,确保工控安全管理工作有序开展;

b) 工业企业应成立由企业负责人牵头的,信息化、生产管理、设备管理等相关部门组成的工业控制系统信息安全协调小组,负责统筹协调工业控制系统信息安全相关工作;

c) 工业企业应在工业控制系统信息安全协调小组指导下,按照管理机制,明确工控安全管理责任人,落实工控安全责任制,部署工控安全防护措施。

# ICS安全防护能力评估介绍



## ➤ 工业控制系统信息安全防护能力评估系统（ICSEP）

- 《工业控制系统信息安全防护能力评估工作实施细则（试行）》
- 《工业控制系统信息安全防护指南》（工信软函[2016]338号）



### ➤ 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。
- **安全介绍/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。

### ➤ 标准实施应用工作介绍单位：

- 神华集团
- 国家电网公司

### ➤ 对企业工业信息安全保障体系开展防护能力评估：

- **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。**

# ICS安全防护能力评估介绍



## ➤ 工业控制系统信息安全防护能力评估系统

工业控制系统信息安全防护能力 评估工具

Q OK 退出

资产脆弱性评估

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

安全评估

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。

开始安全评估

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



# ICS安全防护能力评估介绍



## 工业控制系统信息安全防护能力评估系统

### 《工业控制系统信息安全防护能力评估工作实施细则（试行）》

明确目标资产，梳理评估对象



评估模式

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

### 资产管理

全区域

北京

海淀

昌平

上海

沈阳

大连

桂林

区域管理

北京

新增区域设备

资产IP	资产名	资产类型	资产厂商	资产系列名	资产区域	资产重要性	操作
1111	1111	PLC	schneider	Premium	北京	非常重要	修改
1111	2131	PLC	schneider	Premium	北京	非常重要	修改
192.1.1.1	111	PLC	schneider	Modicon M340	北京	非常重要	修改
192.1.1.1	11	PLC	siemens	S7-1200	海淀	非常重要	修改
192.1.1.111	111	PLC	siemens	S7-1500	海淀	非常重要	修改
192.1.1.11	1111	PLC	siemens	S7-1200	昌平	非常重要	修改

上海

新增区域设备

资产IP	资产名	资产类型	资产厂商	资产系列名	资产区域	资产重要性	操作
------	-----	------	------	-------	------	-------	----

沈阳

新增区域设备

资产IP	资产名	资产类型	资产厂商	资产系列名	资产区域	资产重要性	操作
------	-----	------	------	-------	------	-------	----

### 总览

当前区域：

设备数量：

负责人：

重要性：

区域评估定级

# ICS安全防护能力评估介绍



## 工业控制系统信息安全防护能力评估系统

### 《工业控制系统信息安全防护能力评估工作实施细则（试行）》

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

评估模式 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

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	<b>极高</b>
定级方式:	快速定级	影响定级	国际定级	
保密性:	低	中	<b>高</b>	极高
完整性:	低	中	高	<b>极高</b>
可获得性:	低	中	<b>高</b>	极高

总览

当前类型: 标准评估

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

开始测评

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

评估模式 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

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》

总览

当前类型: 标准评估

评估类型: 标准评估

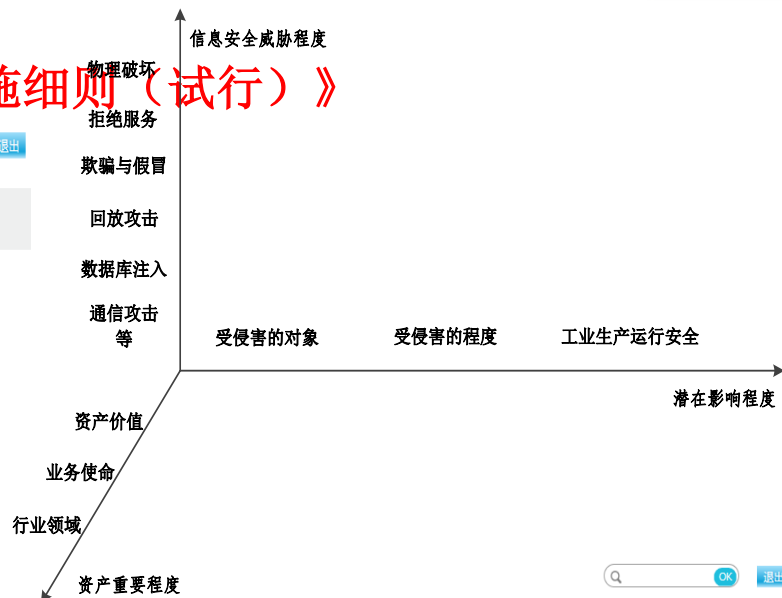
国标: 安全分级规范、管理基本要求、控制应用指南、安全防护指南

危险等级: 极高

开始测评

安全定级

危险等级:	低	中	高	<b>极高</b>
定级方式:	快速定级	<b>影响定级</b>	国际定级	
死亡人数:	[Slider]			34 人
里伤个数:	[Slider]			329 人
直接经济损失:	[Slider]			48446 万元



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。

# ICS安全防护能力评估介绍

## 工业控制系统信息安全防护能力评估系统

- ✓ 《工业控制系统信息安全防护指南》（工信软函[2016]338号）
- ✓ 《工业控制系统信息安全防护能力评估工作实施细则（试行）》

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

评估模式

安全定级

问卷调查

报告管理

### 问题分类

所有标准

所有标准

工业控制系统信息安全管理  
基本要求

访问控制

教育培训

审计与问责

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

是  否  未回答

不适用  不涉及

已标记  未标记

完成率： 0.00

### 访问控制

#### 策略和规程

1. 该组织有访问控制策略吗？
2. 该组织有访问控制程序吗？

#### 帐户管理

1. 系统帐户是通过帐户类型和管理识别吗？
2. 当静止在预期定义的时长或描述时，用户需要退出系统吗？

查看分析结果

### 问题描述

备注

详情

控制：

组织应制定并发布：

- a) 正式的访问控制策略，内容包括目的、范围、角色、责任、管理承诺、组织实体间的协调关系以及依从关系等；
- b) 正式的访问控制章程，以推动访问控制方针政策及与相关安全控制的实施；
- c) 应按【赋值：组织定义的时间间隔】，对访问控制策略及规程进行评审和更新。

补充指导：

- a) 访问控制策略和章程应与相关的法律、法规、规章、制度、策略及标准相一致；
- b) 访问控制策略可以包含在组织的通用信息安全策略中，也可为一般的安全程序或特殊ICS制定访问控制规程。

控制增强：无

OK

退出

### 问题描述

详情

该问题

ID:AC-1-1

问题进行备注  
备注信息

附件

文件名称

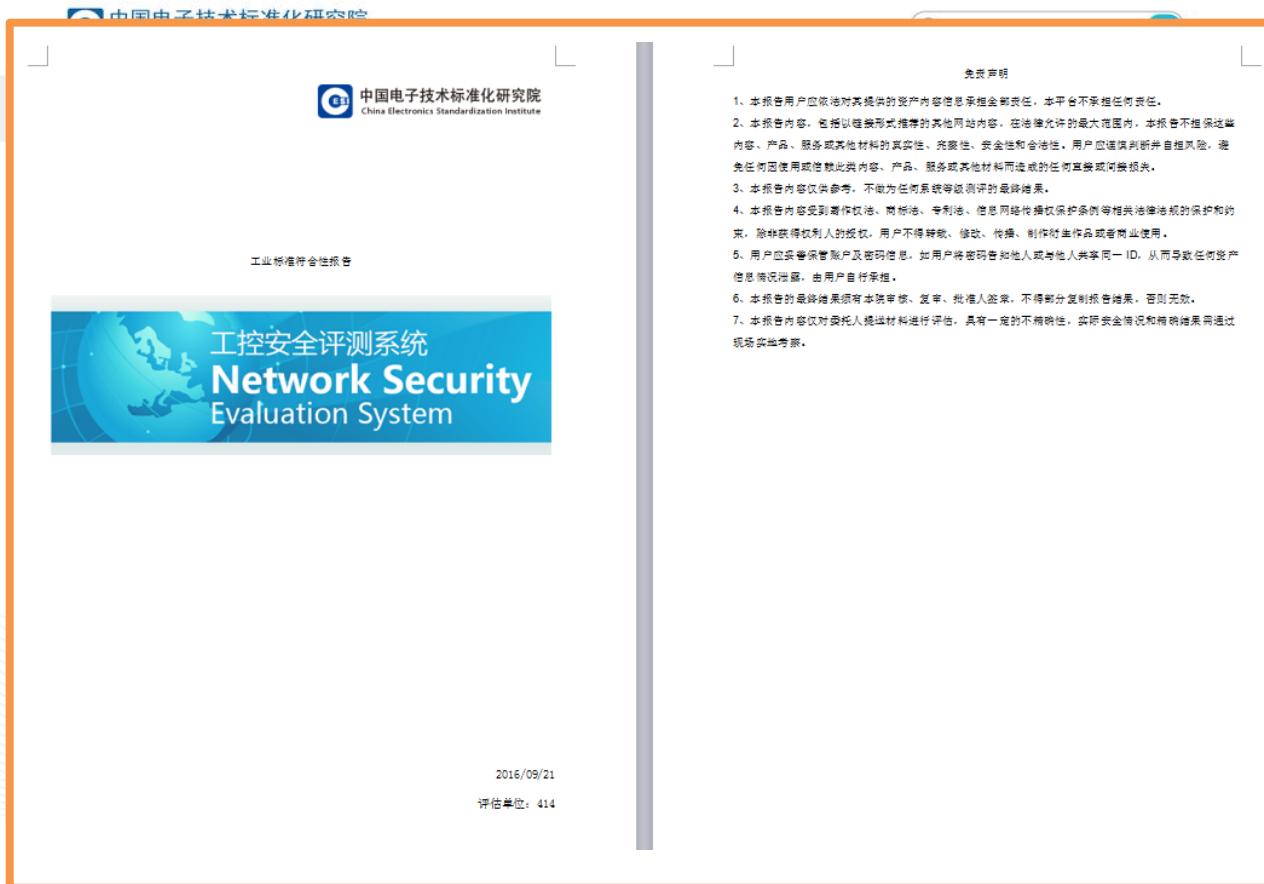
操作

# ICS安全防护能力评估介绍



## ➤ 工业控制系统信息安全防护能力评估系统

- ✓ 《工业控制系统信息安全防护指南》（工信软函[2016]338号）
- ✓ 《工业控制系统信息安全防护能力评估工作实施细则（试行）》



# ICS安全防护能力评估介绍

## 工业控制系统安全标准与测评工信部重点实验室

2016年，工信部正式批复中国电子技术标准化研究院成立工业控制系统安全标准与测评工信部重点实验室。在工信部、中央网信办等有关部门指导下，面向国家关键信息基础设施保护和智能制造信息安全保障工作，通过对工业生产过程中的关键生产环节进行归纳提取，搭建通用测试环境，开展关键技术标准研究、检测方法和检测工具研制，提供第三方测评介绍。目前建立了以轨道交通、石化、污水处理、城市管网4个测试平台为核心，6套国内首创检测工具为手段，1个资源库为支撑的工控系统及产品安全测评实验室体系。





# 工业控制系统安全标准与测评



## 工业和信息化部重点实验室

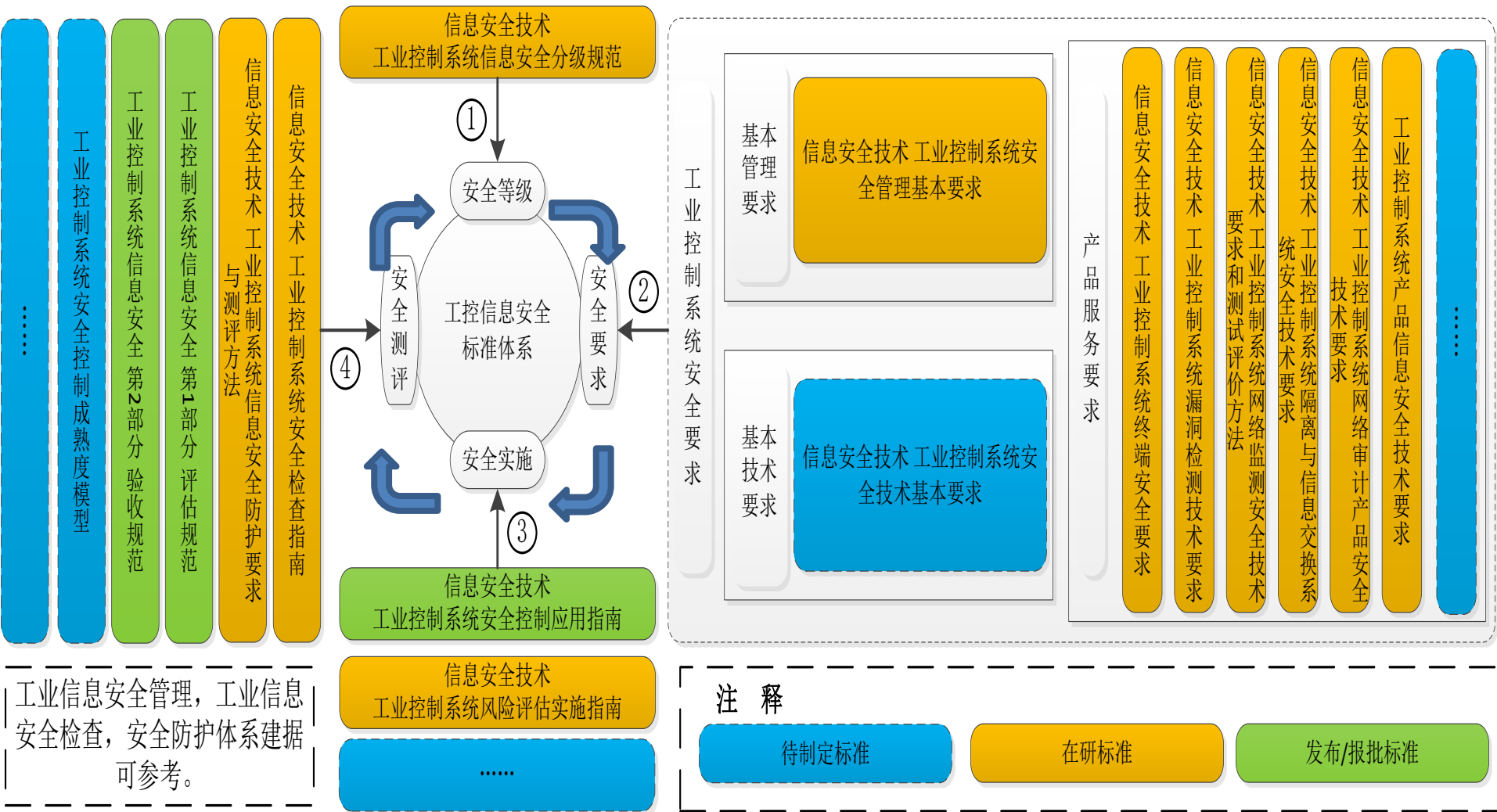
- 工业控制系统信息安全标准符合性评估（来自CESI权威的ICSST评估品牌）
- ✓ 部分标准验证测试环境





## 工业和信息化部重点实验室

### 工业控制系统信息安全标准体系研究



# 工业控制系统安全标准与测评

## 工业和信息化部重点实验室



[www.tc260.org.cn](http://www.tc260.org.cn)

序号	标准名称	所出状态
1	《信息安全技术 工业控制系统安全控制应用指南》（GB/T 32919-2016）	发布实施
2	《信息安全技术 工业控制系统测控终端安全要求》	报批稿
3	《信息安全技术 工业控制系统安全管理基本要求》	报批稿
4	《信息安全技术 工业控制系统安全分级指南》	报批稿
5	《信息安全技术 工业控制系统风险评估实施指南》	报批稿
6	《信息安全技术 工业控制系统安全检查指南》	征求意见稿
7	《信息安全技术 信息系统安全等级保护基本要求 第5部分：工业控制系统》	草案
8	《信息安全技术 工业控制系统安全防护技术要求和测试评价方法》	草案
9	《信息安全技术 工业控制系统网络审计产品安全技术要求》	征求意见稿
10	《工业控制系统专用防火墙技术要求》	征求意见稿
11	《信息安全技术 工业控制系统网络监测安全技术要求和测试评价方法》	征求意见稿
12	《信息安全技术 工业控制系统漏洞检测技术要求》	征求意见稿
13	《信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求》	征求意见稿
14	《工业控制系统产品信息安全评估准则 第1部分 简介和一般模型》	征求意见稿
15	《工业控制系统产品信息安全评估准则 第2部分 安全功能要求》	征求意见稿
16	《工业控制系统产品信息安全评估准则 第3部分 安全保障要求》	征求意见稿

## 工业和信息化部重点实验室

### ➤ 工业控制系统信息安全知识产权保护

#### ✓ 核心发明专利申请

一种面向Modbus协议的数据异常分析方法，专利号：201610546106.0

一种基于SCADA系统的安全DNP协议的实现方法，专利号：201610906114.1

一种基于FPGA的DCS数据加密方法，专利号：201610905577.6

一种PLC认证和安全通信的方法，专利号：201610808071.3

一种基于层次分析法的ICS信息安全评估方法，专利号:201610805410.2

工控网络安全检测装置（实用新型）申请号:2016212825598.5

基于工控协议的自适应漏洞挖掘框架，专利号:201611005127.8

一种工控网络安全检测装置和未知漏洞检测方法，专利号：201610619256X

基于PLC仿真的工控入侵检测方法和入侵检测系统，专利号：2016101316551

一种物联网设备认证与安全接入的方法，专利号：201611111340.7

一种基于数据依赖的工控行为异常检测系统，专利号：20160575649.5

#### ✓ 软件著作权

工业控制系统信息安全评估平台V1.0，软件登记号：2016SR271979

工业控制系统网络安全检查平台V1.0，软件登记号：2016SR273032

工业控制系统标准符合性评估软件V1.0，软件登记号：2016SR272096

工业控制网络安全设备检测软件V1.0，软件登记号：2016SR282203

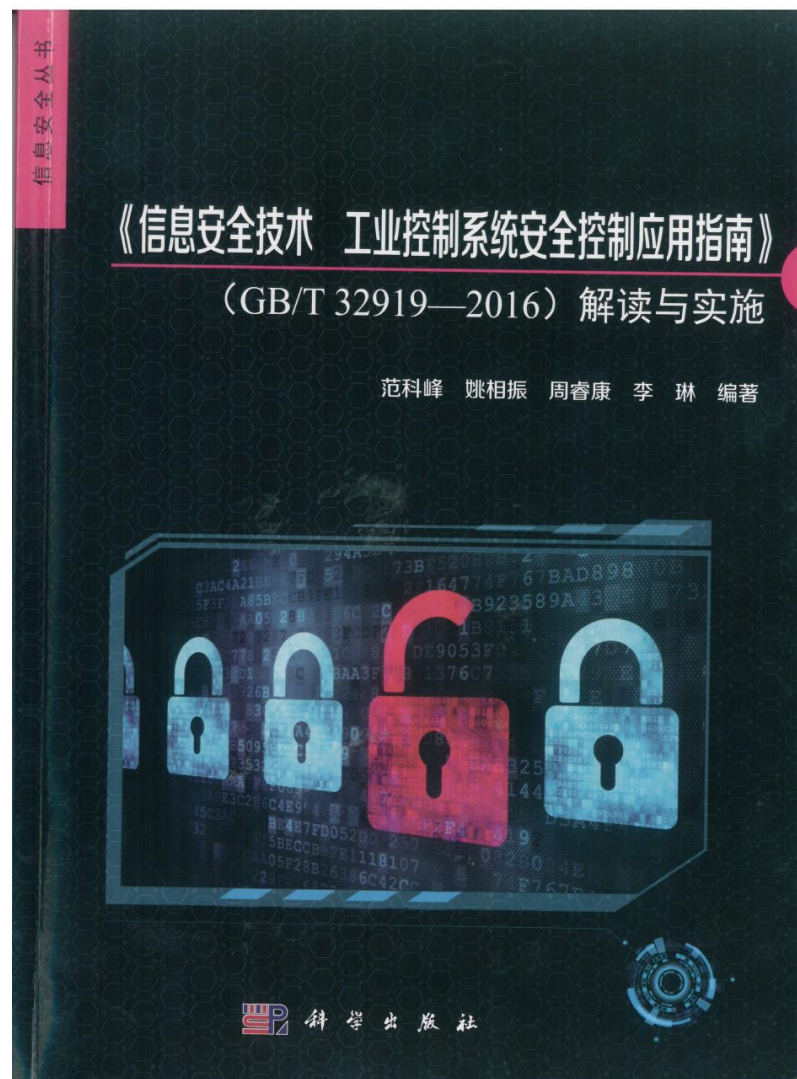
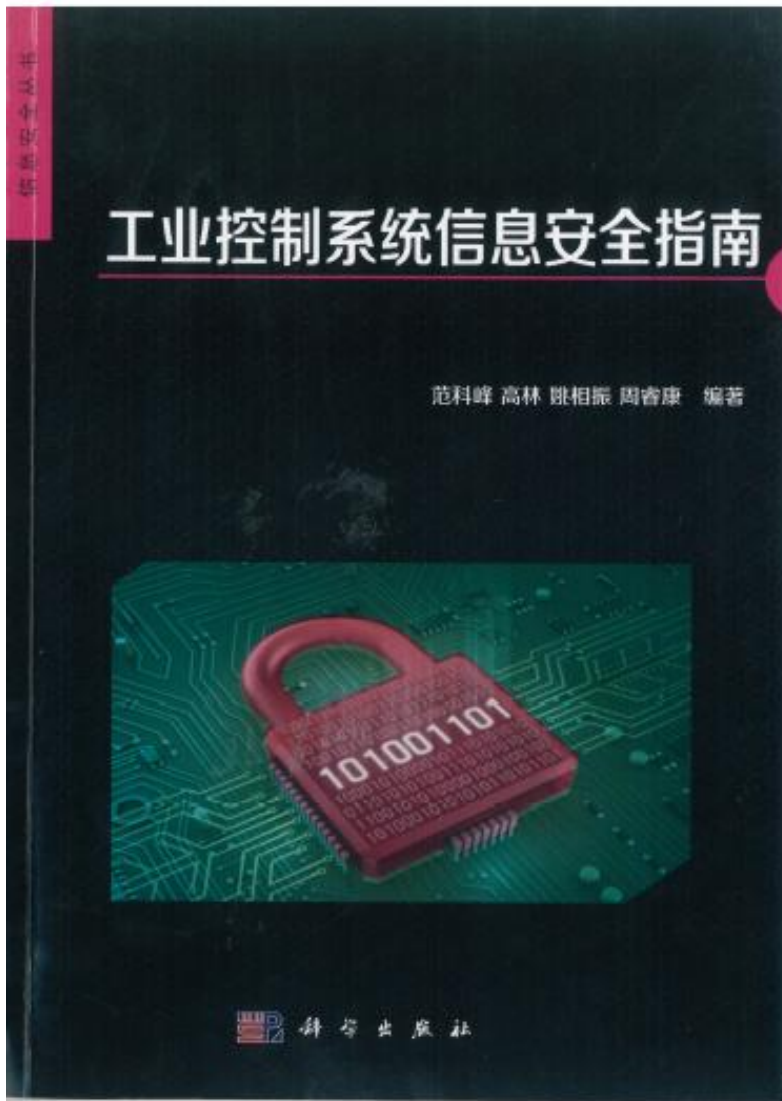
工业控制漏洞检测软件V1.0，软件登记号：2016SR283702

#### ✓ 论文

IEEE会刊等发表理论方法文章多篇

## 工业和信息化部重点实验室

- 工业控制系统信息安全标准知识产权
- ✓ 宣贯教材（公开发售，京东网有售）





## 工业和信息化部重点实验室

- 实验室基本能力
- ✓ 工业控制系统安全防护能力评估
- ✓ 工业控制系统标准体系研究
- ✓ 工业控制系统产品安全测评
- ✓ 工业控制系统标准符合性评估
- ✓ .....

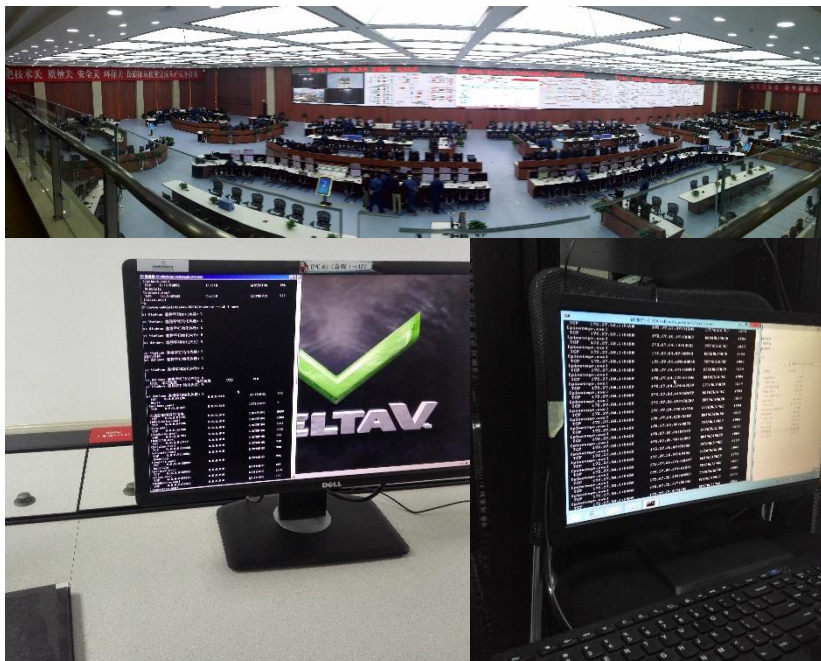
# ICS安全防护能力评估介绍



## 成功案例：神华集团和国家电网

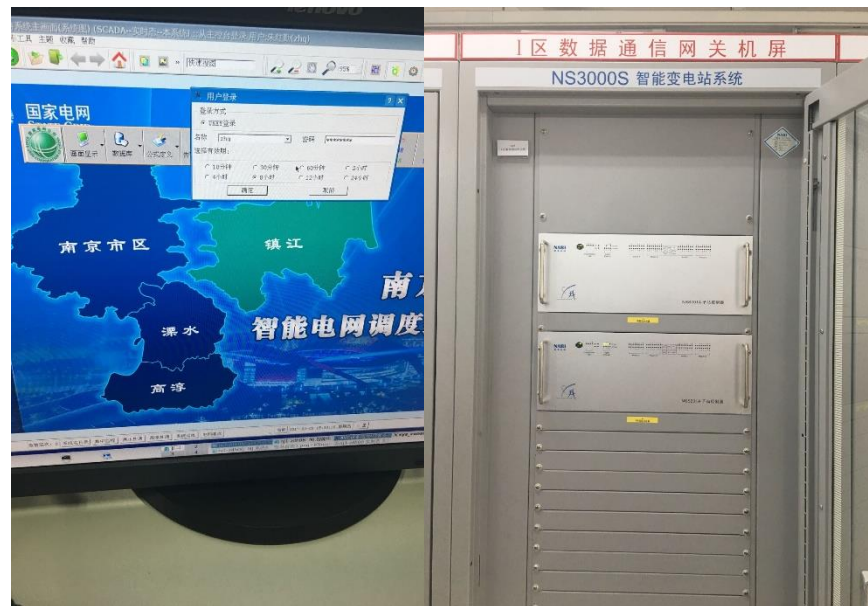
2017年4月，受工信部委托，赴神华集团和国家电网开展工业控制系统安全防护能力评估工作，针对宁煤集团的煤制油分公司和国家电网嘉庆变电站开展评估介绍，发现安全隐患，形成安全评估报告。

### 神华集团



- 检查系统安全漏洞
- 分析系统风险隐患
- 提出改进方案建议

### 国家电网



- 梳理工控系统架构
- 发现存在安全问题
- 形成安全解决方案

# 目 录

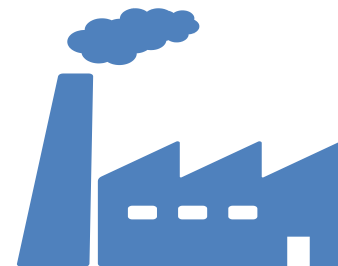
**1. 必要性**

**2. 保障体系建设及评估介绍**

**3. 合作**



- 依据《工业控制系统信息安全防护指南》（工信软函[2016]338号）、《工业控制系统信息安全防护能力评估工作实施细则（试行）》、《信息安全技术 工业控制系统安全控制应用指南》（GB/T 32919-2016）等，开展指南及标准培训宣贯与评估业务，提供工控安全保障全方位解决方案，为广大用户企业提供优质的技术评估介绍。欢迎垂询！





谢谢!

业务联系人：李琳 博士、姚相振博士、徐会真测评主管

联系电话：64102738（办公），64102739（实验室）

电子邮箱：[lilin9@cesi.cn](mailto:lilin9@cesi.cn)