中国电子技术标准化研究院

发电企业信息安全防护能力建设

报告人：夏冀

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

目 录

CONTENTS

1 基本情况

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：保密性—完整性—可用性

工控系统信息安全基本特征：可用性—完整性—保密性

→ 新的信息安全需求

1 基本情况

必要性

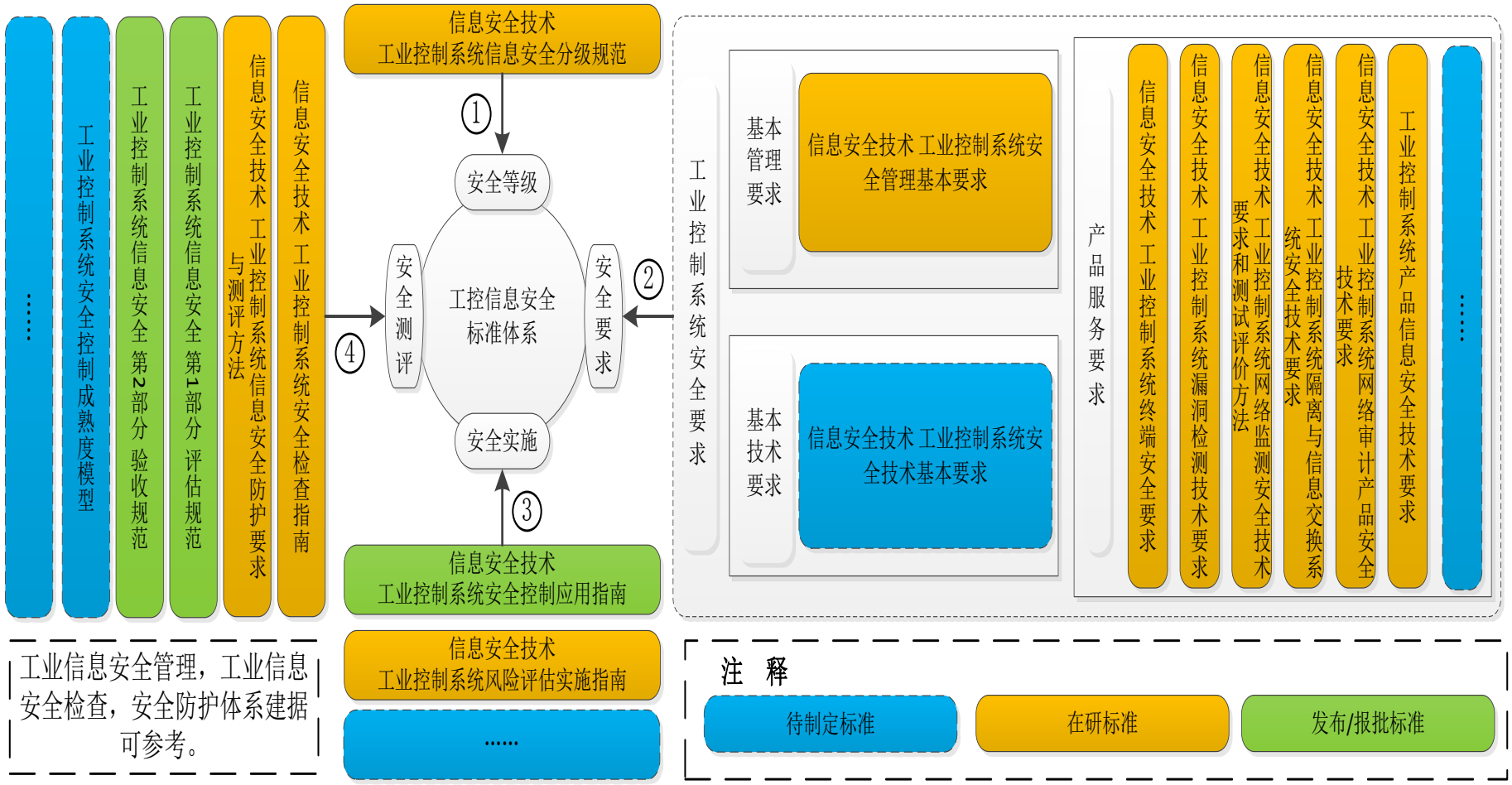
- 为切实做好工业信息安全保障工作，主管部门发布系列政策文件和法规：
  - 《 关于加强工业控制系统信息安全管理的通知》（工信部协〔2011〕 451号）；
  - 《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23 号）
  - 《关于开展2015年智能制造试点示范专项行动的通知》 （工信部装〔2015〕 72号）；
  - 《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号）；
  - 《关于加强国家网络安全标准化工作的若干意见》 （中网办发文〔2016〕5号 ）；
  - **《中华人民共和国网络安全法》（2016.11）**
  - **《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。

1 基本情况

工业控制系统信息安全标准体系



工业信息安全管理，工业信息安全检查，安全防护体系建据可参考。

注 释

待制定标准　在研标准　发布/报批标准

1 基本情况

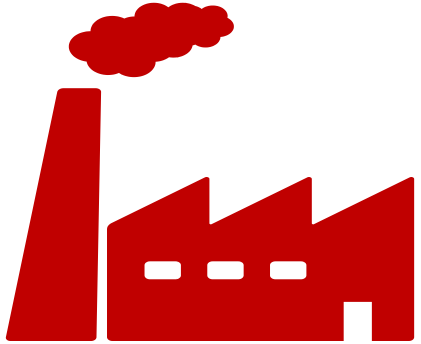
工业控制系统信息安全标准体系

序号	国标编号	信安标委立项号	名称	当前状态
1	GB/T 32919-2016	—	《信息安全技术 工业控制系统安全控制应用指南》	已发布
2	—	2012bzzd-WG5-005	《信息安全技术 工业控制系统安全管理基本要求》	报批稿
3	—	2012bzzd-WG5-007	《信息安全技术 工业控制系统测控终端安全要求》	报批稿
4	—	2012bzzd-WG5-009	《信息安全技术 工业控制系统安全分级指南》	报批稿
5	—	2014bzzd-WG5-002	《信息安全技术 工业控制系统风险评估实施指南》	报批稿
6	—	2012bzzd-WG5-006	《信息安全技术 工业控制系统安全检查指南》	征求意见稿
7	—	2014bzzd-WG5-004	《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
8	—	2013bzzd-WG5-008	《信息安全技术 工业控制系统专用防火墙技术要求》	征求意见稿
9	—	2015bzzd-WG5-007	《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
10	20160782-T-469	2015bzzd-WG5-006	《信息安全技术 工业控制系统漏洞检测技术要求和测试评价方法》	征求意见稿
11	—	2015bzzd-WG5-001	《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
12	—	2013bzxd-WG5-002	《信息系统安全等级保护基本要求 第5部分：工业控制系统》	征求意见稿
13	—	2015bzxd-WG5-005	《信息安全技术 信息系统等级保护安全设计技术要求 第5部分：对工业控制系统的扩展设计要求》	征求意见稿
14	—	2013bzzd-WG5-006	《信息安全技术 信息系统安全等级保护测评要求 第5部分 工业控制安全扩展测评要求》	征求意见稿
15	—	2016BZZD-WG5-002	《信息安全技术 数控网络安全技术要求》	征求意见稿
16	—	2012bzzd-WG5-008	《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》	标准草案
17	—	2015bzzd-WG5-003	《信息安全技术 工业控制系统产品信息安全通用评估准则》	标准草案

1 基本情况

评估和检查

2016年11月，中央网信办组织实施国家网络安全关键信息基础设施检查。
2017年4月，工信部信软司开展工业控制系统信息安全防护能力预评估工作。
2017年7月，工信部信软司组织工业控制系统信息安全检查。

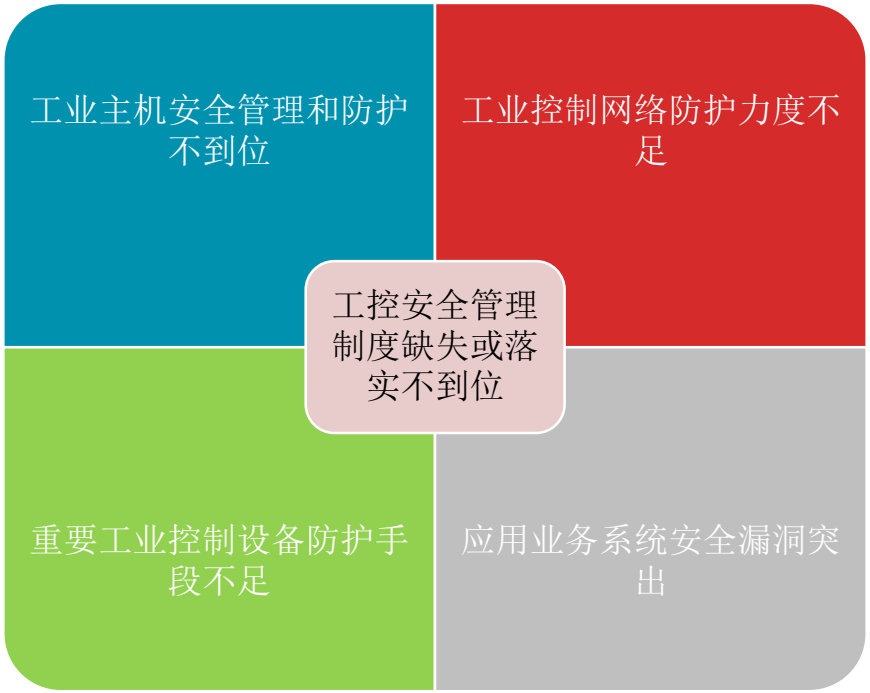


目 录

CONTENTS

2 发电企业评估开展工作

通过国家网络安全关键信息基础设施检查、工业控制系统信息安全防护能力预评估、工业控制系统信息安全检查工作，初步摸清了我国工业企业安全防护现状，也发现了一些共性问题。



- 工控领域行业众多，行业之间工控系统存在差别。为区分行业之间的差异性，我院计划通过对多家发电企业进行调研评估，在通用检查指标的基础上，建立一套基于发电企业的工业控制系统信息安全评估指标。
- 评估工作需侧重于从系统整体上对发电企业的信息安全现状进行评价。

2 发电企业评估

开展工作

我院已经数次组织评估队伍分别赴**浙江某发电厂**和**江苏某发电厂**进行工业控制系统信息安全标准符合性评估工作。

2 发电企业评估开展工作

➢ 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、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。

➢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。

开展工作

➢ 评估工具

在工控安全评估系统的基础上，搭配工控系统漏洞扫描工具、PLC安全监测工具，可以更准确、快捷的了解工控系统中潜在的安全问题。

工控系统漏洞扫描工具

PLC安全监测工具

发现问题

- 发电厂的管理信息系统（MIS）与厂级监控信息系统（SIS）之间没有网络安全设备或设备未配置安全策略。
- 可能会导致非授权人员通过企业办公网获取到SIS镜像服务器、SIS应用服务器、SIS性能计算服务器等的数据，造成企业重要信息的泄露。

2 发电企业评估

发现问题

- 工业控制网络中未部署通过国家认证的网络安全监测设备。
- 可能会导致企业不能及时发现、报告并处理网络攻击或异常行为。例如：设备状态异常、恶意软件传播、异常流量等。

发现问题

- 网络设备未合理分配、设置账户权限，未定期更新口令，口令未做相关要求，有些直接采用默认口令。
- 可能会导致口令泄露或由于口令简单被轻易破解，非授权人员登录系统，进行不合规操作，对电厂造成极大危害。

发现问题

- 杀毒软件未及时更新，系统补丁未及时更新。
- 可能会导致受感染的系统或设备连接到内部网络，植入恶意软件，导致系统的完整性/机密性受到危及。目前越来越多的漏洞攻击源自于针对已发布的补丁的逆向推演，利用漏洞攻击没有及时安装补丁的主机。

2 发电企业评估

发现问题

- 设备的USB、光驱等外部接口未封闭。
- USB、光驱等接口会增加主机感染病毒泄露数据的风险。在评估工作中发现，有些值班的工作人员直接将手机接在操作员站上充电。

发现问题

- 目前发电厂多数基础和核心设备严重依赖国外的产品和技术。
- 工业协议缺乏加密认证、运行环境存在大量漏洞和隐患并缺乏防护。
- 系统缺乏相应的访问控制策略，系统直接暴露在互联网上的风险较大。

发现问题

- 非授权人员通过B/S应用，基于Web窃取工控系统数据库中数据。
- 软件种类较多，存在跨站脚本漏洞、本地提权漏洞、缓冲区溢出漏洞和逻辑错误漏洞等安全问题。
- 存在管理和技术障碍，安全策略和管理流程欠缺。

2 发电企业评估

发现问题

- 数据库服务器备份周期过长，备份方式不合理。工业数据没有建立分级分类管理制度。
- 没有日志审计制度，未开展过日志审计工作，不能及时发现异常事件并采取相关措施。
- 工业控制系统应急预案未核实是否有效，未修改改进。

发现问题

风险	等级	说明
旁路控制	高	非授权人员对发电厂发送非法控制命令，导致电力系统故障。
数据泄露	中	非授权人员修改电力系统配置，窃取电力交易中的敏感数据。
违反授权	低	工作人员执行非授权的操作。
篡改数据	中	非授权人员篡改控制命令、参数设置、交易报价等敏感数据。
操作失误	中	工作人员无意识地泄露口令或带入病毒木马等。

目 录

CONTENTS

3 防护能力建设

建设依据

发电企业信息安全防护能力建设依据：
《中华人民共和国网络安全法》
《电力监控系统安全防护总体方案》国能安全〔2015〕36号文
《电力监控系统安全防护规定》国家发展和改革委员会令〔2014〕14号
《工业控制系统安全控制应用指南》GB/T 32919-2016
《工业控制系统信息安全防护指南》工信软函〔2016〕338号

- 为发电企业构筑工控系统整体防护体系，保护国家基础设施安全。

➢ 接入设备需可信；
➢ 传输消息需可信；
➢ 执行软件需可信。

3 防护能力建设

解决方案

针对网络安全：

- 需部署网络安全监测设备，对网络进行状态监测、日志采集、流量采集，能对异常行为进行分析、告警，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、暴力破解等网络攻击或异常行为。

3 防护能力建设

解决方案

针对网络安全：

- 需在管理信息系统（MIS）与厂级监控信息系统（SIS）之间部署网络安全设备，避免非授权人员通过企业办公网获取到SIS镜像服务器、SIS应用服务器等数据，保证企业重要历史信息的安全。

3 防护能力建设
解决方案

针对主机安全：

- 建立防病毒和恶意软件入侵管理机制，对工控系统及临时接入设备采取病毒查杀等安全预防措施。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，补丁更新时间不小于两个月。在补丁安装前，需对补丁进行安全评估和测试验证。

3 防护能力建设

解决方案

针对主机安全：

- 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、技术手段严格限制使用。

3 防护能力建设

解决方案

针对主机安全：

- 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。在设定密码最小位数、字符数字组合、密码使用期限等方面做要求。

3 防护能力建设

解决方案

针对综合安全：

- 需制定应用程序白名单，完善计算机防病毒制度，工控系统主机需安装杀毒软件，对工业控制系统及临时接入设备进行查杀。

3 防护能力建设

解决方案

针对综合安全：

- 建立工业控制系统安全策略配置清单，定期对工业控制系统进行安全配置基线检查；制定重大配置变更管理制度，重大变更前进行影响分析和评估、必要时应在离线环境中进行安全验证。

3 防护能力建设

解决方案

针对综合安全：

- 对应急预案进行演练核实，对不合理的地方进行改进。建立重要数据清单，重点管理。缩短定期备份关键业务数据的周期，防止数据的丢失。

3 防护能力建设

解决方案

针对综合安全：

- 与服务商签订保密协议，防止泄露工控系统的配置方案和重要数据。对相关人员进行工控安全培训，加强工控信息安全协调小组对其职责的了解。

目 录

CONTENTS

4 下一步工作

➢加强发电企业信息安全意识培训和宣传引导。通过对企业人员的信息安全意识培训、可减少工作中的不当操作、及时发现一些异常行为。

➢针对已发现的、常见的信息安全问题及时处理。目前发电企业暴露出许多很常见的信息安全问题，通过对问题的处理，可以有效提升企业的信息安全防护能力。

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