ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 37980—2019

# 信息安全技术
# 工业控制系统安全检查指南

**Information security technology—Guide for security inspection of industrial control systems**

2019-08-30 发布　　　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

# 目　次

# 前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国信息安全测评中心、中国电子技术标准化研究院、中国石油天然气集团公司、北京三零卫士信息安全技术有限公司,北京匡恩网络科技有限责任公司、青岛海天炜业过程控制技术股份有限公司、网神信息技术(北京)股份有限公司、浙江浙能台州第二发电有限责任公司、华能国际电力股份有限公司。

本标准主要起草人:戴忠华、彭勇、赵伟、韩雪峰、向憧、熊琦、邸丽清、高洋、范科锋、姚相振、李琳、周睿康、靖小伟、腾征岑、张建军、张大江、宿凤芹、李航、夏克晁、李辉。

# 引　　言

随着工业化和信息化的深度融合，工业控制系统广泛应用于核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。工业控制系统指应用于工业领域的数据采集、监视与控制系统，是由计算机设备、工业过程控制组件和网络组成的控制系统，是工业领域的神经中枢。工业领域使用的控制系统包括监控与数据采集系统(SCADA)、分布式控制系统(DCS)、可编程逻辑控制器(PLC)系统等。近年来针对工业控制系统的攻击事件层出不穷，工业控制系统的安全性将直接关系到国家重要基础工业设施生产的正常运行和广大公众的利益。

本标准制定的目的是为了指导我国国家关键基础设施中相关工业控制系统行业用户开展工业控制系统信息安全自评工作，掌握工业控制系统信息安全总体状况，及时有效发现工业控制系统存在的问题和薄弱环节，进一步健全工业控制系统信息安全管理制度，完善工业控制系统信息安全技术措施，提高工业控制系统信息安全防护能力，为国家对重点行业工业控制系统信息安全检查等工作提供支撑，为实现更安全的工业控制系统并在其内部进行有效的风险管理提供帮助。

# 信息安全技术
# 工业控制系统安全检查指南

## 1 范围

本标准给出了工业控制系统信息安全检查的范围、方式、流程、方法和内容。

本标准适用于开展工业控制系统的信息安全监督检查、委托检查工作，同时也适用于各企业在本集团(系统)范围内开展相关系统的信息安全自检查。

注：本标准适用的检查范围是广泛应用于核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、钢铁、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关领域的工业控制系统。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069—2010 信息安全技术 术语

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

## 3 术语和定义

GB/T 25069—2010 和 GB/T 32919—2016 界定的以及下列术语和定义适用于本文件。

3.1

**工业控制系统 industrial control system**

由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统。

注：工业控制系统的核心组件包括监控和数据采集系统、分布式控制系统、可编程逻辑控制器、主终端单元、远程终端单元、上位机，以及确保各组件通信的接口技术。

3.2

**监控和数据采集系统 supervisory control and data acquisition system**

在工业生产控制过程中，对大规模远距离地理分布的资产和设备在广域网环境下进行集中式数据采集与监控管理的控制系统。

注：SCADA 系统以计算机为基础，对远程分布运行设备进行监控调度，其主要功能包括数据采集、参数测量和调节、信息报警等。SCADA 系统一般由设在控制中心的主终端单元(MTU)、通信线路和设备、远程终端单元(RTU)等组成。

3.3

**分布式控制系统 distributed control system**

以计算机为基础，在系统内部(单位内部)对生产过程进行分布控制、集中管理的系统。

注：DCS 一般包括现场控制级、控制管理级两个层次，现场控制级主要是对单个过程进行控制，控制管理级主要是对多个分散的子过程进行数据采集、统一调度和管理。

3.4

**工业控制设备 industrial control device**

对工业生产过程及装置进行检测与控制的设备。

3.5

**可编程逻辑控制器 programmable logic controller**

采用可编程存储器,通过数字运算操作对工业生产装备进行控制的电子设备。

注:PLC 主要执行各类运算、顺序控制、定时执行等指令,用于控制工业生产装备的动作,是工业控制系统的主要基础单元。

3.6

**主终端单元 master terminal unit**

SCADA 系统中的服务器,用于集中控制,同远程终端单元进行通信。

3.7

**远程终端单元 remote terminal unit**

对较长通信距离和恶劣工业现场环境而设计的具有模块化结构的、特殊的计算机测控单元。

3.8

**上位机 supervisory computer**

直接发出操控命令的计算机。

3.9

**控制网 control network**

控制层网络,主要部署工程师站、操作员站、工业控制设备,为高安全等级的信任区域。

3.10

**安全检查 security inspection**

以查代促、以查促改、以查促管、以查促防,旨在推动提高信息安全工作能力和防护水平。

## 4 缩略语

下列缩略语适用于本文件。

ICS 工业控制系统(Industrial Control System)

SCADA 监控和数据采集(Supervisory Control And Data Acquisition)

DCS 分布式控制系统(Distributed Control System)

PLC 可编程逻辑控制器(Programmable Logic Controller)

MTU 主终端控制单元(Master Terminal Unit)

RTU 远程终端单元(Remote Terminal Unit)

## 5 检查方式

### 5.1 监督检查

监督检查是指上级管理部门组织的或国家有关职能部门依法开展的检查。

监督检查可依据本标准的要求,实施完整的信息安全检查过程。

监督检查也可在自检查的基础上,对关键环节或重点内容实施检查。

### 5.2 自检查

自检查是指信息系统所有者、运营或使用单位发起的对本单位工业控制系统安全状况进行的检查。自检查在本标准的指导下,结合系统特定的安全要求进行实施。

### 5.3 委托检查

受检单位或监督检查的组织部门不具备检查能力的,可委托经相关主管部门认可的机构开展检查。

# 6 检查工作流程

## 6.1 检查准备

### 6.1.1 概述

检查准备是开展检查工作的前提和基础，是整个检查过程有效性的保证。检查准备工作是否充分直接关系到后续工作能否顺利开展。本阶段的主要内容是明确检查工作的方式、依据、范围和内容，调研被检查单位和被检查系统的情况，确定被检查单位的联系人和联络方式，确定检查组成员和检查工具，制定检查方案和计划并通知被检查单位。

### 6.1.2 检查准备过程工作内容

根据检查工作的要求，明确安全检查工作的方式，包括监管机构监督检查、企业信息安全自查等。

明确安全检查工作的依据，包括国家信息安全规范性文件及标准、行业信息安全规范性文件及标准、主管机构要求等。

明确安全检查工作的范围，包括被检查单位、被检查系统、涉及的人员、被检查单位的上级主管单位等，并通过调研形成“工业控制系统信息安全检查工作调研表”。

明确安全检查工作的内容。由两部分内容组成，一部分为基本检查内容，相关要求详见本标准第8章；另外一部分为补充检查内容，由检查机构在每次检查前，依据有关主管单位要求、信息安全发展态势和企业的信息安全管理工作开展情况进行拟定。

由检查机构统一组织实施检查工作，确定现场检查组的人员和设备，可委托第三方信息安全服务机构实施现场检查工作，检查机构安排专人陪同。

根据检查工作的内容，制定“工业控制系统信息安全检查方案”“工业控制系统信息安全检查计划”和“工业控制系统信息安全检查工作表”。

在现场检查开始前，检查组至少提前两天将“工业控制系统信息安全检查方案”和“工业控制系统信息安全检查计划”下发至被检查单位，明确要求被检查单位对必要的系统和数据进行备份，被检查单位积极配合，并提供必要的配合人员和办公条件。

### 6.1.3 检查准备过程的角色和职责

检查机构职责：

a) 向被检查单位介绍安全检查的意义和目的、检查流程和工作方法；
b) 了解被检查单位的工业控制系统建设状况；
c) 指出被检查单位需提供的基本资料；
d) 向被检查单位说明检查工作自身的风险和规避方法；
e) 准备被检查系统基本情况调查表单；
f) 了解被检查系统基本情况；
g) 初步分析系统的安全情况；
h) 准备检查工具和文档。

被检查单位职责：

a) 向检查机构介绍本单位的工业控制系统建设状况与发展情况；
b) 准备检查机构需要的资料；
c) 为检查人员的信息收集提供支持和协调；
d) 根据被检查系统的具体情况，如业务运行高峰期、网络布置情况等，为检查时间安排提供适宜的建议；

e) 备份数据和系统,制定应急预案。

## 6.2 检查实施

### 6.2.1 概述

检查实施是检查工作的核心,主要依据检查方案的总体要求将本检查规范的要求落实到实际检查工作中,通过对被检查单位的人员访谈、文档审查、配置核查和安全测试,并调阅自查或上次检查报告(如果有),对被检查单位工业控制系统的安全保护现状进行取证,取得分析与总结活动所需的、足够的证据和资料。

### 6.2.2 检查实施过程工作内容

检查人员现场填写“工业控制系统信息安全检查工作表”,检查完成后需要由被检查单位签字确认。

现场检查完成后,需要由被检查单位对被检查的运行情况进行确认,并在“工业控制系统运行情况验证记录”上签字确认,对于因检查工作导致系统运行异常的情况,如实记录,并及时上报主管部门。

现场检查采用的方法和可能的风险如下:

a) 现场检查采用的方法主要包括:

1) 人员访谈

检查人员通过与工业控制系统有关人员(个人/群体)进行交流、讨论等活动,获取证据以证明信息系统安全保护措施是否有效的一种方法。

2) 文档审查

检查人员通过对被检查单位支撑工业控制系统安全建设与运维的安全管理制度、记录等文档的核查,获取证据以证明工业控制系统的安全保护要求是否全面,安全保护规定是否得到执行。

3)配置核查

检查人员通过对被检查系统进行观察、查验、分析等活动,获取证据以证明被检查系统安全保护措施是否有效的一种方法。

4) 安全测试

检查人员使用预定的方法/工具使被检查系统产生特定的行为,通过查看、分析这些行为的结果,获取证据以证明工业控制系统安全保护措施是否有效的一种方法。在检查中也可不重新实施安全测试而利用已有的安全测试结果。

b) 该阶段主要可能的风险包括:

1) 验证测试影响工业控制系统正常运行。在现场检查时,需要对设备和系统的安全策略配置和安全功能进行必要的验证测试,部分测试内容涉及到对设备的操作,可能对系统的运行造成一定的影响,甚至存在误操作的可能。

2) 工具测试影响工业控制系统正常运行。在现场检查时,有时会使用一些技术测试工具进行漏洞测试、性能测试甚至抗渗透能力测试等。工具测试可能会对系统的负载造成一定的影响,其中漏洞测试和渗透测试可能对系统数据造成一定破坏。

3) 原则上检查方不接触被检查系统,避免执行系统数据变更操作,由配合人员根据操作规程和检查项需求对被检查系统进行核查操作。

### 6.2.3 现场检查过程的角色和职责

检查机构职责:

利用人员访谈、文档审查、配置核查和安全测试的方法检查系统的保护措施与本标准要求的符合情况,以及正确性和有效性。

被检查单位职责:

a) 协调被检查系统内部相关人员的关系，配合检查工作的开展；
b) 回答检查人员的问询，对某些需要验证的内容上机进行操作；
c) 协助检查人员实施工具测试并提供有效建议，降低安全检查对系统运行的影响；
d) 协助检查人员完成业务相关内容的问询、验证和测试；
e) 相关人员对检查结果进行确认。

### 6.3 检查结果分析

#### 6.3.1 概述

检查结果分析是总结被检查系统整体安全保护能力的综合评价活动，根据现场检查结果和本标准的相关要求，定位系统的安全保护现状与本标准安全要求之间的差距，并分析这些差距导致被检查系统面临的风险，从而给出检查结论，形成检查报告和整改通知书。

#### 6.3.2 检查结果分析过程工作内容

现场检查工作完成后，由检查组对检查结果进行整理，采用定性或定量的风险分析方法（参见附录A），编制“工业控制系统安全检查报告”。

#### 6.3.3 检查结果分析过程的角色和职责

检查机构职责：
a) 分析检查结果，形成检查结论；
b) 编制整改通知书，说明被检查系统存在的安全隐患和缺陷，并给出改进建议；将生成的过程文档归档保存，并将检查过程中生成的电子文档清除。

## 7 检查内容的选择方法

### 7.1 全覆盖法

选取检查内容的所有检查项。

### 7.2 重点项抽取法

根据国家职能部门、上级主管部门或企业对工业控制系统进行安全检查工作的实际预期目标需求，从检查内容中确定重点检查项，只检查重点项。

### 7.3 增项检查法

根据国家职能部门、上级主管部门要求和工业控制系统信息安全发展态势等情况，设计检查内容中未包含的检查项作为新增检查项。

注：对于检查内容的选择，不局限于采取单一方式进行选择，也可根据检查目的，采用多种选择方式相结合，如同时采用重点项抽取法和增项检查法确定检查内容。

## 8 检查内容

### 8.1 概述

参考 GB/T 22239—2008、GB/T 20269—2006 和 GB/T 20984—2007，结合工业控制系统特性，将工业控制系统安全检查内容分为十二类，分别是组织体系、规章制度、资金保障、人员安全管理、服务外包管控、关键信息资产管控、工业控制系统建设安全管理、网路安全防护、上位机主机和设备安全防护、

物理环境安全防护、运行安全管理和应急管理。检查内容分类表参见附录B。

## 8.2 组织体系

### 8.2.1 第一责任人确立

本检查项包括：

检查企业主要负责人是否是信息安全第一责任人。

检查要素：

信息安全第一责任人。

检查方法：

文档审查，查看信息安全文件。

### 8.2.2 信息安全责任落实

本检查项包括：

a) 检查是否设立工业控制系统信息安全管理工作的职能部门，是否设立安全主管、系统管理员、网络管理员、安全管理员等岗位。
b) 是否以文件的形式明确责任部门、责任人员的职责。

检查要素：

信息安全责任部门、责任人员。日常安全生产管理体系。

检查方法：

文档审查，查看信息安全责任部门、责任人员职责文件。日常安全生产管理体系职责文件。

### 8.2.3 专职机构及岗位设置

本检查项包括：

检查组织的信息安全管理部门及岗位设置是否符合以下要求：

a) 企业集团公司总部设置工业控制系统信息安全专职管理机构。
b) 企业集团公司二级单位设置工业控制系统信息安全管理和技术岗位。
c) 工业控制系统基层单位设置信息安全岗位。

检查要素：

企业级别、信息安全管理部门及岗位设置。

检查方法：

a) 人员访谈，访问企业所属级别和信息安全管理部门及岗位设置。
b) 文档审查，根据企业级别查看信息安全管理部门及岗位设置说明文件。

### 8.2.4 安全人员配置

本检查项包括：

检查企业是否配备一定数量的专职信息安全工作人员，能否满足企业信息安全岗位需求。

检查要素：

专职信息安全工作人员数量、信息安全岗位数量。

检查方法：

文档审查，查阅企业网络职责说明及人员岗位职责分配说明。

## 8.3 规章制度

### 8.3.1 整体策略及总体方案制定

本检查项包括：

检查企业是否制定符合国家及行业政策要求的工业控制系统信息安全工作整体策略和总体方案,是否说明了信息安全工作总体目标、范围、防护框架和防护措施。

检查要素:

信息安全工作整体策略、总体方案、信息安全工作总体目标、范围、防护框架和防护措施。

检查方法:

文档审查,查阅信息安全整体策略和总体方案文档。

#### 8.3.2 制度制定及体系完整性

本检查项包括:

检查企业是否针对工业控制系统的信息安全工作制定基本安全管理制度,并以此为基础形成涵盖人员管理、资产管理、介质管理、建设安全管理、运行维护管理、外包服务管理、培训教育等方面的制度体系。

检查要素:

基本安全管理制度。

检查方法:

文档审查,查阅组织是否制定了基本管理制度,内容是否涵盖人员管理、资产管理、介质管理、建设安全管理、运行维护管理、外包服务管理、培训教育等方面。

#### 8.3.3 操作规程制定

本检查项包括:

检查企业是否对信息安全运行维护人员执行的日常操作制定运维流程和操作规程。

检查要素:

运维流程、操作规程。

检查方法:

文档审查,查阅组织制定的运维流程和操作规程文档。

#### 8.3.4 制度发布

本检查项包括:

检查企业是否通过正式、有效的方式发布工业控制系统信息安全管理制度。

检查要素:

制度发布方式。

检查方法:

文档审查,查阅安全管理制度发布方式和相关记录。

### 8.4 资金保障

本检查项包括:

检查企业是否将信息安全建设费用(安全软硬件购置、系统安全功能开发、安全验收测试、安全咨询与培训、安全专项研究等)和运行维护费用(日常安全运维、监测分析、应急演练、应急保障、信息安全监督检查、测试评估等)纳入年度预算。

检查要素:

信息安全建设费用、运行维护费用。

检查方法:

文档审查,查看年度预算计划。

### 8.5 人员安全管理

#### 8.5.1 安全培训与考核

本检查项包括：

检查企业信息安全从业，工业控制系统设计、建设、运维等相关各类人员是否经培训合格后上岗，是否定期接受相应的政策规划和专业技能培训。

检查要素：

人员安全培训及考核。

检查方法：

文档审查，查阅参加安全培训的人员名单及成绩单。

#### 8.5.2 保密协议签订

本检查项包括：

检查企业是否与安全管理员、系统管理员、网络管理员等关键岗位的人员，工业控制系统相关设备及系统的开发单位和供应商签署保密协议。

检查要素：

保密协议签订。

检查方法：

文档审查，查阅签署保密协议的人员名单及其岗位或单位。

#### 8.5.3 人员审查

本检查项包括：

检查企业是否对信息安全岗位人员和其他敏感岗位人员实施身份、背景和资质审查。

检查要素：

人员的身份、背景和资质审查制度和审查结果记录。

检查方法：

文档审查，查阅信息安全岗位人员和其他敏感岗位人员的身份、背景和资质审查记录。

#### 8.5.4 岗位调整管控

本检查项包括：

检查企业是否在信息安全岗位人员及其他敏感岗位人员离岗时执行权限回收和离岗承诺书签署。

检查要素：

人员的权限回收记录、离岗承诺书。

检查方法：

文档审查，查阅信息安全岗位人员及其他敏感岗位人员的回收记录和离岗承诺书。

### 8.6 服务外包管控

#### 8.6.1 外包服务协议

本检查项包括：

检查企业与合约方签订的外包服务协议中是否具有信息安全管控和保密条款。

检查要素：

外包服务协议。

检查方法：

文档审查，查阅外包服务协议中的信息安全管控和保密条款。

#### 8.6.2 外部人员访问管理

本检查项包括：

检查企业是否对外部人员访问机房等受控区域采取书面审批、人员陪同、进出记录等管控措施。

检查要素：

受控区域访问控制措施和记录。

检查方法：

文档审查，查阅第三方人员访问管理制度和记录。

#### 8.6.3 远程服务管控

本检查项包括：

检查企业是否采取远程服务，如采取远程服务，针对远程服务访问采取书面审批、访问控制、在线监测、日志审计等管控措施。

检查要素：

远程服务管控措施和记录。

检查方法：

a) 人员访谈，询问对远程服务访问采取的控制措施。

b) 文档审查，查阅远程服务管控措施制度和记录。

c) 配置核查，如采取远程服务，查阅远程服务管控相关审计日志。

#### 8.6.4 现场开发管控

本检查项包括：

检查企业是否采取技术措施实现开发测试环境与实际生产运行环境物理分离，并对开发人员的活动范围和行为实施管控。

检查要素：

现场开发的管控措施和记录。

检查方法：

a) 人员访谈，询问是否将开发测试环境与实际生产环境物理分离。

b) 文档审查，查阅开发人员的活动范围和行为管控制度。

### 8.7 关键信息资产管控

#### 8.7.1 资产管理

本检查项包括：

检查企业是否识别所有与工业控制系统相关的资产并编制了准确的资产清单，是否对每项资产明确管理责任人及其职责。

检查要素：

资产清单。

检查方法：

文档审查，查阅资产清单，检查是否识别所有与信息系统相关的资产，是否对每项资产明确管理责任人及其职责。

#### 8.7.2 资产维修报废管理

本检查项包括：

检查企业是否在系统、设备维修或报废时，选取了可信服务机构并对数据采取了备份、清除等有效保护措施。

检查要素：

可信服务机构选择、数据保护措施和记录。

检查方法：

文档审查，查阅系统、设备维修或报废管理制度和记录。

### 8.8 工业控制系统建设安全管理

#### 8.8.1 上线安全测评

本检查项包括：

检查企业工业控制系统在上线前是否通过信息安全测评。

检查要素：

上线前通过安全测评的系统清单、信息系统清单。

检查方法：

文档审查，查阅全部信息系统列表，查阅并统计已通过信息安全测评的系统测评报告。

#### 8.8.2 产品采购和使用

本检查项包括：

检查企业安全产品和密码产品的采购及使用是否符合国家有关规定。

检查要素：

安全产品和密码产品。

检查方法：

a） 人员访谈，访谈相关人员是否了解相关制度，是否存在不执行相关制度的特殊情况。
b） 文档审查，查阅企业相关管理制度和资产清单等，检查其采购及使用是否符合国家有关规定。
c） 配置核查，核查已被通报存在隐患的在线运行的系统和设备是否已经整改及相关运行管理和安全防护措施。

#### 8.8.3 核心产品采购测试

本检查项包括：

企业应用的信息安全产品、系统基础软硬件、系统应用软件、工业控制系统或设备等在采购前是否通过了安全性测试。

检查要素：

安全性测试报告。

检查方法：

文档审查，查阅企业应用的信息安全产品、系统基础软硬件、系统应用软件、工业控制系统或设备等的安全性测试报告。

### 8.9 网络安全防护

#### 8.9.1 网络架构安全

本检查项包括：

检查企业是否根据业务特点对网络进行了分区分域管控，并对不同域之间采取了边界防护措施。

检查要素：

网络拓扑结构图。

检查方法：

a) 人员访谈，访谈企业对网络的分区分域管控情况，了解每个分区边界的防护情况。
b) 文档审查，查看网络拓扑结构图与访谈情况的一致性。
c) 安全测试，利用相关命令语句等测试各分区的连通情况。

#### 8.9.2 控制网边界防护

本检查项包括：

检查企业是否设置控制网边界防护的技术措施，检查网络边界连接情况和安全设备部署情况。

检查要素：

a) 控制网边界防护技术措施。
b) 网络边界连接情况。
c) 网络边界安全设备部署情况。

检查方法：

a) 人员访谈，询问采取的控制网边界防护的技术措施。
b) 配置核查，检查网络边界连接情况和安全设备部署情况。
c) 安全测试，验证系统是否能够对非授权设备私自联到内部网络的行为进行有效阻断，验证系统是否能够对内部网络用户私自联到外部网络的行为进行有效阻断。

#### 8.9.3 网络安全审计

本检查项包括：

a) 检查企业是否建立控制服务器等工业控制系统关键设备安全配置和审计制度。
b) 检查企业是否设置网络安全审计的技术措施和审计记录保护措施。

检查要素：

a) 网络安全审计记录。
b) 网络安全审计记录保护措施。

检查方法：

a) 人员访谈，询问采取的网络安全审计的技术措施和审计记录保护措施。
b) 文档审查，查阅控制服务器等工业控制系统关键设备安全配置和审计制度。
c) 配置核查，检查网络安全审计记录，对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。

#### 8.9.4 网络冗余和容差策略

本检查项包括：

检查企业是否设置网络冗余和容差策略。

检查要素：

网络冗余和容差策略。

检查方法：

a) 人员访谈，询问采取网络冗余和容差策略。
b) 配置核查，检查关键节点的网络设备、安全设备的冗余，采用冗余技术设计网络拓扑结构，避免存在网络单点故障；检查控制网内网络设备、安全设备、重要服务器的备件情况。

#### 8.9.5 远程访问

本检查项包括：

检查企业是否按照远程访问方式的使用限制和操作指南进行远程访问，是否设置远程访问监控机制，是否设置远程接入授权机制，是否设置远程接入过程安全性保护措施。

检查要素：

远程访问使用限制和操作指南、远程访问监控机制、远程接入授权机制、远程接入过程安全性保护措施。

检查方法：

a) 文档审查，查阅远程访问方式的使用限制和操作指南，对每一个允许远程访问系统的方法建立使用限制和操作指南。
b) 配置核查，检查远程访问监控机制，监控未经授权的远程访问；检查远程接入授权机制，在建立远程连接之前应用授权过程；检查远程接入过程安全性保护措施，采取无线组网采取严格的身份认证、安全监测等防护措施，防止经无线网络进行恶意入侵，尤其要防止通过侵入远程终端单元（RTU）进而控制部分或整个工业控制系统，能对非授权的远程访问进行阻断。

#### 8.9.6 移动终端安全接入

本检查包括：

检查企业是否针对移动终端接入采取了安全性检测、书面审批、统一接入管理、访问控制、在线监测、日志审计等必要管控措施。

检查要素：

移动终端安全管控措施和记录。

检查方法：

a) 人员访谈，询问对移动终端接入采取的控制措施。
b) 文档审查，查阅管理制度是否要求移动终端接入前采取安全性检测、书面审批、统一接入管控、访问控制、在线监测、日志审计等管控措施。

### 8.10 上位机主机和设备安全防护

#### 8.10.1 补丁更新

本检查项包括：

检查企业是否按照补丁管理制度要求进行可更新补丁的更新。

检查要素：

补丁更新管理制度、补丁更新情况。

检查方法：

a) 文档审查，查阅补丁更新管理制度和补丁更新频率。
b) 配置核查，检查主机操作系统和网络设备的补丁更新情况。
c) 安全测试，在确保应用系统的安全前提下，通过漏洞扫描工具验证主机操作系统和网络设备的补丁更新情况。

#### 8.10.2 恶意代码防护

本检查项包括：

检查企业是否按照恶意代码管理制度要求进行恶意代码检测和可更新恶意代码库的更新。

检查要素：

恶意代码防范管理制度、恶意代码库更新情况。

检查方法：

a） 文档审查，查阅恶意代码防范管理制度和更新频率。

b） 配置核查，检查恶意代码检测程序和可更新恶意代码库的更新情况。

#### 8.10.3 系统安全整改加固

本检查项包括：

检查企业生产控制主机和设备中对等级保护测评、风险评估、信息安全检查等工作中发现的问题是否完成安全整改加固。

检查要素：

安全问题报告、安全整改加固实施工作报告。

检查方法：

a） 文档审查，查阅安全问题报告，查阅安全整改加固实施工作报告。

b） 配置核查，检查与验证安全整改加固工作实施情况。

#### 8.10.4 移动存储介质管理

本检查项包括：

检查企业是否设置限制和管理移动存储介质使用的管理和技术措施，是否对移动存储介质的分发、注册、使用、存放、销毁实施管理。

检查要素：

移动存储介质管理措施。

检查方法：

a） 文档审查，查阅移动存储介质安全管理制度。

b） 安全测试，验证系统中是否具备移动存储介质管理技术措施。

#### 8.10.5 上位机终端管控

本检查项包括：

检查生产控制网上位机终端是否实施了安全管控(安全管理、接入管理等)并统一安装防病毒软件。

检查要素：

终端安全管理措施、实施了安全管控措施的终端。

检查方法：

a） 人员访谈，询问采取了何种终端安全管理措施。

b） 文档审查，查阅终端安全管理制度。

c） 配置核查，检查并统计终端安全管理措施部署情况。

#### 8.10.6 主机和设备账号口令管理

本检查项包括：

检查上位机主机和设备中口令设置是否符合口令管理制度要求。

检查要素：

符合口令管理制度要求的主机和设备。

检查方法：

a) 文档审查，查阅主机和设备安全检测报告。

b) 配置核查，检查并统计符合口令管理制度要求的主机和设备数量。

## 8.11 物理环境安全防护

本检查项包括：

检查企业生产控制网机房是否按照等级保护要求落实物理安全防护。

检查要素：

按照等级保护要求落实物理安全防护的机房清单。

检查方法：

文档审查，查阅等级测评报告等并统计按照等级保护要求落实物理安全防护的机房。

## 8.12 运行安全管理

### 8.12.1 日常维护

本检查项包括：

检查企业是否按照制定的规章制度、运维流程、操作规程等执行生产控制系统日常维护并有详尽记录。

检查要素：

日常运维制度、运维流程、操作规程和记录。

检查方法：

文档审查，查阅是否按照制定的规章制度、运维流程、操作规程等执行信息系统日常维护并有详尽记录。

### 8.12.2 安全审计

本检查项包括：

检查是否对网络运行日志、操作系统日志、数据库访问日志、业务应用系统运行日志、安全设备和系统运行日志等进行集中收集、定期分析。

检查要素：

日志集中收集措施、日志定期分析报告。

检查方法：

a) 文档审查，查阅是否具备集中日志定期分析报告。

b) 配置核查，检查是否对网络运行日志、操作系统日志、数据库访问日志、业务应用系统运行日志、安全设备和系统运行日志等进行集中收集。

### 8.12.3 补丁管理

本检查项包括：

检查企业是否按照补丁管理制度制定补丁升级策略，是否针对关键业务系统建立补丁升级测试环境或建立了获取已测试补丁的有效渠道。

检查要素：

补丁管理制度和记录、补丁升级策略、补丁升级测试环境或渠道。

检查方法：

a) 文档审查，查阅是否具备补丁管理制度，是否明确补丁升级策略，查阅是否具备补丁升级记录。

b) 配置核查，检查是否对关键业务系统建立补丁升级测试环境或建立了获取已测试补丁的有效

渠道。

#### 8.12.4 安全监测

本检查项包括：

检查企业是否建立安全监测系统对控制网网络流量、重要网络设备、工控系统终端、病毒木马情况、安全防护情况等进行实时监测。

检查要素：

安全监测系统、安全监测报告。

检查方法：

a) 文档审查，查阅是否描述了安全监测系统的监测对象范围和监测内容，查阅是否具备安全监测报告。
b) 配置核查，检查安全监测系统的监测对象范围和监测内容。

### 8.13 应急管理

#### 8.13.1 信息通报

本检查项包括：

检查企业是否建立网络与信息安全信息通报机制，按要求向监管机构通报网络和信息系统安全状况。

检查要素：

网络与信息安全信息通报机制。

检查方法：

文档审查，查阅是否通过制度建立网络与信息安全信息通报机制，是否明确需要通报的内容和范围，是否落实负责人员。

#### 8.13.2 应急预案制定

本检查项包括：

检查企业是否按照网络与信息安全应急预案，制定本组织网络与信息安全及专项应急预案。

检查要素：

网络与信息安全应急预案。

检查方法：

a) 人员访谈，询问是否制定不同事件的应急预案。
b) 文档审查，查阅是否按照信息安全应急预案，制定本组织网络与信息安全应急预案，是否明确启动应急预案的条件、应急处理流程、系统恢复流程、事后教育培训和定期审核更新等方面的内容。

#### 8.13.3 应急演练

本检查项包括：

检查企业是否实施年度应急演练，是否有演练脚本和演练实施记录文档。

检查要素：

应急演练制度和记录。

检查方法：

文档审查，查阅是否制定应急演练制度，是否实施年度应急演练，是否有演练脚本和演练实施

记录文档。

#### 8.13.4 应急资源配备

本检查项包括：

检查企业是否根据信息安全工作需求，配置应急支援技术队伍并储备备机备件。

检查要素：

应急支援技术队伍与物资。

检查方法：

a) 人员访谈，询问是否具备应急支援技术队伍，是否具备应急备机备件并能正常工作。

b) 文档审查，查阅应急支援技术队伍人员名单，查阅应急备机备件清单。

#### 8.13.5 事故调查

本检查项包括：

检查企业是否按照行业及本单位应急预案要求，配合或组织开展事故调查。

检查要素：

事故调查制度、事故调查记录或报告。

检查方法：

a) 人员访谈，询问是否曾配合或组织开展事故调查。

b) 文档审查，查阅信息安全事故调查制度，查阅信息安全事故调查记录或报告是否记录引发安全事故的原因，是否记录事故调查过程。

# 附　录　A
（资料性附录）
风险分析方法

## A.1　定性分析

### A.1.1　判断安全问题发生的可能性

判断工业控制系统安全问题发生的可能性是工业控制系统定性分析方法的第一步，其取值范围为高、中和低，详见表A.1。

**表A.1　工业控制系统安全问题发生的可能性取值表**

| 标识 | 定义 |
|---|---|
| 高 | 安全问题出现的频率较高(大于或等于1次/月)；或在大多数情况下很有可能会发生；或可以证实多次发生过；或其实现条件较容易被攻击者获得 |
| 中 | 安全问题出现的频率中等(大于1次/半年)；或在某种情况下可能会发生；或被证实曾经发生过；或其实现条件难以被攻击者获得 |
| 低 | 安全问题出现的频率较小；或一般不太可能发生；或没有被证实发生过；或其实现条件很难被攻击者获得 |

### A.1.2　判断对工业控制系统造成的影响程度

工业控制系统的安全问题被威胁利用后，对工业控制系统安全造成的影响程度取值范围为高、中和低，详见表A.2。

**表A.2　对工业控制系统安全造成的影响程度取值表**

| 标识 | 定义 |
|---|---|
| 高 | 如果安全问题出现，将对工业控制系统造成重大损害 |
| 中 | 如果安全问题出现，将对工业控制系统造成一般损害 |
| 低 | 如果安全问题出现，将对工业控制系统造成较小或轻微损害 |

### A.1.3　判断工业控制系统面临的安全风险

综合A.1.1和A.1.2的结果，对工业控制系统面临的安全风险进行赋值，风险值的取值范围为高、中和低，详见表A.3。

**表A.3　工业控制系统面临的安全风险取值表**

| 标识 | 描述 |
|---|---|
| 高 | 一旦发生将产生较为严重的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害 |
| 中 | 一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度不大 |
| 低 | 一旦发生造成的影响程度较低甚至几乎不存在，一般仅限于组织内部，通过较为简单的手段很快能解决 |

## A.2 定量分析

根据工业控制系统生产企业信息安全工作实际情况是否符合检查项描述，为检查项赋予权重值($V_{ij}$)，根据检查结果判定赋予量化判定值($P_{ij}$)，安全检查结果量化由式(A.1)计算求得：

$$ISL = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} V_{ij} P_{ij}\right) \qquad \cdots\cdots (A.1)$$

式中：

$n$ ——检查项个数；

$m$——第 $i$ 检查项中检查条款的个数。

工业控制系统安全各检查项的权重值和量化判定值详见表 A.4。

**表 A.4 工业控制系统安全定量分析赋值表**

| 检查类 | 检查项 | 权重值 $V_{ij}$ | 量化判定值 $P_{ij}$ |
|---|---|---|---|
| 组织体系 | 第一责任人确立 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 信息安全责任落实 | 2 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 专职机构及岗位设置 | 2 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 安全人员配置 | 2 | 比值$=\frac{\text{专职信息安全人员数量}}{\text{信息安全岗位总数}}$<br>$P_{ij}$=比值的小数点后两位 |
| 规章制度 | 整体策略及总体方案制定 | 2 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 制度制定及体系完整性 | 2 | 形成体系：$0.5<P_{ij}\leqslant 1$<br>制定基本制度：$0<P_{ij}\leqslant 0.5$<br>无制度：$P_{ij}=0$ |
| | 操作规程制定 | 2 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 制度发布 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| 资金保障 | 经费预算 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |

**表 A.4（续）**

| 检查类 | 检查项 | 权重值 $V_{ij}$ | 量化判定值 $P_{ij}$ |
|---|---|---|---|
| 人员安全管理 | 安全培训与考核 | 1 | 比值$=\frac{年度培训人数}{员工总数}$<br>$P_{ij}=$比值的小数点后两位 |
| | 保密协议签订 | 1 | 比值$=\frac{签署保密协议员工数量}{员工总数}$<br>$P_{ij}=$比值的小数点后两位 |
| | 人员审查 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 岗位调整管控 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| 服务外包管控 | 外包服务协议 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 外部人员访问管理 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 远程服务管控 | 2 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 现场开发管控 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| 关键信息资产管控 | 资产管理 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 资产维修报废管理 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| 工业控制系统建设安全管理 | 上线安全测评 | 1 | 比值$=\frac{通过上线测评系统数}{已投运系统总数}$<br>$P_{ij}=$比值的小数点后两位 |
| | 产品采购和使用 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 核心产品采购测试 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |

**表 A.4（续）**

| 检查类 | 检查项 | 权重值 $V_{ij}$ | 量化判定值 $P_{ij}$ |
|---|---|---|---|
| 网络安全防护 | 网络架构安全 | 2 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 控制网边界防护 | 2 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 网络安全审计 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 网络冗余和容差策略 | 2 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 远程访问 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 移动终端安全接入 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| 上位机主机和设备安全防护 | 补丁更新 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 恶意代码防护 | 2 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 系统安全整改加固 | 2 | $比值=\frac{已完成加固的主机和设备数}{应加固主机和设备数}$<br>$P_{ij}$＝比值的小数点后两位 |
| | 移动存储介质管理 | 1 | 符合：$P_{ij}=1$<br>部分符合：$P_{ij}=0.5$<br>不符合：$P_{ij}=0$ |
| | 上位机终端管控 | 2 | $比值=\frac{已管控终端数}{总终端数}$<br>$P_{ij}$＝比值的小数点后两位 |
| | 主机和设备账号口令管理 | 2 | $比值=\frac{未发现问题的主机和设备台数}{总检测台数}$<br>$P_{ij}$＝比值的小数点后两位 |
| 物理环境安全防护 | 机房安全建设 | 2 | $比值=\frac{符合要求的机房数}{组织机房总数}$<br>$P_{ij}$＝比值的小数点后两位 |

表 A.4(续)

| 检查类 | 检查项 | 权重值 $V_{ij}$ | 量化判定值 $P_{ij}$ |
| --- | --- | --- | --- |
| 运行安全管理 | 日常维护 | 2 | 符合:$P_{ij}=1$<br>部分符合:$P_{ij}=0.5$<br>不符合:$P_{ij}=0$ |
| | 安全审计 | 1 | 未开启日志审计功能,$P_{ij}=0$<br>仅开启日志审计功能,$P_{ij}=0.3$<br>开启日志审计功能并定期分析,$0.3<P_{ij}\leqslant 0.7$<br>实施日志集中审计和分析预警,$0.7<P_{ij}<1$ |
| | 补丁管理 | 2 | 符合:$P_{ij}=1$<br>部分符合:$P_{ij}=0.5$<br>不符合:$P_{ij}=0$ |
| | 安全监测 | 2 | 符合:$P_{ij}=1$<br>部分符合:$P_{ij}=0.5$<br>不符合:$P_{ij}=0$ |
| 应急管理 | 信息通报 | 1 | 符合:$P_{ij}=1$<br>部分符合:$P_{ij}=0.5$<br>不符合:$P_{ij}=0$ |
| | 应急预案制定 | 1 | 符合:$P_{ij}=1$<br>部分符合:$P_{ij}=0.5$<br>不符合:$P_{ij}=0$ |
| | 应急演练 | 1 | 符合:$P_{ij}=1$<br>部分符合:$P_{ij}=0.5$<br>不符合:$P_{ij}=0$ |
| | 应急资源配备 | 1 | 符合:$P_{ij}=1$<br>部分符合:$P_{ij}=0.5$<br>不符合:$P_{ij}=0$ |
| | 事故调查 | 1 | 符合:$P_{ij}=1$<br>部分符合:$P_{ij}=0.5$<br>不符合:$P_{ij}=0$ |

注:权重值及量化判定值是根据实际项目实施经验总结进行设置的,标准使用者可根据实际情况进行调整和优化。

# 附　录　B
（资料性附录）
检查内容分类表

工业控制系统安全检查内容分类按表B.1。

**表B.1　工业控制系统安全检查内容分类表**

| 序号 | 检查类 | 检查项 |
|---|---|---|
| 1 | 组织体系 | 第一责任人确立 |
| | | 信息安全责任落实 |
| | | 专职机构及岗位设置 |
| | | 安全人员配置 |
| 2 | 规章制度 | 整体策略及总体方案制定 |
| | | 制度制定及体系完整性 |
| | | 操作规程制定 |
| | | 制度发布 |
| 3 | 资金保障 | 经费预算 |
| 4 | 人员安全管理 | 安全培训与考核 |
| | | 保密协议签订 |
| | | 人员审查 |
| | | 岗位调整管控 |
| 5 | 服务外包管控 | 外包服务协议 |
| | | 外部人员访问管理 |
| | | 远程服务管控 |
| | | 现场开发管控 |
| 6 | 关键信息资产管控 | 资产管理 |
| | | 资产维修报废管理 |
| 7 | 工业控制系统建设安全管理 | 上线安全测评 |
| | | 产品采购和使用 |
| | | 核心产品采购测试 |
| 8 | 网络安全防护 | 网络架构安全 |
| | | 控制网边界防护 |
| | | 网络安全审计 |
| | | 网络冗余和容差策略 |
| | | 远程访问 |
| | | 移动终端安全接入 |

**表 B.1（续）**

| 序号 | 检查类 | 检查项 |
|---|---|---|
| 9 | 上位机主机和设备安全防护 | 补丁更新 |
| | | 恶意代码防护 |
| | | 系统安全整改加固 |
| | | 移动存储介质管理 |
| | | 上位机终端管控 |
| | | 主机和设备账号口令管理 |
| 10 | 物理环境安全防护 | 机房安全建设 |
| 11 | 运行安全管理 | 日常维护 |
| | | 安全审计 |
| | | 补丁管理 |
| | | 安全监测 |
| 12 | 应急管理 | 信息通报 |
| | | 应急预案制定 |
| | | 应急演练 |
| | | 应急资源配备 |
| | | 事故调查 |

## 参 考 文 献

[1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[2] GB/T 20984—2007 信息安全技术 信息安全风险评估规范
[3] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[4] 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)
[5] IEC/TS 62443-1 Terminology,concepts and models
[6] IEC/TR 62443-2 Establishing an industrial automation and control system security program
[7] IEC/TR 62443-3 Operating a manufacturing and control systems security program
[8] IEC/TR 62443-4 Specific security requirements for manufacturing and control systems
[9] IEC 62443-5 Security technologies for industrial automation and control systems
[10] NIST SP 800-82—2011 Guide to Industrial Control Systems(ICS) Security