ICS 25.040
L 70
备案号：46298-2015

DB32

江　苏　省　地　方　标　准

DB32/T 2765-2015

工业控制系统信息安全管理监督检查工作规范

Supervision and inspection specification for information security management of industrial control systems

2015-06-15 发布　　2015-08-15 实施

江苏省质量技术监督局 发布

目　次

前　言

本规范依据 GB/T 1.1-2009《标准化工作导则　第 1 部分：标准的结构和编写》编写。

本标准附录 A 是规范性附录。

本规范由江苏省经济和信息化委员会提出并归口。

本规范起草单位:江苏省电子信息产品质量监督检验研究院(江苏省信息安全测评中心)。

本规范起草人：黄申、吴兰、张腾标、李国琴、程恺、王坤、赵川、赵兆。

引　言

工业控制系统广泛应用于工业生产、电力设施、水利油气、交通运输和市政等领域，用以控制生产设备的运行。随着计算机和网络技术的发展，特别是我国信息化与工业化深度融合工作的不断推进，以及物联网等新一代信息技术的快速发展，工业控制系统产品越来越多地采用通用协议、通用硬件和通用软件，以各种方式与互联网等公共网络连接，病毒、木马等威胁正在向工业控制系统扩散，工业控制系统信息安全问题随之日益突出，如何保障工业控制系统信息安全已经成为国家战略问题。

工业控制系统信息安全管理监督检查是帮助各重点领域工业控制系统运营、管理、维护和使用等部门充分认识工业控制系统信息安全重要性和紧迫性的重要手段，是切实加强工业控制系统信息安全管理保障工作的基础和重要环节。

工业控制系统信息安全管理监督检查工作规范

1 范围

本标准规定了工业控制系统信息安全管理监督检查工作的术语和定义、检查对象、检查目的、检查形式、检查方法、检查原则、检查流程和检查内容。

本标准适用于规范工业控制系统的运营、使用、维护、管理等部门开展的工业控制系统信息安全管理监督检查工作。

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 26333 工业控制网络安全风险评估规范

GB/T 26802.1 工业控制计算机系统 通用规范 第1部分：通用要求

GB/T 30976.1 工业控制系统信息安全 第1部分：评估规范

GB/T 30976.2 工业控制系统信息安全 第2部分：验收规范

DB32/T 2289 重点领域工业控制系统信息安全保护基本要求

3 术语和定义

GB/T 26333 和 DB32/T 2289 界定的及下列术语和定义适用于本标准。

3.1

工业控制系统 industrial control systems

在工业和关键基础设施领域，采用数据采集监控、分布式控制、过程控制、可编程逻辑控制等技术监测和控制生产设备运行的控制系统，包括监控和数据采集（SCADA）系统、分布式控制系统（DCS）、可编程逻辑控制器（PLC）等。

3.2

工业控制系统信息安全管理监督检查 information security management supervision and inspection in industrial control systems

工业控制系统的运营、使用、维护、管理等部门依据国家相关政策法规、信息安全技术和管理标准，依法对重点领域工业控制系统的信息安全管理进行监督检查，并对其监督检查结果依法进行处理的活动。

3.3

强反馈 strong feedback

电子信息系统自身不具备直接操控工业控制系统的能力，但其传递的数据会导致工业控制系统发生重大调整和变化，从而可能间接控制工业控制系统的能力。

4 符号和缩略语

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）
IT　　信息技术（Information Technology）
SNMP　简单网络管理协议（Simple Network Management Protocol）
VPN　　虚拟专用网（Virtual Private Network）

5 总则

5.1 监督检查对象

江苏省行政区域内各重点领域工业控制系统，主要包括核设施、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领域的工业控制系统，但不包括涉及国家秘密的工业控制系统。

5.2 监督检查目的

工业控制系统信息安全管理监督检查的目的通常包括以下几个方面：

——规范重点领域工业控制系统信息安全管理的监督检查工作，保障工业控制系统的安全、稳定运行；

——指导监督检查方和被检查方开展工业控制系统信息安全管理监督检查工作，提升监督检查的质量和效率；

——帮助重点领域工业控制系统的运营、使用、维护、管理等相关部门充分认识工业控制系统信息安全管理的重要性和紧迫性，增强风险意识和责任意识；

——准确了解重点领域工业控制系统的信息安全管理现状和可能存在的安全威胁；

——明确重点领域工业控制系统的信息安全管理需求，制定安全策略和安全解决方案；

——通过监督检查工作的实施，着力培养专业的工业控制系统安全队伍和专业人才。

5.3 监督检查形式

5.3.1 自查

各重点领域工业控制系统主管单位依据工业控制系统信息安全管理监督检查工作规范及其他信息安全技术和管理规范，对运维或使用工业控制系统的下属单位、内设机构自行组织实施的监督检查活动。

自查是保障工业控制系统信息安全的基础。通过对本单位工业控制系统信息安全管理情况开展自查，了解和掌握工业控制系统的信息安全管理现状及存在的安全隐患，督促被检查方落实安全整改和加固措施，切实加强和保障工业控制系统的信息安全管理工作。

5.3.2 抽查

省、市信息化主管部门联合行业主管部门或监管部门、国有资产监督管理部门等单位，依据工业控制系统信息安全管理监督检查工作规范及其他信息安全技术和管理规范，对各自行政区域内重点领域工业控制系统的主管、运维或使用单位共同组织实施的监督检查活动，旨在监督检查各重点领域工业控制系统主管、运维或使用单位是否已开展自查，工业控制系统信息安全管理基本措施落实情况，工业控制系统关键领域或关键点是否存在重大安全隐患，以及其信息安全风险是否在可接受的范围内。

5.4 监督检查方法

监督检查方法是监督检查人员在工业控制系统信息安全管理监督检查工作过程中以获取检查证据或检查结果所使用的方法，主要包括人员访谈、人工查验和技术测试等方法。

人员访谈是监督检查人员通过引导工业控制系统相关人员进行有目的和有针对性的交流以帮助其理解、分析和获取检查证据或结果的过程。人工查验是监督检查人员在监督检查过程中采取文档查阅、现场观察、实地查验、设备配置核查等方式分析、评估和掌握工业控制系统安全属性的过程。技术测试是监督检查人员使用专业成熟的测试工具、技术手段和操作方法，对工业控制系统进行扫描、测试以验证其安全状况的过程。

5.5 监督检查原则

为保证监督检查的质量和检查结果的客观性、准确性，工业控制系统信息安全管理监督检查工作遵循以下原则：

5.5.1 可控性原则

在监督检查的实施过程中，主要从人员可控性、工具可控性和过程可控性三个方面对监督检查工作进行监管，以确保整个监督检查工作过程的可控性。

监督检查的所有实施人员应经过严格的身份背景、专业资格和资质审查，具备相关领域的学习或工作经历、专业知识和技能，签署保密协议，确保人员可控。

监督检查实施过程中使用的专业工具应经过相关部门的认证和认可，确保工具可控。

监督检查的实施应具有相应的过程控制规程和质量保证要求，确保过程可控。

5.5.2 保密性原则

监督检查实施人员均应签署保密协议，对监督检查工作中产生的过程数据和结果数据严格保密，未经授权不得泄露和利用。

5.5.3 整体性原则

在监督检查的实施过程中，严格按照与被检查方约定的监督检查范围和检查内容进行全面检查，避免由于遗漏或越界检查造成潜在的安全隐患。

5.5.4 最小影响原则

从管理层面和技术工具层面，将监督检查工作对被检查方的工业控制系统和网络的正常运行可能造成的影响或干扰，降至最低。

6 监督检查流程

工业控制系统信息安全管理监督检查的实施流程如图1所示。

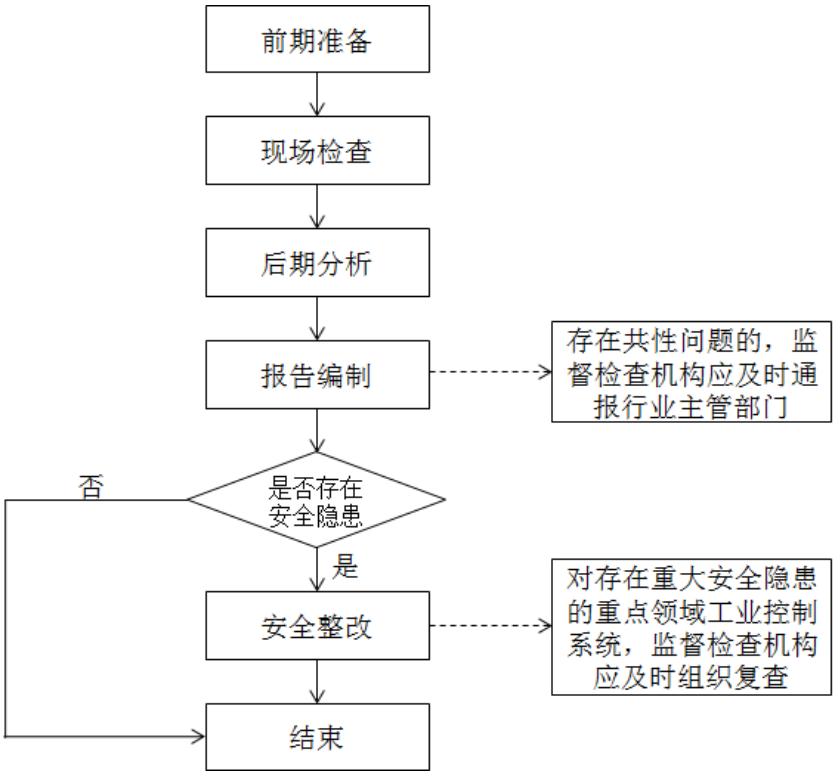

图 1　工业控制系统信息安全管理监督检查流程

6.1 前期准备

前期准备是整个工业控制系统信息安全管理监督检查过程有效性的前提和保证。因此，在监督检查活动正式实施前，应：

a） 确定监督检查的目标；
b） 确定监督检查的范围；
c） 组建监督检查管理与实施团队；
d） 开展前期系统调研；
e） 明确监督检查依据；
f） 制定监督检查方案；
g） 获得最高管理者对监督检查工作的支持。

6.1.1 确定目标

在满足和保障组织业务稳定持续发展的前提下，明确其在工业控制系统信息安全管理方面的需求、法律法规的符合性等内容，识别现有工业控制系统信息安全管理上的不足或存在的安全威胁，以及可能造成的影响或危害。

6.1.2 确定范围

工业控制系统信息安全管理监督检查范围可以是组织全部的信息及与信息处理相关的各类资产、管理机构，也可以是某个独立的工业控制系统、关键业务流程、与工业控制系统相关的系统或部门等。

6.1.3 组建团队

监督检查实施团队，由管理层、相关业务骨干、IT 技术工程师等人员组成监督检查实施小组，设立项目负责人一名。必要时，可组建由监督检查方、被检查方领导和相关部门负

责人参加的监督检查领导小组，或聘请相关专业的技术专家和技术骨干组成专家小组。

监督检查实施团队应做好评估前的表格、文档、检测工具等各项准备工作，开展工业控制系统检查实施工作的技术培训和保密教育，制定监督检查实施过程管理的相关规定。可根据被检查方要求，双方签署保密合同，或适情签署个人保密协议。

6.1.4 系统调研

系统调研是确定具体被检查对象的过程。监督检查小组应进行充分的系统调研，为监督检查依据和方法的选择、检查内容的实施奠定基础。调研内容至少应包括：

a） 主要业务功能、业务范围和业务流程；
b） 网络结构与网络区域划分，包括内部连接和外部连接；
c） 系统边界，与其他系统的连接情况；
d） 主要的软、硬件资产；
e） 系统和数据的敏感性；
f） 维护和使用系统的人员；
g） 管理制度、操作规程等文档。

系统调研采取问卷调查为主、现场访谈为辅的方式进行，在问卷调查不能完全达到系统调研目的的情况下，可结合现场访谈的方式进行。调查问卷是提供一套关于系统资产或管理相关的表格，供被检查方的系统技术或管理人员填写；现场访谈则是由监督检查人员到现场观察、了解并收集系统在物理、环境和操作等方面的相关信息。

6.1.5 确定依据

根据前期的系统调研结果，并依据业务实施对系统安全运行的需求，确定监督检查的依据和方法，使之能够与组织的环境和安全要求相适应。监督检查依据包括（但不仅限于）：

a） 国家法律、法规及有关规定；
b） 现有国际标准、国家标准、行业标准、地方标准和按规定程序备案的企业标准等；
c） 行业主管部门针对业务系统制定的要求和规定；
d） 系统的安全保护等级要求；
e） 系统互联单位的安全要求；
f） 系统本身的实时性或性能要求等。

6.1.6 制定方案

制定监督检查方案的目的是为后期的监督检查实施活动提供一个总体计划，用于指导监督检查实施小组开展后续的检查工作。监督检查方案的内容一般包括（但不仅限于）：

a） 安全检查计划：监督检查各阶段的具体检查计划，包括检查目标、检查内容、检查范围、检查形式、检查交付成果等内容；
b） 实施团队组织：包括监督检查团队成员组成、成员角色与定义、成员职责等内容；
c） 时间进度安排：监督检查工作实施的时间进度安排。

6.1.7 获得支持

在确定上述内容的基础上，应形成科学合理和较为完整的监督检查实施方案，并得到组织最高管理者的支持和批准；及时向监督检查实施小组内的所有人员进行传达，明确相关人员在监督检查实施过程中的任务和责任，并就监督检查的相关内容开展培训和保密教育。

6.2 现场检查

6.2.1 首次会议

在现场检查正式实施前，检查实施方与被检查方应共同召开本次监督检查工作的首次会议，参会人员应包括：

a） 被检查方的管理层领导或负责人；

b） 双方的项目负责人；

c） 监督检查实施小组的所有成员；

d） 被检查方相关部门的中层领导或负责人；

e） 系统使用和维护人员等。

在首次会议上，被检查方的管理层领导或负责人应明确表示对本次监督检查工作的大力支持，以确保监督检查工作的参与人员在检查实施过程中全力配合，从而保证监督检查实施的质量和效果，确保监督检查工作的顺利开展。

在首次会议上，监督检查方的项目负责人根据前期所确定的检查实施方案，介绍监督检查工作的大体流程、检查的目的与范围、检查工作的实施方法、工作交付成果等信息，与被检查方确认检查实施时间和检查计划、人员配合与沟通渠道，并向被检查方提供询问的机会，使与会人员能够对即将开始的监督检查工作有一个清晰、全面的认识。

首次会议结束后，被检查方的与会相关领导或负责人应及时将首次会议的主要内容有效传达给相关部门和人员。

6.2.2 检查实施

在现场检查的实施过程中，结合人员访谈、现场观察、实地查验、配置核查、文档审查、工具扫描等方式，监督检查人员应按照附录 A 的检查内容和检查条款进行逐项检查，对照被检查工业控制系统的实际安全状况如实、准确填写检查结果，形成检查结果原始记录，为后续的结果分析做准备。

监督检查实施的具体内容和实施要求详见本标准第 6 部分。

6.2.3 过程控制

监督检查实施小组成员应严格按照监督检查方案和实施计划开展现场检查工作。必要时，为了更好地达到检查目的或适应实际环境变化的需求，可适当调整检查计划，及时告知并与双方相关人员进行商榷，直到得到相关人员的认同。

监督检查项目负责人应及时与被检查方的相关人员交换意见，对已收集获取的检查证据进行确认。对于被检查方存有异议的检查结果，应采取检查核对的方法进行再次确认。当收集到的检查证据不能达到检查目的时，应及时向被检查方报告理由，并商定相应的解决措施，包括调整检查计划，以及改变检查目的、检查范围等。

6.2.4 末次会议

在完成现场检查实施后，检查方与被检查方应共同召开本次监督检查工作的末次会议，除参与首次会议的各方人员外，与会人员还包括监督检查实施过程中被访谈对象、被调查对象以及其他相关参与人员。

在末次会议上，监督检查方的项目负责人根据现场检查的实施情况，向被检查方报告监督检查中发现的具体问题和整体检查结果。

6.3 后期分析

检查方应根据现场收集获取的信息和检查结果原始记录，对被检查工业控制系统的实际安全管理情况进行梳理和汇总，分析被检查工业控制系统面临的安全威胁和安全风险情况，评估其是否存在严重安全隐患，根据检查分析评估结果形成检查结论。在对工业控制系统的检查证据和结果进行分析评估时，应按照附录 A 的结果分析方法对被检查工业控制系统的风

险情况进行分析与评估。

6.4 报告编制

检查方应在规定时间内编制完成监督检查报告，反馈给被检查方。对监督检查过程中发现的共性问题，监督检查机构应及时通报行业主管部门，并协助其开展信息安全管理咨询、业务培训及安全整改工作。

工业控制系统信息安全管理监督检查报告应清晰、准确、客观地给出监督检查的实施情况、检查结果和相关内容，说明被检查工业控制系统存在的安全隐患和缺陷，并给出改进建议。

工业控制系统信息安全管理监督检查报告至少应包含以下内容：

——检查系统名称；

——系统主管部门；

——检查时间和地点；

——监督检查依据；

——监督检查结论；

——报告编制人；

——报告审核人；

——报告批准人；

——检查结果汇总表；

——安全整改建议；

——检查实施机构的公章。

工业控制系统信息安全管理监督检查报告应附封面，封面注明报告标题、统一的报告编号、检查系统名称、系统主管部门和检查实施机构。

6.5 安全整改

工业控制系统经检查发现存在安全隐患的，其主管、运维或使用单位应尽快组织实施安全整改工作，并及时向所在地信息化主管部门及行业主管部门报告整改情况。

对存在重大安全隐患的重点领域工业控制系统，通知被检查单位立即采取防护措施实施安全整改。监督检查方应及时对其安全整改情况进行复查，对已采取的安全整改措施应进一步考虑是否引入新的安全问题并进行检查和分析，督促其改进和完善信息安全管理技术措施。对于安全整改实施不到位的工业控制系统，要求被检查方继续进行安全整改。

6.6 结束

检查方通过现场检查和后期分析后确认被检查方工业控制系统不存在安全隐患的，或经安全整改后确认被检查方工业控制系统的安全风险在可控范围内的，结束监督检查工作。

7 监督检查内容

7.1 组织制度管理

7.1.1 组织管理

7.1.1.1 检查内容

应设立工业控制系统信息安全管理工作的职能部门，设置信息安全管理岗位，配备相应的安全管理人员，并指定安全管理负责人，明确部门、岗位和人员的职责分工。

7.1.1.2 检查实施

本项检查要求包括：

a） 应访谈业务主管或系统负责人，询问是否设立工业控制系统信息安全管理工作的职能部门，组织内的部门设置情况，是否明确各部门的职责分工；

b） 应访谈业务主管或系统负责人，询问是否设置信息安全管理岗位，设置了哪些信息安全管理岗位，各个信息安全管理岗位的职责分工是否明确；

c） 应访谈业务主管或系统负责人，询问是否指定信息安全管理各个方面的负责人，是否明确各个负责人的工作职责；

d） 应访谈业务主管或系统负责人、各个信息安全管理人员、信息安全管理各个方面的负责人，询问其岗位、人员职责包括哪些内容；

e） 应查阅部门、岗位、人员的职责分工文件，查看文件内容是否明确安全管理职能部门的职责；是否设置信息安全管理岗位、信息安全管理各个方面的负责人，明确定义岗位和人员的职责分工；

f） 应访谈业务主管或系统负责人，询问是否将部门、岗位、人员的职责分工文件有效传达给了所有相关人员，通过何种方式进行有效传达；

g） 应询问和检查信息安全管理部门和信息安全管理人员及负责人是否具有执行日常管理活动的相关文件或工作记录。

7.1.2 人员管理

7.1.2.1 检查内容

本项检查内容包括：

a） 应建立包括人员录用流程、标准、要求、方式和保密协议等在内的人员录用制度；

b） 应建立包括人员离岗剩余信息保护、资产归还、保密承诺等在内的人员离岗制度；

c） 应建立包括人员考核指标、考核方式、考核对象、考核内容等在内的人员考核制度；

d） 应建立包括人员培训计划、培训周期、培训对象、培训内容等在内的人员培训制度；

e） 应指定专职信息安全员，建立信息安全员的培训与交流计划；

f） 应建立包括外部人员访问条件、访问范围、访问控制措施、保密要求等在内的外部人员管理制度。

7.1.2.2 检查实施

本项检查要求包括：

a） 应访谈安全主管或人事负责人，询问是否制定包括人员录用流程、标准、要求、方式等在内的人员录用制度，人员录用流程和方式如何，人员录用包括哪些标准和要求；人员录用后是否与其签署保密协议，是否对其说明保密职责；

b） 应查阅人员录用制度文件，查看是否包含人员录用流程、标准、要求、方式等内容；检查保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容；

c） 应访谈安全主管或人事负责人，询问是否制定包括人员离岗剩余信息保护、资产归还、保密承诺等在内的人员离岗制度，是否及时终止离岗人员的所有访问权限，是否及时取回各种身份证件、钥匙等物件，以及机构提供的软硬件设备等；

d） 应查阅人员离岗制度文件，查看是否包含人员离岗剩余信息保护、资产归还等内容；查看是否具有相关资产归还的记录等证明文件；

e） 应访谈安全主管或人事负责人，询问人员离岗手续包括哪些，是否要求关键岗位人员承诺相关保密义务后方可调离；

f） 应查看是否具有按照人员离岗程序办理的离岗手续文件；查阅保密承诺文档，查看是否有调离人员的签字；

g） 应访谈安全主管或人事负责人，询问是否制定包括人员考核指标、考核方式、考核对象、考核内容等在内的人员考核制度，是否有人负责定期对各个岗位人员进行安全技能及安全知识的考核，如何考核，考核周期多长，考核对象和内容包括哪些；

h） 应检查考核记录，查看记录的考核人员是否包括各个岗位的人员，考核内容是否包含安全知识、安全技能等；查看考核记录日期与考核周期是否一致；

i） 应访谈安全主管或人事负责人，询问是否制定包括人员培训计划、培训周期、培训对象、培训内容等在内的人员培训制度，以什么形式进行，效果如何；是否对考核结果进行记录并归档保存；

j） 应检查人员培训记录，查看是否有培训人员、培训内容、培训结果等方面的描述；查看培训记录与培训计划是否一致；

k） 应访谈安全主管或人事负责人，询问是否指定至少一名专职信息安全员，制定信息安全员培训、交流计划；

l） 应检查信息安全员职责文件和信息安全员培训计划，查看是否与上述情况相符；

m） 应访谈安全主管或人事负责人，询问是否建立了外部人员访问管理文档，针对外部人员的访问采取了哪些安全措施，外部人员的访问是否需要经过有关部门或负责人的正式批准，是否由专人全程陪同或监督，是否进行记录并存档管理；

n） 应检查外部人员访问管理文档，查看是否明确规定了外部人员的访问条件、访问范围、访问控制措施、保密等相关管理要求；检查外部人员访问登记记录，查看是否记录了外部人员访问重要区域的访问者个人信息（至少包括姓名、工作单位、联系方式）、进入时间、离开时间、访问区域、访问及操作内容、陪同人等。

7.1.3 资产管理

7.1.3.1 检查内容

本项检查内容包括：

a） 应建立包括工业控制系统软硬件、文档、资料、工具等在内的资产安全管理规定和资产清单，资产清单中应包括资产责任部门、保管人员、所处位置、重要程度、资产编号、采购日期、型号版本等信息；

b） 应明确工业控制系统资产管理的责任部门，指定专人负责工业控制系统资产管理，详实记录资产管理相关情况。

7.1.3.2 检查实施

本项检查要求包括：

a） 应访谈资产管理员，询问是否建立包括工业控制系统软硬件、文档、资料、工具等在内的资产安全管理规定；

b） 应检查资产安全管理规定文档，查看其是否包括工业控制系统软硬件、文档、资料、工具等资产，是否覆盖资产使用、借用、维护等方面的规定内容；

c） 应访谈资产管理员，询问是否编制工业控制系统相关资产的资产清单，资产清单是否覆盖资产责任部门、保管人员、所处位置、重要程度、资产编号、采购日期、型号版本等方面内容；

d） 应检查资产清单，查看其内容是否覆盖资产责任部门、保管人员、所处位置、重要程度、资产编号、采购日期、型号版本等方面内容；

e） 应访谈资产管理员，询问是否指定资产管理的责任部门，是否指定专人负责工业控制系统资产的管理，具体由何部门/何人负责；

f） 应检查资产清单中的设备，查看其是否具有相应的资产编号与标识，标识是否清晰可见，且不易去除。

7.1.4 应急管理

7.1.4.1 检查内容

本项检查内容包括：

a） 应制定工业控制系统信息安全事件应急预案，明确应急组织领导、应急处置流程、应急支撑队伍、应急资源保障、事后总结教育等内容；

b） 应对工业控制系统中的关键设备保有备机备件；

c） 应进行应急预案培训，定期开展应急演练，对应急演练过程进行记录和总结。

7.1.4.2 检查实施

本项检查要求包括：

a） 应访谈业务主管或系统负责人，询问是否制定工业控制系统信息安全事件应急预案，是否明确应急组织领导、应急处置流程、应急支撑队伍、应急资源保障、事后总结教育等内容；

b） 应查阅工业控制系统信息安全事件应急预案文档，查看其内容是否覆盖应急组织领导、应急处置流程、应急支撑队伍、应急资源保障、事后总结教育等方面，且操作可行；

c） 应访谈业务主管或系统负责人，询问是否对工业控制系统的关键设备保有备机备件，如何保证备机备件在应急时能够正常工作；

d） 应访谈业务主管或系统负责人，询问是否开展应急预案培训，培训人员包括哪些；是否定期开展应急演练，演练周期有多长，是否对应急演练过程进行记录并存档，是否对应急演练进行总结并改进应急预案；

e） 应检查是否具有应急预案培训记录、应急预案演练记录和应急处置记录。

7.2 连接管理

7.2.1 网络与系统接入管理

7.2.1.1 检查内容

本项检查内容包括：

a） 工业控制系统应具有网络结构拓扑图，并与实际部署情况一致；工业控制系统网络边界清晰；

b） 应详细登记工业控制系统与公共网络、办公网络之间的所有连接，断开所有不必要连接；

c） 工业控制系统与公共网络、办公网络之间应部署强隔离设备（如硬件防火墙等）；工业控制系统网络边界隔离设备的安全控制策略应符合实际安全要求；

d） 工业控制系统及设备应未非法连接其他网络；

e） 工业控制系统与电子信息系统之间应不存在无必要的关联，必要关联的电子信息系统应运行良好、安全可控，对特别重要的关联电子信息系统进行封闭式风险评估，其安全风险在可接受范围内；

f） 电子信息系统应由明确的工业控制系统安全管理部门进行管理和控制；

g） 电子信息系统对工业控制系统应不具备直接控制、强反馈等操控能力；
h） 电子信息系统与工业控制系统之间应有严格的互相识别、认证机制，如设备标识、身份鉴别、访问控制、地址隐藏、资源限制等。

7.2.1.2 检查实施

本项检查要求包括：

a） 应检查工业控制系统的网络结构拓扑图，查验是否与网络拓扑的实际部署情况一致；工业控制系统的网络边界是否清晰；
b） 应访谈网络管理员，询问是否详细登记工业控制系统与公共网络、办公网络之间的所有连接，是否已断开所有不必要连接；
c） 应检查网络连接登记信息，对涉及连接公共网络、办公网络的事项进行必要性评估；
d） 应访谈网络管理员，询问工业控制系统是否与公共网络、办公网络之间部署强隔离设备，部署的安全设备包括哪些；
e） 应检查工业控制系统网络边界隔离设备的安全控制策略配置情况，是否满足实际安全要求；
f） 应查验现场无线信号覆盖情况；查验工业控制系统主要设备的网络连接痕迹，是否存在违规外联的情况；
g） 应访谈业务主管、网络管理员，询问电子信息系统是否由工业控制系统安全管理部门负责管理和控制，具体由何部门负责管理；
h） 应访谈业务主管、网络管理员，查阅业务流程图，了解和查验电子信息系统功能、对工业控制系统的实际操控能力情况；
i） 应访谈业务主管、信息管理员，询问电子信息系统的信息安全测评工作开展情况，做过哪些安全测评，测评周期为多长，是否完成安全整改工作；
j） 应查阅电子信息系统的风险评估、等级测评以及安全整改报告等文档，评估其安全风险是否在可接受范围内；
k） 应访谈业务主管、信息管理员，询问电子信息系统与工业控制系统之间是否具有严格的互相识别、认证的安全机制，采取的安全机制有哪些，安全效果如何；
l） 应查阅系统设计文档，查验相互识别与认证的安全措施。

7.2.2 移动存储介质管理

7.2.2.1 检查内容

本项检查内容包括：

a） 应建立工业控制系统移动存储介质管理制度，对可接入移动存储介质进行登记管理，规范移动存储介质的使用、维护和销毁过程；
b） 工业控制系统主要设备应采取技术措施，限制或封堵所有不必要接口，使得未登记移动存储介质无法在工业控制系统中直接插拔或读取数据；
c） 工业控制系统的主要设备应设置禁止移动存储介质自动播放策略，明确专人对设备清单中的移动存储介质定期进行病毒木马查杀。

7.2.2.2 检查实施

本项检查要求包括：

a） 应访谈资产管理员，询问是否对移动存储介质的使用和管理要求制度化和文档化；
b） 应查阅介质安全管理制度、移动存储介质设备清单、移动存储介质使用记录等文档，检查是否对移动存储介质的存放环境、使用、维护和销毁等方面作出规定，是否进