ICS 35. 040
L 80
备案号：

天 津 市 商 用 密 码 团 体 标 准

T/TCCIA 0005-2024

信息安全技术
工业物联网安全等级评价机制

Information security technology

Industrial Internet of Things security rating mechanism

天津市商用密码行业协会 发布

目录

前　　言

本文件根据 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由天津市信息安全标准化技术委员会归口。

本文件起草单位：XXX。

本文件主要起草人：XXX。

引　言

依据《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)文件要求制定本标准。

随着工业控制系统和信息化技术的融合，工业控制系统广泛应用于冶金、电力、石化、水处理、铁路、航空和食品加工等行业。工业控制系统指应用于工业控制领域的数据采集、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。某些国家和地区，把工业控制系统信息安全作为信息安全保障的一个相对独立的体系进行建设，其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使用工业物联网系统的行业进行信息安全建设以及国家政府机构对国家重点行业进行信息安全检查中选择和指定的安全控制提供评价准则。本标准制定的目标是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估工作，及时有效发现工业物联网系统存在的突出问题，为国家对重点行业工业控制信息安全检查等工作提供支撑，为实现更安全的工业物联网系统并在其内部进行有效的安全管理提供帮助。

本标准主要为第三方安全检测评估机构在工业控制系统现场实施风险评估提供指南，也可供工业控制系统业主单位进行自评估时参考。

1 范围

本标准对工业控制系统安全的定义、目标、原则和工业控制系统资产面临的安全进行了描述，同时，本标准规定了对工业控制系统安全进行安全评估的要素及要素间的关系、实施过程、工作形式、遵循的原则、实施方法，在工业控制系统生命周期不同阶段的不同要求及实施要点。

本标准适用于指导第三方检测评估机构在工业控制系统现场的安全评估实施工作，也可供工业控制系统业主单位进行自评估时参考。

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 20984-2022《信息安全技术信息安全风险评估方法》

GB/T 32919-2016《信息安全技术工业控制系统安全控制应用指南》

ISO/IEC62264-1-2013 《企业控制系统综合--第1部分：模型和术语》

GB/T 22239-2019 《网络安全等级保护基本要求》

GB/T 39786-2021 《信息安全技术信息系统密码应用基本要求》

3 术语、定义和缩略语

3.1 术语、定义

GB/T 20984-2022中界定的以及下列术语和定义适用于本文件。

3.1.1 SCADA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。

3.1.2 分布式控制系统 DCS 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。

3.1.3 主终端单元 MTU master terminal unit

一般部署在调度控制中心，作为工业控制系统主站，主要用于生产过程的信息收集和监测。

3.1.4 远程终端单元 RTU remote terminal unit

用于监测、控制远程工业生产装备的各类设备的统称，作为工业控制系统的远程站点。

3.1.5 可编程逻辑控制器 PLC 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。

3.1.6 智能电子设备 IED intelligent electronic device

一般部署在管网站场，主要用于生产过程的信息采集、自动测量记录和传导，通过网络与MTU保持通信。

3.1.7 人机界面 HMI human-machine interface

为操作者和控制器之间提供操作界面和数据通信的软硬件平台。

3.2 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 监视控制与数据采集系统（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）

PCS 过程控制系统（Process Control System）

RTU 远程终端设备（Remote Terminal Unit）

MTU 主终端设备 （Master Terminal Unit）

DRP 灾难恢复计划（Disaster Recovery Planning）

ACL 访问控制列表（Access Control List）

DNS 域名系统（Domain Name System）

DHCP 动态主机配置协议（Dynamic Host Configuration Protocol）

DNP 分布式网络协议(Distributed Network Protocol）

RPC 远程过程调用协议（Remote Procedure Call Protocol）

DCOM 分布式组件对象模式（Microsoft Distributed Component Object Model）

OPC 用于过程控制的对象连接与嵌入(Object Linking and Embedding for Process Control)

PAD 个人数字助手，又称掌上电脑（Personal Digital Assistant）

DoS 拒绝服务(Denial of Service)

4 标准概述

4.1 标准设计

本标准研究关于工业控制系统安全检查内容及要求的广泛定义及概况，研究主要包括工业控制系统信息安全检查的关键安全要求，以及工业控制系统信息系统安全评估的方法、流程和方案。为安全检查要求的实施提供一般性指导，适用于工业控制系统环境下加强信息系统安全自查及管理；为使用工业控制系统的行业进行信息安全建设以及国家政府机构对国家重点行业进行信息安全检查中选择和制定的安全控制提供准则。

本标准从技术、管理和工程三个层面对安全检查要求进行扩展，为国家工业控制系统信息安全的类似标准提供补充，研究每个方面对工业控制网络应用软件安全性的影响程度。

4.2 评价机制实施的目的及原则

4.2.1 实施的目的

工业控制系统评价机制实施的目的是通过对工业控制网络应用软件进行安全评估，来加强工业控制系统的安全防护能力，确保工业控制系统的安全性和可靠性。

4.2.2 实施的基本原则

工业控制系统安全评估实施的基本原则包括：

a） 最小影响原则是：工业控制网络应用软件的安全评估，应采用最小影响原则，即首要保障在线系统的稳定运行，避免对其进行攻击性的测试。可能对系统造成影响的评估测试项，评估方需与被评估方沟通，选择于工业控制系统不在线时间、模拟仿真环境中进行测试，同时将攻击可能造成的不可逆损坏告知被评估方；

b） 可控性原则是：

1） 人员与信息可控性，所有参与评估人员应签署保密协议，以保证项目信息的安全；应对工作过程数据和结果数据严格管理，未经授权不得泄露给任何单位和个人；

2） 过程可控性，应按照项目管理要求，成立项目实施团队，项目组长负责制，达到项目过程的可控；

3） 工具可控性，评估人员所使用的评估工具应该事先通告用户，并在评估实施前获得被评估方织的许可。

5 安全评估实施

5.1 评估准备

5.1.1 评估准备概述

安全评估的准备是整个安全评估过程有效性的保证。实施安全评估是一种战略性的考虑，其结果将受到业务战略、业务流程、安全需求、工业控制系统规模和结构等方面的影响。为保证整个安全评估过程的有效性，评估方应到工业控制系统现场进行沟通交流，条件不允许的情况下，可通过邮件、电话、电子邮件等不同方式进行沟通交流。图1是工业控制系统安全评估准备工作流程图。

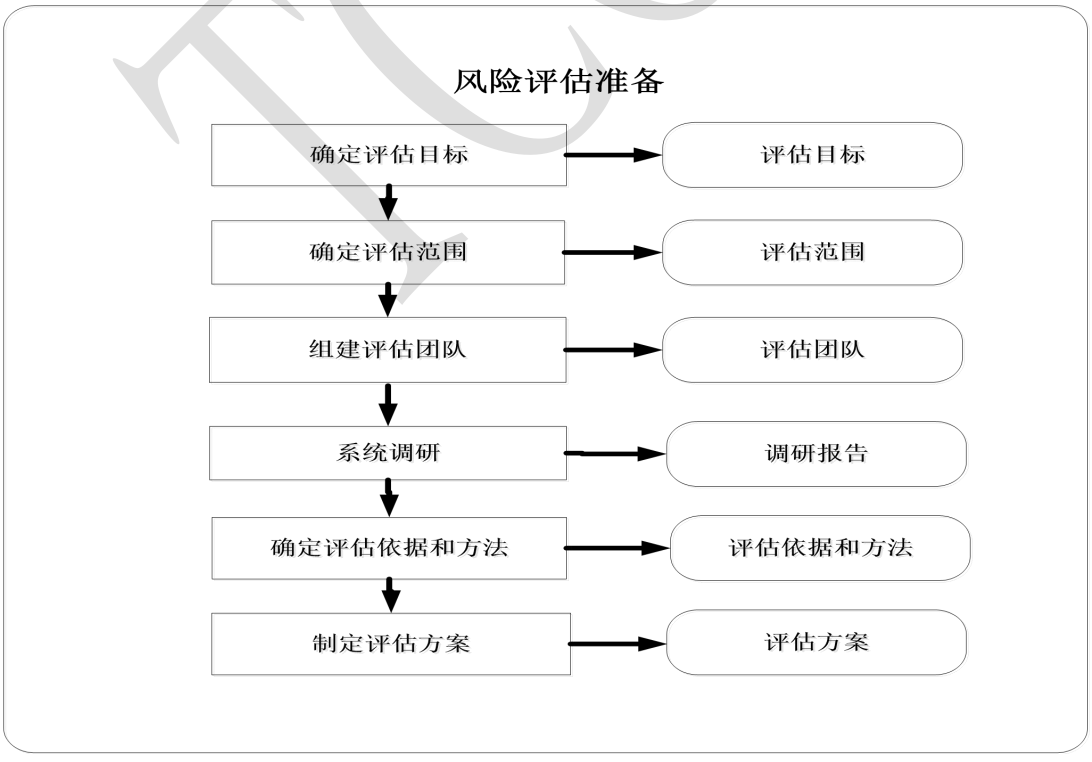

图 1 安全评估准备工作流程

实施指南如下：

a） 确定安全评估的目标；

b） 确定安全评估的范围；

c） 组建适当的评估管理与实施团队；

d） 进行系统调研；

e） 确定评估依据和方法，制定方案。

5.1.2 确定目标

安全评估应贯穿于工业控制系统生命周期的各阶段中，由于工业控制系统生命周期各阶段中安全评估实施的内容、对象、安全需求均不同，因此评估方应首先根据当前工业控制系统的实际情况来确定在工业控制系统生命周期中所处的阶段，并以此来明确安全评估目标，如图2所示。

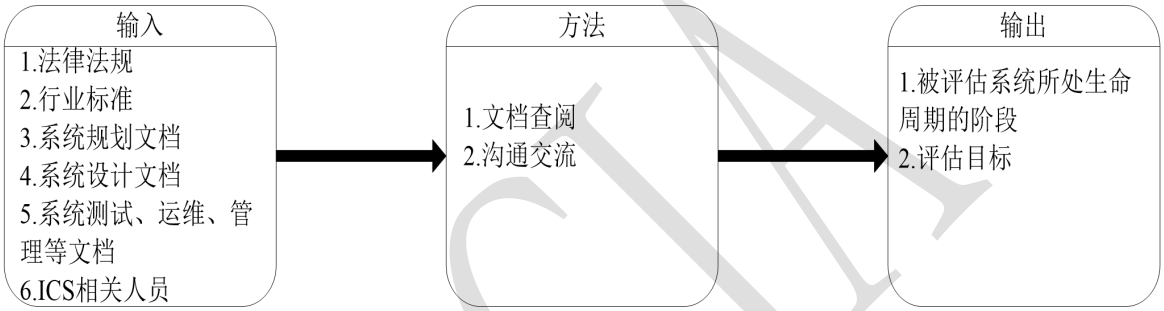

图 2 确定评估目标

实施指南如下：

a） 评估方应根据输入的文档材料及对相关人员的访谈，分析研判出工业控制系统现在所处的生命周期；

b） 确定其所处的生命周期之后，参见本标准第 6 章内容，确定评估目标。

5.1.3 确定范围

安全评估实施范围是评估方工作的范围，确定评估范围如图3所示。

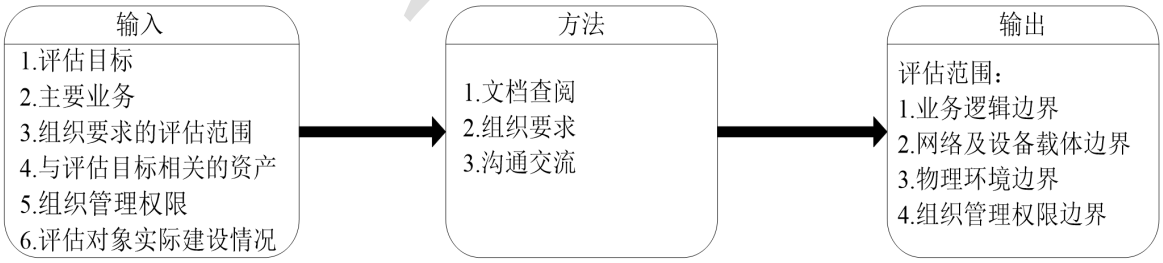

图 3 确定评估范围

实施指南如下：

a） 评估方应了解工业控制系统所处的工业控制安全基线级别，参见GB/T32919-2016《信息安全技术工业控制系统安全控制应用指南》；

b） 评估方应了解组织要求评估的范围和组织的实际工业控制系统建设情况；

c） 安全评估实施范围应包括组织工业控制系统相关的资产、管理机构，关键业务流程等；

d） 评估方应结合已确定的评估目标、组织要求评估的范围和组织的实际工业控制系统建设情况，合理定义评估对象和评估范围边界。

5.1.4 组建团队

评估方应由工业控制系统专业人员、工业控制系统网络专业人员、信息技术评估人员等组成；被评估方由工业控制系统供应商、系统集成商、工业控制系统管理员、工业控制系统操作员等人员组成。评估组成员应该具有评估工业控制系统的经验，并意识到在生产环境中测试的局限性和存在的挑战。

评估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，进行安全评估技术培训和保密教育，制定安全评估过程管理相关规定。由于评估实施团队将访问众多敏感信息，同时掌握系统的脆弱性，可根据被评估方要求，双方签署保密合同，必要时签署个人保密协议。组织选择评估方时很难控制实际的评估方的成员。组织可以要求评估方提供其成员的信息包括职业认证、经验、技能和背景调查。

每个团队成员应具有明确的角色和责任。为确保安全评估实施工作的顺利有效进行，应采用合理的项目管理机制，主要相关成员角色与职责说明如表1、表2所示。

表 1 评估方成员角色与职责说明

评估组 人员角色	工作职责
项目组长	是安全评估项目中实施方的管理者、责任人，具有丰富的工业控制系统安全评估经验。具体工作职责包括： 1） 根据项目情况组建评估项目实施团队； 2） 根据项目情况与被评估方一起确定评估目标和评估范围，并组织项目组成员对被评估方实施系统调研； 3） 根据评估目标、评估范围及系统调研的情况确定评估依据，并组织编写评估方案； 4） 组织项目组成员开展安全评估各阶段的工作，并对实施过程进行监督、协调和控制，确保各阶段工作的有效实施； 5） 与被评估方进行及时有效的沟通，及时商讨项目进展状况及可能发生问题的预测等； 6） 组织项目组成员将安全评估各阶段的工作成果进行汇总，编写《安全评估报告》等项目成果物； 7） 负责将项目成果物移交被评估方，向被评估方汇报项目成果，并提请项目验收。
评估人员	是负责安全评估项目中技术方面评估工作的实施人员，应熟悉工业控制系统专用的通信协议（例如：DNP3、ModBus、PROFINET、PROFIBUS等）；同时应精通编码、逆向工程、协议分析和渗透测试等；部分工业控制系统使用非桌面操作系统，评估实施团队成员应熟悉被检测工业控制系统使用的操作系统。具体工作职责包括： 1） 根据评估目标与评估范围的确定参与系统调研；

	2） 参与编写《评估方案》； 3） 遵照《评估方案》实施各阶段具体的评估工作，主要包括：资产调查、威胁调查、脆弱性核查、安全性检测等； 4） 对评估工作中遇到的问题及时向项目组长汇报，并提出需要协调的资源； 5） 将各阶段的技术性评估工作成果进行汇总，参与编写《安全评估报告》等项目成果物； 6） 负责向被评估方解答项目成果物中有关技术性细节问题。
质量管控员	是负责安全评估项目中质量管理的人员。具体工作职责包括： 1） 监督审计各阶段工作的实施进度与时间进度，对可能出现的影响项目进度的问题及时通告项目组长； 2） 负责对项目资料进行管控。

表 2　被评估方成员角色与职责说明

被评估方 人员角色	工作职责
项目组长	是安全评估项目中被评估方的管理者。具体工作职责包括： 1） 与评估机构的项目组长进行工作协调； 2） 组织本单位的项目组成员在安全评估各阶段活动中的配合工作； 3） 组织本单位的项目组成员对项目过程中评估方提交的评估信息、数据及文档资料等进行确认，对出现的偏离及时指正； 4） 组织本单位的项目组成员对评估方提交的《安全评估报告》等项目成果物进行审阅； 5） 可授权项目协调人负责各阶段性工作，代理实施自己的职责，并指定项目协调人。
项目协调人	是指安全评估项目中被评估方的工作协调人员。具体工作职责包括： 1） 负责与被评估方各级部门之间的信息沟通，及时协调、调动相关部门的资源，包括工作场地、物资、人员等，以保障项目的顺利开展。
信息安全管理人员	是指被评估方的专职信息安全管理人员。在安全评估项目中的具体工作职责包括： 1） 在项目组长的安排下，配合评估组在安全评估各阶段中的工作； 2） 参与对项目过程中评估方提交的评估信息、数据及文档资料等进行确认，及时指正出现的偏离； 3） 参与对评估机构提交的《安全评估报告》等项目成果物进行审阅；
运维及操作人员	是指在被评估方的工业控制系统运行维护及操作人员。运维及操作人员承担工业控制系统中的现场控制层及现场设备层的管理运维及使用。在安全评估项目中的具体工作职责包括： 1） 在项目组长的安排下，配合评估组在安全评估各阶段中的工作； 2） 参与对项目过程中实施方提交的评估信息、数据及文档资料等进行确认，及时指正出现的偏离； 3） 现场核查时，运维操作人员必须在场，并由其进行现场核查操作，评估人员负责

	核查并记录其操作结果； 4） 参与对评估组提交的《安全评估报告》等项目成果物进行审阅；
开发集成人员	是指在被评估方本单位或第三方外包商的软件开发或系统集成人员代表。在安全评估项目中的具体工作职责包括： 1） 在项目组长的安排下，配合评估组在安全评估各阶段中的工作； 2） 参与对项目过程中实施方提交的评估信息、数据及文档资料等进行确认，及时指正出现的偏离；

5.1.5 系统调研

系统调研是熟悉了解被评估对象的过程，安全评估组应进行充分的系统调研，修正评估目标跟范围，同时为安全评估依据和方法的选择、评估内容的实施奠定基础。评估方对工业控制系统进行调研可采取文档查阅、资料收集、现场交流和现场查看等方式进行，如图4所示。

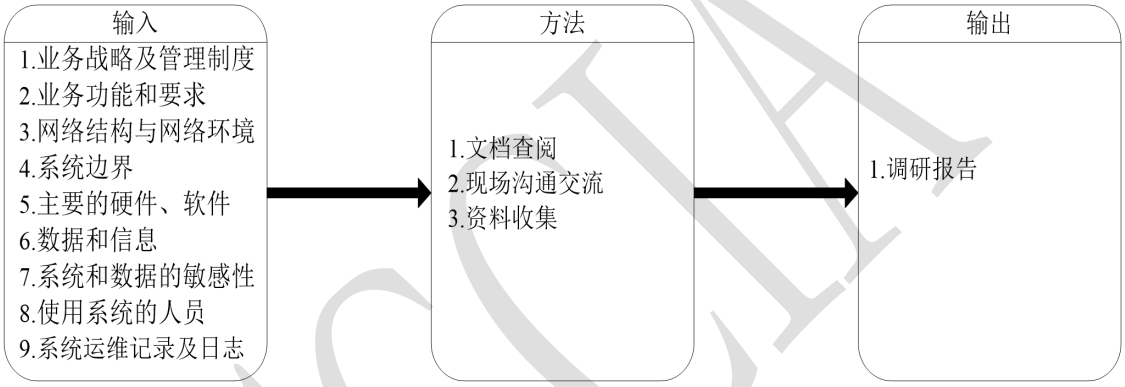

图 4 系统调研

实施指南如下：

a） 现场交流是由评估组针对工业控制系统与系统运维、系统操作、采购系统设备及软件等相关人员进行交流，了解其承担的业务、网络结构、系统边界等；

b） 文档查阅主要是查看其设计文档、使用说明文档等文档；

1） 在工业控制系统中，若现场设备及其应用软件非组织自己开发，评估组需仔细审查供应商提供的所有资料，并与供应商取得联系，以便评估实施时可以进行技术沟通；

2） 查看工业控制系统的安全需求及对应工业控制系统所处安全控制基线级别，采取哪些工业控制系统安全措施；

c） 评估组现场核查工业控制系统的物理环境、操作过程、设备组成等方面的信息并进行资料收集；

d） 评估组根据现场调研整理调研结果，编写调研报告。

5.1.6 确定评估依据

根据系统调研结果，确定评估依据和评估方法。评估依据包括（但不限于）：

a） 工业控制系统本身的特性要求及所处的生命周期等；

b） 现行国际标准、国家标准、行业标准；

c） 行业主管机关系统的要求和制度；
d） 工业控制系统安全保护等级要求及安全控制基线等级；
e） 系统互联单位的安全要求；

根据评估依据，应考虑评估的目的、范围、时间、效果等因素来选择具体的安全计算方法，并依据业务实施对系统安全运行的需求，确定相关的判断依据，使之能够与组织环境和安全要求相适应。

5.1.7 制定方案

安全评估方案是评估工作实施活动总体计划，用于管理评估工作的开展，使评估各阶段工作可控，并作为评估项目验收的主要依据之一。安全评估方案应得到被评估方的确认和认可。安全评估方案的内容应包括（但不仅限于）：

a） 安全评估工作框架：包括评估目标、评估范围、评估依据等；
b） 评估团队：包括评估组成员、组织结构、角色、责任；
c） 评估工作计划：包括各阶段工作内容和工作形式；
d） 评估环境要求：根据具体的评估方法选取相应的评估环境，包括工业控制系统现场环境，工业控制系统开发和测试环境，模拟仿真环境；
e） 安全规避：包括保密协议、评估工作环境要求、评估方法、工具选择、应急预案等；
f） 时间进度安排：评估工作实施的时间进度安排。

5.2 技术类

5.2.1 软件版本和更新情况

软件版本和更新情况的检查要求包括：

a） 检查对工业控制应用软件版本的管理情况，密切关注产品漏洞和补丁发布，严格软件升级、补丁安装管理，严防病毒、木马等恶意代码侵入。关键工业控制系统软件升级、补丁安装前要请专业技术机构进行安全评估和验证。

5.2.2 身份标识与鉴别

身份标识与鉴别的检查要求包括：

a） 检查工业控制软件用户身份标识和鉴别的管理：
   1） 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
   2） 应使用密码技术，对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种是不可伪造的；
   3） 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；
   4） 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
   5） 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数；
b） 检查鉴别信息的保密措施，当对服务器进行远程管理时，应采用密码技术，实现鉴别信息在网络传输过程中的机密性和完整性保护，防止鉴别信息在网络传输过程中被窃听或被篡改。

5.2.3 访问控制

访问控制的检查要求包括：

a) 检查工业控制应用软件的访问控制策略：
   1) 应提供自主访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
   2) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；
   3) 应通过比较安全标记来确定是授予还是拒绝主体对客体的访问；
   4) 应采用密码技术，实现对访问控制信息的完整性保护；
b) 检查工业控制应用软件账户管理策略：
   1) 应由授权主体配置访问控制策略，并禁止默认帐户的访问；
   2) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
   3) 严格账户管理，根据工作需要合理分类设置账户权限。

5.2.4 口令管理

口令管理的检查要求包括：

a) 检查口令的安全性：
   1) 口令应有复杂度要求并定期更换；
   2) 严格口令管理，及时更改产品安装时的预设口令，杜绝弱口令、空口令；
b) 检查口令鉴别失败处理策略，应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

5.2.5 安全审计

安全审计的检查要求包括：

a) 检查安全审计功能：
   1) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；
   2) 根据安全评估和项目需求，应建立一个可审计项目列表；
b) 检查审计记录的内容：
   1) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；
   2) 工业控制系统的审计记录应包含：发生事件的种类、时间、发生地点及原因、事件的结果、以及任何与事件相关的用户和项目 ID；
c) 检查审计报表，应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；
d) 检查审计记录的备份和保存方式：
   1) 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；
   2) 应防止对审计信息和审计工具进行未授权的访问、修改、删除；
   3) 应采用密码技术，实现审计记录在存储过程中的机密性和完整性保护。

5.3 管理类

5.3.1 工业控制系统信息安全规划管理

5.3.1.1 控制系统信息安全规划

控制系统信息安全规划的检查要求包括：

a) 检查工业控制系统信息安全规划内容，应当为控制系统开发了安全计划：该计划满足与企业构架一致；明确定义系统的授权边界；描述任务和业务过程的中的操作环境；提供安全控制系统的分类；描述控制系统的操作环境；描述与其他控制系统或企业网络的连接或关系；提供控制系统安全性要求的概述；
b) 检查工业控制系统信息安全规划实施前的审查和批准记录：
   1) 应检查控制系统的安全计划；
   2) 在计划实施前由授权官员或指定代表审查和批准；
c) 检查工业控制系统信息安全规划的更新情况，应当实时更新计划，以解决再计划实施和安全控制评估中控制系统和环境变化产生的问题。

5.3.1.2 信息安全方案设计

信息安全方案设计的检查要求包括：
a) 检查信息安全建设工作计划：
   1) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；
   2) 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案和密码应用方案，并形成配套文件；
b) 检查信息安全总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的评审记录，应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；
c) 检查总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的更新和修订记录，应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。

5.3.2 工业控制系统信息安全制度管理

5.3.2.1 管理制度范围

管理制度范围的检查要求包括：
a) 检查信息安全工作总体方针和安全策略，应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
b) 检查安全管理制度，应对安全管理活动中的各类管理内容建立安全管理制度；
c) 检查日常管理操作的操作规程，应对要求管理人员或操作人员执行的日常管理操作建立操作规程；
d) 检查信息安全管理制度体系建设情况，应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

5.3.2.2 制定和发布

制定和发布的检查要求包括：
a) 检查制定安全管理制度的人员安排，应指定或授权专门的部门或人员负责安全管理制度的制定；
b) 检查安全管理制度的格式和版本控制，安全管理制度应具有统一的格式，并进行版本控制；

c) 检查安全管理制度的论证和审定记录，应组织相关人员对制定的安全管理制度进行论证和审定；
d) 检查安全管理制度发布方式，安全管理制度应通过正式、有效的方式发布；
e) 检查安全管理制度的发布范围以及收发文登记记录，安全管理制度应注明发布范围，并对收发文进行登记；
f) 检查针对安全管理制度的密级管理，有密级的安全管理制度，应注明安全管理制度密级，并进行密级管理。

5.3.2.3 评审和修订

评价和修订的检查要求包括：
a) 检查对安全管理制度合理性和适用性的审定记录，应由信息安全领导小组负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；
b) 检查对安全管理制度的改进和修订记录：
   1) 应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订；
   2) 应明确需要定期修订的安全管理制度，并指定负责人或负责部门负责制度的日常维护；
c) 检查安全管理制度评审和修订的操作范围，应根据安全管理制度的相应密级确定评审和修订的操作范围。

5.3.3 工业控制系统信息安全组织建设

5.3.3.1 岗位设置

岗位设置的检查要求包括：
a) 检查信息安全工作领导小组的设立情况，应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；
b) 检查工业控制系统信息安全管理工作的职能部门和岗位设置情况：
   1) 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
   2) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；
   3) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求；
   4) 进一步加强工业控制系统信息安全工作的组织领导。

5.3.3.2 人员配备

人员配备的检查要求包括：
a) 检查安全管理工作中专职人员的配备情况：
   1) 应配备一定数量的系统管理员、网络管理员、安全管理员等；
   2) 应配备专职安全管理员，不可兼任；
   3) 关键事务岗位应配备多人共同管理。

5.3.3.3 授权和审批

授权和审批的检查要求包括：
a) 检查审批事项、审批部门和批准人相关职责设定情况，应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

b) 检查针对系统变更、重要操作、物理访问和系统接入等事项的审批程序以及对重要活动的逐级审批制度，应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
c) 检查需审批事项更新记录：
   1) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
   2) 应记录审批过程并保存审批文档。

5.3.3.4 沟通和合作

沟通和合作的检查要求包括：
a) 检查外联单位联系列表，应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
b) 检查安全顾问的聘请情况，应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。

5.3.3.5 审核和检查

审核和检查的检查要求包括：
a) 检查安全管理员对系统定期安全检查的记录，安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
b) 检查安全检查结果的通报记录，应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
c) 检查内部人员或上级单位定期全面安全检查的记录，应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
d) 检查安全审核和安全检查制度规范的制定和执行记录，应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

5.3.4 工业控制系统人员安全管理

5.3.4.1 人员录用

人员录用的检查要求包括：
a) 检查人员录用的负责人指定情况，应指定或授权专门的部门或人员负责人员录用；
b) 检查人员录用过程，应严格规范人员录用过程，对被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；
c) 检查保密协议的签署情况：
   1) 应签署保密协议；
   2) 应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

5.3.4.2 人员离职

人员离职的检查要求包括：
a) 检查人员离职的管理规范：
   1) 应制定有关管理规范，严格规范人员离岗过程，及时终止离岗员工的所有访问权限；
   2) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
   3) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开；

4) 人员终止雇佣后，应终止其对控制系统的访问；
5) 人员终止雇佣后，应回收所有与内部工控系统安全相关的物品。

5.3.4.3 人员变动

人员变动的检查要求包括：

a) 检查人员变动的管理规范，人员内部变动后，应检查其对工控系统逻辑上、物理上的授权访问。

5.3.4.4 安全教育和培训

安全教育和培训的检查要求包括：

a) 检查信息安全教育和培训记录：
   1) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
   2) 应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；
   3) 应对安全教育和培训的情况和结果进行记录并归档保存；
   4) 组织应对所有工控系统用户进行基础的安全意识培训；
   5) 工控系统安全培训活动(包括安全意识培训和特定的工控系统安全培训应以文档的形式加以记录，做到随时查阅监控。

5.3.4.5 人员考核

人员考核的检查要求包括：

a) 检查进行安全技能和安全认知的考核的情况，应定期对各个岗位的人员进行安全技能及安全认知的考核；
b) 检查对信息安全关键岗位人员的安全审查和技能考核记录，应对关键岗位的人员进行全面、严格的安全审查和技能考核；
c) 检查保密制度的教育和考核记录：
   1) 应建立保密制度，并定期或不定期的对保密制度执行情况进行检查或考核；
   2) 应对考核结果进行记录并保存。

5.3.4.6 第三方人员安全

第三方人员安全的检查要求包括：

a) 检查第三方人员安全管理制度：
   1) 应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案；
   2) 对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行；
   3) 对关键区域不允许外部人员访问；
   4) 应当为第三方供应商建立了包括安全角色和职责的人员安全要求；
   5) 应对供应商的服务情况进行了监管；
b) 检查第三方人员安全管理记录。

5.3.4.7 人员处罚

人员处罚的检查要求包括：

a) 检查对违反工控系统安全政策和程序的人员的处罚制度和记录，应对不服从已建立的工控系统安全政策和程序的人员进行处罚。

5.3.5 工业控制系统开发管理

5.3.5.1 产品采购

产品采购的检查要求包括：

a) 检查安全产品采购和使用相关的规范和制度，应确保安全产品采购和使用符合国家的有关规定；
b) 检查产品采购前的选型测试记录，应预先对产品进行选型测试，确定产品的候选范围；
c) 检查定期对候选产品名单的审定和更新记录：
   1) 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品；
   2) 定期审定和更新候选产品名单。

5.3.5.2 第三方管理

第三方管理的检查要求包括：

a) 检查第三方管理的执行情况，慎重选择工业控制系统设备，在供货合同中或以其他方式明确供应商应承担的信息安全责任和义务，确保产品安全可控。

5.3.5.3 离线测试

离线测试的检查要求包括：

a) 检查系统的安全性测试报告：
   1) 应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；
   2) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；
   3) 应创建和执行安全性测试和评估计划；
   4) 应将安全测试/评估和漏洞补救过程进行记录存档；
b) 检查对系统测试验收的控制方法和人员行为准则的书面规定，应对系统测试验收的控制方法和人员行为准则进行书面规定；
c) 检查系统测试验收工作完成情况，应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；
d) 检查对系统测试验收报告审定的情况，应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

5.3.5.4 验收交付

验收交付的检查要求包括：

a) 检查验收交付规定，应对系统交付的控制方法和人员行为准则进行书面规定；
b) 检查验收交付记录：
   1) 应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
   2) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

5.3.6 工业控制系统信息安全运维管理

5.3.6.1 资产管理

资产管理的检查要求包括：

a) 检查信息系统相关的资产清单，应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
b) 检查资产安全管理制度，应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；
c) 检查对资产进行标识管理的措施，应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
d) 检查对信息分类与标识方法的管理情况，应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

5.3.6.2 介质管理

介质管理的检查要求包括：

a) 检查介质安全管理制度制定情况，应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；
b) 检查介质安全管理制度实施情况：
    1) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
    2) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；
    3) 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，重要数据的存储介质带出工作环境必须进行内容加密并进行监控管理，对于需要送出维修或销毁的介质应采用多次读写覆盖、清除敏感或秘密数据、对无法执行删除操作的受损介质必须销毁，保密性较高的信息存储介质应获得批准并在双人监控下才能销毁，销毁记录应妥善保存；
    4) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；
    5) 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理；
    6) 应对工控系统的移动介质进行标记；
    7) 应在残留内容消除后免除移动设备的标记；
    8) 应在物理上安全管控、存放电子或非电子的介质；
    9) 应保护工控系统介质直到介质被摧毁或者通过了经认可的设备、技术、过程进行清理；
    10) 应对在控制地区外使用的介质传输进行保护和控制；
    11) 应对在控制地区外使用的介质传输保留问责资料；
    12) 应在废除、重用电子和非电子介质前清理工控系统的介质；
    13) 应采用与信息敏感性相称的强力、完整的清理机制。

5.3.6.3 设备管理

设备管理的检查要求包括：

a) 检查信息系统相关的各种设备维护管理记录，应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；

b) 检查设备安全管理制度，应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
c) 检查配套设施、软硬件维护方面的管理制度，应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；
d) 检查终端计算机、工作站、便携机、系统和网络等设备的操作和使用的相关管理制度：
   1) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
   2) 应确保信息处理设备必须经过审批才能带离机房或办公地点；
   3) 设备选择与升级管理要求；
   4) 应采用密码技术，建立安全运维通道，以实现对重要设备的安全运维，以及运维数据的机密性和完整性保护。

5.3.6.4 控制系统维护

控制系统维护的检查要求包括：
a) 检查工控系统维护相关制度：
   1) 应以正式文件的形式制定系统维护的法规来明确相关目的目标、维护范围、角色，应承担的责任、管理架构、以及各组织间的协调等事项；
   2) 应当按照制造商、供应商的规范要求或组织的需要对工控系统进行规划、实施维护维修，并做好记录登记以便复查；
   3) 在维护和修理完毕后，应检查所有潜在的影响系统控制安全的问题；
   4) 应授权、监视、控制非本地的维护和诊断活动；
   5) 应当仅在符合组织的相关规定和信息系统安全规划的情况下才允许非本地的维护和诊断；
   6) 建立非本地维护和诊断会话时，应采用识别和授权技术；
   7) 应在非本地的维护和诊断完成后终止所有的会话连接；
b) 检查工控系统的维护规划、维护维修记录：
   1) 应保持记录对非本地维护和诊断活动；
   2) 应建立了一套维护人员授权以及维持现有已授权维护组合和人员名单的程序；
   3) 应建立一份安全系数要求高的工控系统组件以及关键信息技术组件的名单，并在其发生故障之前定期对其进行维护或配备了配用组件。

5.3.6.5 网络安全管理

网络安全管理的检查要求包括：
a) 检查网络安全管理制度的制定：
   1) 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期、密码应用安全等方面作出规定；
   2) 检查网络安全管理人员配置及职责；
   3) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
   4) 检查网络设备维护记录；

5) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

b) 检查网络安全管理措施的实施记录：

1) 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；
2) 应实现设备的最小服务配置和优化配置，并对配置文件进行定期离线备份；
3) 应保证所有与外部系统的连接均得到授权和批准；
4) 应检查是否采用了密码技术，搭建了安全的网络通信信道，实现了对通信双方的身份鉴别、通信数据的机密性和完整性保护以及网络边界访问控制信息的完整性保护等密码应用要求。

5.3.6.6 系统监控管理

系统监控管理的检查要求包括：

a) 检查系统监控管理情况：

1) 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；
2) 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；
3) 应采用密码技术，实现对检测和报警记录的存储完整性保护；

b) 检查安全管理中心的建立和实施情况，应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计、密码应用安全等安全相关事项进行集中管理。

5.3.6.7 补丁管理

补丁管理的检查要求包括：

a) 检查系统补丁的可靠性，在工控系统环境中，为操作系统组件打补丁应当对补丁进行充分测试（例如，在不同的离线工控系统上测试）；

b) 检查工控系统漏洞补丁管理机制的建立，机构应当建立一个系统的、负责的、并具有记录的工控漏洞补丁管理机制；

c) 检查安全计划中关于更新补丁的措施，应将打补丁过程中可能发生的工控系统业务中断的情况列入计划之中。

5.3.7 工业控制系统信息安全应急管理

5.3.7.1 应急预案

应急预案的检查要求包括：

a) 检查应急预案制定情况：

1) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
2) 应制定工控系统的应急计划；
3) 应根据工控系统运行状态定期复查应急计划；
4) 应依据不断改变的组织、工控信息系统或运行环境以及应急计划实施、测试过程中遇到的新问题来修订应急计划；
5) 组织是否制定了应急人员和组织要素的名单（包括其姓名和职务）并将应急计划分发给名单中的人员。

5.3.7.2 应急演练

应急演练的检查要求包括：

a) 检查应急演练执行记录：
   1) 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；
   2) 是否依据组织制定的演练内容，定期的进行工控系统应急计划演练，从而检验计划的可行性以及组织对计划的反应程度。

5.3.7.3 应急保障

应急保障的检查要求包括：

a) 检查应急保障队伍的建立情况，应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障。

5.3.7.4 业务连续性规划

业务连续性规划的检查要求包括：

a) 检查业务连续性规划的制定：
   1) 应制定业务连续性规划来解决生产中断情况下继续维持或重建，这些中断可能来自于自然灾害、或无意的人为事件或蓄意的认为事件，或设备故障；
   2) 规划应全盘考虑长期中断（灾难恢复）和短期中断（业务恢复）的影响；
   3) 在制定政策规划时，应将业务连续性控制与物理控制结合起来；
   4) 在创建一个业务连续性计划以应付潜在的业务中断之前，应基于典型的业务需求，明确各种系统和子系统的恢复目标。恢复目标包含系统恢复和数据恢复。

5.4 工程类

5.4.1 备用电源

备用电源的检查要求包括：

a) 检查供电线路上的稳压器和过电压防护设备，应在机房供电线路上配置稳压器和过电压防护设备；
b) 检查备用电力供应，应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
c) 检查置冗余或并行的电力电缆线路，应设置冗余或并行的电力电缆线路为计算机系统供电；
d) 检查备用供电系统：
   1) 应建立备用供电系统；
   2) 是否提供了短期不间断电源来保证主电源出现断电或电力不足等问题时保持电力系统有序关机。

5.4.2 消防措施

消防措施的检查要求包括：

a) 检查重点区域内火灾自动消防系统，机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
b) 检查机房、控制室的建筑材料，机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
c) 检查重点区域的隔离防火措施，机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

5.4.3 防水和防潮

防水和防潮的检查要求包括：

a) 检查水管安装线路，水管安装，不得穿过机房屋顶和活动地板下；
b) 检查机房窗户、屋顶和墙壁的防雨水措施，应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
c) 检查机房内防止水蒸气结露和地下积水的转移与渗透的措施，应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
d) 检查机房的防水检测和报警措施，应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

5.4.4 控制系统组件选址

控制系统组件选址的检查要求包括：

a) 检查控制系统组件设备的选址，在控制系统组件设备选址时应考虑将物理和环境损害以及非法入侵降到最小；
b) 检查工控系统网络设备的物理隔离措施，工控系统网络，包括交换机、路由器、网络接口、服务器、工作站和控制器上的网络设备，应当设在一个安全的区域，只能由授权的人员访问。

5.4.5 控制中心/控制站

控制中心/控制站的检查要求包括：

a) 检查控制中心、控制站的访问授权管理，应通过身份鉴别或授权才能访问这些区域；
b) 检查控制中心、控制室的防爆能力，在极端情况下，应能够保证控制中心/控制室的防爆能力；
c) 检查备用控制中心、控制室的设置，在主控制中心/控制室无法启用的情况下，应采用了满足工控系统安全控制管理、运营和技术要求的备用控制中心/控制室；
d) 检查备用控制中心、控制室的可行性和有效性，应评估备用控制中心/控制室在安全控制过程中的有效性和可行性；
e) 检查应急处理措施，如果发生安全事件或问题，应提供了方法让员工与信息安全人员取得联系。

5.4.6 环境因素控制

环境因素控制的检查要求包括：

a) 检查保持工厂设备以及工厂内部的温度和湿度水平的措施：
    1) 应采取措施来保持工控系统所在地设备（工厂）内部的温度和湿度水平；
    2) 应定期对温度和湿度值进行采集监控；
    3) 机房应设置温湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内；
b) 检查机房防静电措施：
    1) 设备应采用必要的接地防静电措施；
    2) 机房应采用防静电地板；
    3) 应采用静电消除器等装置，减少静电的产生；
c) 检查工控系统防尘土措施，对于在尘土飞扬地点工作的工控系统，是否采取了相应的过滤措施。特别在有些灰尘可能会导电或具有磁场的情况下尤为重要；

d) 检查工控系统防共振措施，在考虑共振的场合下，系统是否安装了橡胶衬套，以防止磁盘崩溃和接线问题。

5.4.7 电磁防护

电磁防护的检查要求包括：

a) 检查防止外界电磁干扰和设备寄生耦合干扰的措施，应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；
b) 检查防止电源线和通信线缆互相干扰的措施，电源线和通信线缆应隔离铺设，避免互相干扰；
c) 检查对关键区域电磁屏蔽的措施：
   1) 应对关键区域实施电磁屏蔽；
   2) 应采取了防止通过电磁信号泄露信息的保护措施。

5.4.8 物理访问控制

物理访问控制的检查要求包括：

a) 检查分区域管理划分情况。应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；
b) 检查区域访问控制情况：
   1) 应对工控系统所在地的设备所有的物理访问点（包括指定的出入口）执行物理访问授权（指定可公开访问的除外），如设置路障、栅栏、保卫室、门禁等；
   2) 在出入口和重点区域是否装配了访问检测系统，包括视频摄像机、传感器和各种识别设备，用于监视和存储记录；
c) 检查访客记录和物理访问日志，应建立并维持了工控系统所在地设备的访客访问记录（组织批准可公开访问的设备除外）；
d) 检查授权访问设备和各区域的人员列表，应建立并维护工控系统所在地授权访问设备人员的列表（指定可公开访问的除外）；
e) 检查重要区域（如机房、控制中心/控制室等）第二道电子门禁系统配置情况，重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员；
f) 检查物理访问设备的维护记录，应定期清查维护物理访问设备，保证其可用性能；
g) 检查更换密钥和密码的记录：
   1) 应确保密钥、暗码和其他物理访问设备的安全；
   2) 应定期或在密钥丢失、暗码失效或相关个人调离的情况下更换暗码和密钥；
h) 检查物理和环境安全层面密码应用情况：
   1) 应采用密码技术，实现对重要物理访问点进出用户的身份鉴别；
   2) 应采用密码技术，实现对重要物理访问点用户进出记录数据的存储完整性保护；
   3) 应采用密码技术，实现对重要区域视频监控音像记录数据的存储完整性保护。

5.4.9 防盗窃和防破坏

防盗窃和防破坏的检查要求包括：

a) 检查设备和主要部件的防盗、防破坏措施：
   1) 应将主要设备放置在机房内；
   2) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；
b) 检查通信线缆防盗和防破坏措施，应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；

c） 检查重点区域的监控和防盗报警系统安装情况：

1） 应利用光、电等技术设置机房防盗报警系统；

2） 应对机房设置监控报警系统。

6 工业控制系统信息安全等级定级方法

6.1 工业控制系统信息安全定级流程

本标准基于风险评估过程规定工业控制系统信息安全定级流程。

依据GB/T 31722-2015，风险管理应先建立语境，再进入风险评估、风险处置等过程。风险评估过程由风险分析和风险评价活动组成，其中风险分析包括风险识别及风险估算活动。这与本标准中工业控制系统信息安全定级流程是一致的。定级流程的确定工业控制系统定级对象，是在建立风险评估的语境；定级流程的确定工业控制系统资产重要程度、确定受侵害后的潜在影响程度、确定需抵御的信息安全威胁程度，属于风险分析的风险识别及风险估算活动；定级流程的确定工业控制系统信息安全等级，属于风险评价活动。

确定作为定级对象的工业控制系统信息安等级的一般流程如图5所示：

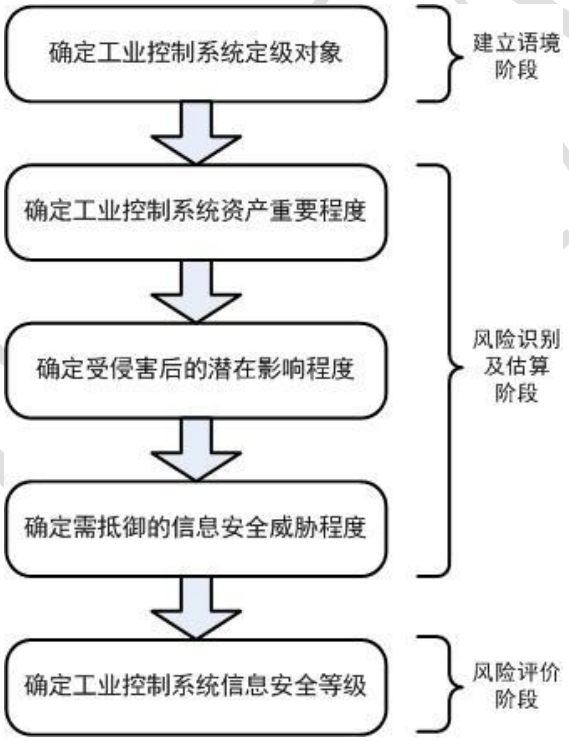

图 5 工业控制系统信息安全定级流程

6.2 确定工业控制系统定级对象

6.2.1 定级对象的确认条件

确认一个工业控制系统作为定级对象，该工业控制系统应具备如下基本条件：

a） 一个具体的完整的工业控制系统

1） 承载“单一”的工业控制业务应用，属于企业的一个自动化生产过程或一个生产装置（如聚苯乙烯生产装置）的工业控制系统；

2） 与其他业务应用的控制过程没有交叉或嵌套以及控制信息的交换，且独享所有信息处理设备、控制设备和受控设备；

3) 以 DCS 或 SCADA 为主构成生产过程控制的自动化系统，可由若干服务器、工程师工作站、操作员工作站、数据采集接口或控制接口，以及相关网络等其他设施组成；

b) 工业控制系统中相对独立的一部分

1) 承载“相对独立”的工业控制过程中一部分业务应用或控制过程独立，处于一个工业生产装置中一个相对独立的区域，与其他业务应用的控制过程有上位或下位关系或少量控制信息交换，可能会与其他业务应用共享一些设备，如网络传输设备；

2) 这个相对独立的区域一般属于比较大的或复杂的工业控制系统的一个或几个相邻的层、安全区域、通信网络，可按地理位置或管理责任划分，但应具有共同的安全需求；

3) 必要时，起传输作用的工业控制基础网络系统可作为单独的定级对象；

c) 具有工业控制系统的基本要素

1) 作为定级对象的工业控制系统应该是由相关的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按照一定的工业控制目标、控制流程和和控制规则组合而成的有形实体，保留完整的控制过程；

2) 一个工业控制系统可由多个厂家的设备与系统组成，所有功能协调一起为工业生产装置提供整合自动化功能；

3) 避免将某个单一的系统组件，如服务器、控制终端、网络设备、通信路径以及控制部件等作为定级对象；

d) 具有唯一确定的安全责任单位

1) 作为定级对象的工业控制系统应能够唯一地确定其安全责任单位，即定级对象的责任单位应对所定级的工业控制系统具有安全管理责任；

2) 如果一个单位的某个下级单位负责工业控制系统安全建设、运行维护等过程的全部安全责任，则这个下级单位可以成为工业控制系统的安全责任单位；

3) 如果一个单位中的不同下级单位分别承担工业控制系统不同方面的安全责任，则该工业控制系统的安全责任单位应是这些下级单位共同所属的单位。

6.2.2 定级对象的系统描述

对定级对象进行系统描述的目的是识别该工业控制系统的任务和使命，即该工业控制系统的任务要求和它所要达到的能力，包括工业控制系统执行的功能、所需的接口及这些接口相关的能力、所要处理的信息、所支持的运行结构以及需要抵御的威胁等。

对作为定级对象的工业控制系统描述应包括：

a) 工业控制系统的基本信息：

1) 工业控制系统及其归属的工业生产装置的目的、任务和使命；

2) 工业控制系统的控制过程、控制范围、边界、信息流；

3) 工业控制系统的业务体系、技术体系和管理体系等；

4) 形成资产列表、与资产相关的业务过程及其相关性的列表；

b) 工业控制系统的网络及设备部署：包括工业控制系统的物理环境、工业控制系统网络拓扑结构、控制系统及受控设备的部署情况，并明确工业控制系统的边界；

c) 工业控制系统的业务种类和特性：包括工业控制系统涉及的业务种类和受控设备数量，以及工业控制系统对可用性、实时性、可操作性、完整性、保密性需求及业务特性，如是否形成闭合控制回路、是否为连续控制系统等；

d) 工业控制系统的系统服务：包括为完成预定的业务目标和任务，提供的操作、控制过程和其他业务功能，以及这些服务在可用性（如及时有效）、完整性和保密性等方面的重要性；
e) 工业控制系统的业务数据：包括工业控制系统涉及的主要数据及相关协议，以及这些数据在保密性、完整性和可用性等方面的重要性；
f) 工业控制系统的密码应用要求：包括技术层面（物理和环境安全、网络和通信完全、设备与计算安全、应用和数据安全）和管理层面（管理制度、人员管理、建设运行、应急处理）的要求；
g) 工业控制系统与企业相关信息系统的连接：包括连接方式、接口控制、传输内容，及相关用户范围和用户类型等；
h) 工业控制系统的管理框架：包括工业控制系统的组织管理结构、管理策略、相关部门设置和部门在业务运行中的作用、岗位职责；
i) 比较大的或复杂的工业控制系统的安全区域和通讯网络作为定级对象，应描述与相关安全区域和通讯网络的相互依赖关系。

6.3 确定工业控制系统资产重要程度

6.3.1 评价工业控制系统安全领域和业务使命

评价作为定级对象的工业控制系统重要性相关内容，确认方法如下：
a) 按照本标准 5.2.1.4 的要求，对工业控制系统资产进行分析，确定该工业控制系统的资产价值属于以下类型之一：
   1) 一般资产价值；
   2) 很高资产价值；
b) 按照本标准 5.2.1.2 的要求，对工业控制系统所属工业生产行业分类进行分析，确定该工业控制系统的行业领域属于以下类型之一：
   1) 一般安全领域；
   2) 重点安全领域；
   3) 关键安全领域；
c) 按照本标准 5.2.1.3 的要求，对工业控制系统在工业生产系统中所具有的业务使命进行分析，确定该工业控制系统的业务使命属于以下类型之一：
   1) 一般业务使命；
   2) 重要业务使命；
   3) 关键业务使命。

6.3.2 评价工业控制系统资产重要程度

根据作为定级对象的工业控制系统行业领域、工业控制系统业务使命，按照本标准5.2.1.1的要求，分析工业控制系统重要性相关内容，依照表2得出工业控制系统资产重要程度特征值，取值范围是由低到高1至5，共5个等级。

6.4 确定受侵害后的潜在影响程度

6.4.1 确认工业控制系统信息安全受到破坏

工业控制系统信息安全主要包括保护、维持工业控制系统所采取的可用性、完整性、保密性措施，通常是指工业控制系统的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及其系统中的工业控制系统数据受到保护，且不受偶然的或者恶意的原因而遭

到破坏，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连续可靠正常地运行。

工业控制系统信息安全属性主要包括：

a) 可用性：是指已授权实体一旦需要就可访问和使用的数据和资源的特性，确保工业控制系统及其所有部件能够可靠地运行，防止拒绝服务的发生，通常也包含工业控制系统的实时性（时间响应性，如要求系统响应时间可在毫秒级以内）、可靠性、可控性、业务连续性等；

b) 完整性：是指保护工业控制系统资产准确和完整的特性，确保工业控制系统能够以不受损害的方式执行其预定功能，避免对工业控制系统故意的或意外的未授权操作，确保工业控制相关数据没有遭受以未授权方式所作的更改或破坏，通常也包含工业控制系统的抗抵赖性、可核查性、真实性等属性；

c) 保密性：是指使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性，确保工业控制系统中保密或敏感信息在传输和存储中受到保护，能够防止窃听和非授权访问。

工业控制系统信息安全受到破坏是指，工业控制系统信息安全的可用性、完整性、保密性属性的部分或全部受到破坏。在确认工业控制系统信息安全受到破坏中，需要分别查看这三个方面安全属性受到破坏的情况，并选择其中受到破坏最严重的安全属性的破坏程度，作为工业控制系统信息安全受到破坏的程度。

6.4.2 依据侵害的客观方面进行分析

在客观方面，对受侵害对象的侵害外在表现为对工业控制系统本身的破坏。对工业控制系统的危害方式表现为：

a) 对工业控制系统提供的系统服务的破坏，是指对工业控制系统的正常运行受到性能下降、功能失效、运行中断等，影响系统预定的工业控制系统目标的完成，破坏工业控制系统的可用性（如系统可控性、业务连续性）、系统完整性、保密性；

b) 对工业控制系统涉及的业务数据的破坏，是指工业控制系统中的相关数据、控制指令、保密信息等数据被窃取、篡改、伪造等，破坏工业控制系统业务数据的完整性、可用性、保密性；

由于工业控制系统服务安全和工业控制系统业务数据安全受到破坏，所侵害的对象及其受侵害程度可能会有所不同，在确定受侵害后的潜在影响过程中，需要分别处理这两种危害方式。对受侵害对象的侵害程度的确认应按照工业控制系统服务安全和工业控制系统业务数据安全方式分别进行分析确认，并选用受侵害后的潜在影响程度特征值较高者。

6.4.3 评价受侵害的对象

定级的工业控制系统信息安全受到破坏所侵害的对象包括国家安全、国家经济安全，环境安全和人民生命安全、社会秩序稳定、公共利益、工业生产运行安全，以及公民、企业和其他组织的合法权益及重要财产安全，以及工业控制系统及相关生产装置。

对定级的工业控制系统信息安全受到破坏所侵害的对象的确认，应根据以下条件的优先顺序，逐一进行分析和选择：

a) 侵害国家安全的事项

是指定级的工业控制系统信息安全受到侵害，及其造成工业生产系统受到侵害，并由此产生对国家安全的影响，造成国家外部的威胁和侵害，造成内部的混乱和疾患，造成危害国家的安全、荣誉和利益的行为，主要包括以下方面：

1) 影响国家政权稳固和国防实力；

2) 影响国家统一、民族团结和社会安定；
3) 影响国家对外活动中的政治、经济利益；
4) 影响国家重要的安全保卫工作；
5) 影响国家经济竞争力和科技实力；
6) 其他影响国家安全的事项。

b) 侵害国家经济安全的事项

是指定级的工业控制系统信息安全受到侵害，及其造成工业生产系统受到侵害，并由此产生对国家经济安全的影响，主要包括以下方面：

1) 影响国家保持其经济存在和发展所需资源有效供给；
2) 影响经济体系独立稳定运行；
3) 影响整体经济福利；
4) 影响系统防护恶意侵害和非可抗力损害能力；
5) 影响国民经济发展和经济实力；
6) 其他影响国家经济安全的事项。

c) 侵害社会秩序稳定的事项

是指定级的工业控制系统信息安全受到侵害，及其造成工业生产系统受到侵害，并由此产生对社会秩序稳定的影响，主要包括以下方面：

1) 影响国家机关社会管理和公共服务的工作秩序；
2) 影响各种类型的经济活动秩序；
3) 影响各行业的科研、生产秩序；
4) 影响公众在法律约束和道德规范下的正常生活秩序等；
5) 其他影响社会秩序稳定的事项。

d) 侵害公共利益的事项

是指定级的工业控制系统信息安全受到侵害，及其造成工业生产系统受到侵害，并由此产生对公共利益及重要公共财产安全的影响，主要包括以下方面：

1) 影响社会成员使用公共设施；
2) 影响国有财产、劳动群众集体所有的财产安全或造成损失；
3) 影响社会成员获取公开信息资源；
4) 影响社会成员接受公共服务等方面；
5) 其他影响公共利益及重要公共财产安全的事项。

e) 侵害环境安全和人民生命安全的事项

是指定级的工业控制系统信息安全受到侵害，及其造成工业生产系统受到侵害，并由此产生对环境安全的影响，主要包括以下方面：

1) 影响工业控制系统及工业生产系统的生产技术性环境、相关自然生态环境，造成污染或破坏；
2) 因环境污染或破坏直接导致人员死亡或中毒、造成人员疏散转移、造成直接经济损失、造成区域生态功能丧失或国家重点保护物种灭绝、造成集中式饮用水水源地取水中断、造成严重辐射污染后果等。

f) 侵害公民、企业和其他组织的合法权益及重要财产安全的事项

是指定级的工业控制系统信息安全受到侵害，及其造成工业生产系统受到侵害，并由此产生对公民、法人和其他组织的合法权益及财产安全的影响，主要包括以下方面：

1) 影响由法律确认的并受法律保护的公民、法人和其他组织所享有的社会权利和利益；
2) 影响公民、法人和其他组织所有的资金和物质财产损失；

3) 影响工业生产系统运行安全，引发的工业生产安全事故；
4) 影响公民、法人和其他组织的人员生命安全，直接或间接造成的相关人员的伤害。

g) 侵害工业生产运行安全的事项

是指定级的工业控制系统信息安全受到侵害，直接产生对其控制范围内的以及上下游相关的工业生产运行安全的影响，主要包括以下方面：

1) 影响工业生产运行的有关过程不能正常；
2) 影响工业生产运行的业务连续性，出现运行中断；
3) 影响工业生产运行安全，发生生产安全事故，甚至影响人员生命财产安全；
4) 影响工业生产运行安全，发生突发环境事件，甚至影响环境安全；
5) 其他影响工业生产运行安全的事项。

h) 侵害工业控制系统及相关生产装置安全的事项

是指定级的工业控制系统信息安全受到侵害，及其造成工业控制系统自身功能受到损害或丧失，并由此产生对其所控制的相关生产装置功能受到损害或丧失，以致影响工业生产运行安全，主要包括以下方面：

1) 工业控制系统自身功能不能正常；
2) 工业控制系统自身功能完全丧失；
3) 工业控制系统自身受到毁坏；
4) 工业控制系统相关生产装置功能不能正常；
5) 工业控制系统相关生产装置功能受到损害或丧失；
6) 工业控制系统相关生产装置受到毁坏。

6.4.4 评价受侵害的程度

6.4.4.1 判定对国家安全的侵害程度

当工业控制系统信息安全保护对象受到破坏时，造成对国家安全的侵害程度，判定条件如下：

a) 一般损害：当对国家的安全、荣誉和利益未造成影响或较小的危害，可判定对国家安全的侵害程度为一般损害；
b) 严重损害：当对国家的安全、荣誉和利益造成较严重的危害，可判定对国家安全的侵害程度为严重损害；
c) 特别严重损害：当对国家的安全、荣誉和利益造成非常严重危害，可判定对国家安全的侵害程度为特别严重损害。

6.4.4.2 判定对国家经济安全的侵害程度

当工业控制系统信息安全保护对象受到破坏时，造成对国家经济安全的侵害程度，判定条件如下：

a) 一般损害：当对国民经济发展和经济实力未造成影响或较小的破坏时，可判定对国家经济安全的侵害程度为一般损害；
b) 严重损害：当对国民经济发展和经济实力造成较严重的破坏时，可判定对国家经济安全的侵害程度为严重损害；
c) 特别严重损害：当对国民经济发展和经济实力造成非常严重破坏时，可判定对国家经济安全的侵害程度为特别严重损害。

6.4.4.3 判定对社会秩序稳定的侵害程度

当工业控制系统信息安全保护对象受到破坏时，造成对社会秩序稳定的侵害程度，判定条件如下：

a) 一般损害：当对国家机关社会管理和公共服务的工作秩序、各类经济活动秩序、各行业科研及生产秩序、正常生活秩序产生有限的社会不良影响，可判定对社会秩序稳定的侵害程度为一般损害；
b) 严重损害：当对国家机关社会管理和公共服务的工作秩序、各类经济活动秩序、各行业科研及生产秩序、正常生活秩序产生较大范围的社会不良影响，可判定对社会秩序稳定的侵害程度为严重损害；
c) 特别损害：当对国家机关社会管理和公共服务的工作秩序、各类经济活动秩序、各行业科研及生产秩序、正常生活秩序产生大范围的社会不良影响，可判定对社会秩序稳定的侵害程度为特别严重损害。

6.4.4.4 判定对公共利益的侵害程度

当工业控制系统信息安全保护对象受到破坏时，造成对公共利益及重要公共财产安全的侵害程度，判定条件如下：

a) 一般损害：当对社会成员使用公共设施、获取公开信息资源、接受公共服务等公共利益产生有限的社会不良影响，对重要公共财产造成较小损失，可判定对公共利益、重要公共财产的侵害程度为一般损害；
b) 严重损害：当对社会成员使用公共设施、获取公开信息资源、接受公共服务等公共利益产生较大范围的社会不良影响，对重要公共财产造成较高损失，可判定对公共利益、重要公共财产的侵害程度为严重损害；
c) 特别损害：当对社会成员使用公共设施、获取公开信息资源、接受公共服务等公共利益产生大范围的社会不良影响，对重要公共财产造成极高损失，可判定对公共利益、重要公共财产的侵害程度为特别严重损害。

6.4.4.5 判定对环境安全和人员生命安全的侵害程度

当工业控制系统信息安全保护对象受到破坏时，造成对环境安全和人员生命安全的侵害程度，可通过生产安全事故和突发环境事件的等级表述，判定条件如下：

a) 生产安全事故等级：根据国务院第 493 号令《生产安全事故报告和调查处理条例》中规定的条件（参见附录 A 中 A.1），确定为下列等级之一：
   1) 特别重大事故；
   2) 重大事故；
   3) 较大事故；
   4) 一般事故；
b) 突发环境事件等级：根据环境保护部令第 17 号《突发环境事件信息报告办法》中规定的条件（参见附录 A 中 A.2），确定为下列等级之一：
   1) 特别重大（Ⅰ级）突发环境事件；
   2) 重大（Ⅱ级）突发环境事件；
   3) 较大（Ⅲ级）突发环境事件；
   4) 一般（Ⅳ级）突发环境事件。

6.4.4.6 判定对公民、企业和其他组织的合法权益及重要财产安全的侵害程度

当工业控制系统信息安全保护对象受到破坏时，造成对公民、企业、其他组织的合法权益及重要财产安全的侵害程度，判定条件如下：

a) 一般损害：当对公民、企业、其他组织的工作职能产生局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，以及较低的财产损失时，可判定对公民、企业、其他组织的合法权益及重要财产安全的侵害程度为一般损害；
b) 严重损害：当对公民、企业、其他组织的工作职能产生严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，以及较高的财产损失时，可判定对公民、企业、其他组织的合法权益及重要财产安全的侵害程度为严重损害；
c) 特别严重损害：当对公民、企业、其他组织的工作职能产生特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，以及极高的财产损失时，可判定公民、企业、其他组织的合法权益及重要财产安全的侵害程度为特别严重损害。

6.4.4.7 判定对工业生产运行安全的侵害程度

当工业控制系统信息安全保护对象受到破坏时，造成对其范围内相关工业生产运行安全的侵害程度，判定条件如下：

a) 一般损害：判定对工业生产系统运行安全的侵害程度为一般损害的条件为：
   1) 对工业生产系统的任务无影响、整体功能有所下降或一部分任务不能完成；
   2) 出现部分系统故障或功能下降，能够通过调整消除故障或能够立即修复出现的故障；
   3) 可能出现较轻的过程安全、业务连续性问题；
   4) 对工业生产系统运行的地理区域、人群区域、生产生活领域、时间跨度影响较小；
   5) 不会发生生产安全事故或突发环境事件；
b) 严重损害：判定对工业生产系统运行安全的侵害程度为严重损害的条件为：
   1) 对工业生产系统的大部分任务不能完成或整体功能严重下降；
   2) 出现部分系统的功能严重下降或产生中断，出现的故障不能立即通过检修予以修复；
   3) 可能出现严重的过程安全、业务连续性问题，或者较轻的人员安全、环境安全；
   4) 对工业生产系统运行的地理区域、人群区域、生产生活领域、时间跨度影响为中等；
   5) 可能会发生一般、较大的生产安全事故或突发环境事件（见附录 A）；
c) 特别严重损害：判定对工业生产系统运行安全的侵害程度为特别严重损害的条件为：
   1) 对工业生产系统的整体任务完不能成或功能部分丧失；
   2) 出现部分系统的功能全部丧失或完全中断，出现的故障需经彻底修理才能消除；
   3) 可能出现特别严重的过程安全、业务连续性问题，或者严重的人员安全、环境安全；
   4) 对工业生产系统运行的地理区域、人群区域、生产生活领域、时间跨度影响为较大；
   5) 可能会发生重大、特别重大的生产安全事故或突发环境事件（见附录 A）。

6.4.4.8 判定对工业控制系统及相关生产装置的侵害程度

当工业控制系统信息安全保护对象受到破坏时，造成对工业控制系统及相关装置的侵害程度，判定条件如下：

a) 一般损害：当对工业控制系统及相关装置产生局部影响或较轻影响，生产过程局部且非关键部位丧失完整性或可用性，较轻地干扰了生产过程的准确顺序或协调性，

未产生设备功能受到损害或丧失，没有导致停工、重新加工、重新设计，对上游或下游生产过程没有产生影响，可判定对工业控制系统及相关装置的侵害程度为一般损害；

b) 严重损害：当对工业控制系统及相关装置产生关键部位的影响或严重影响，生产过程关键部位丧失完整性或可用性，严重地干扰了生产过程的准确顺序或协调性，产生了设备功能受到损害或丧失但资产更新产生的成本不高，导致短时间的停工且在短时间内恢复工业过程控制，对上游或下游生产过程产生较轻影响，可判定对工业控制系统及相关装置的侵害程度为严重损害；

c) 特别严重损害：当对工业控制系统及相关装置产生全局影响或特别严重影响，生产过程全部丧失完整性或可用性，产生了设备功能受到损害或丧失且资产更新产生的成本很高，导致停工且不能在短时间内恢复工业过程控制，甚至需要重新加工、重新设计，对上游或下游生产过程产生严重影响，由于泄露了知识产权丧失竞争优势（如生产过程的技术秘密），可判定对工业控制系统及相关装置的侵害程度为严重损害。

6.4.5 评价受侵害后的潜在影响程度

对受侵害程度用侵害后的潜在影响程度特征值表示，评价工业控制系统受侵害后的潜在影响程度，包括：

a) 根据 5.2.2.2,按照 6.4.3 提供的方法，分析工业控制系统信息安全受到破坏后受侵害的对象，判定为下列受侵害的对象中的一个或几个：
   1) 工业控制系统及相关生产装置安全；
   2) 工业生产运行安全和公民、企业、其他组织的合法权益及重要财产安全；
   3) 环境安全、社会秩序、公共利益和人员生命安全；
   4) 国家安全、国家经济安全；

b) 根据 5.2.2.3,分析工业控制系统信息安全受到破坏后对受侵害对象的侵害程度：
   1) 按照 6.4.4.1 提供的方法，判定对国家安全的侵害程度；按照 6.4.4.2 提供的方法，判定对国家经济安全的侵害程度；选择其中侵害程度高的作为对“国家安全、国家经济安全”的侵害程度；
   2) 按照 6.4.4.3 提供的方法，判定对环境安全和人员生命安全的侵害程度；按照 6.4.4.4 提供的方法，判定对社会秩序稳定的侵害程度；按照 6.4.4.5 提供的方法，判定对公共利益及重要公共财产安全的侵害程度；选择其中侵害程度最高的作为对“环境安全、社会秩序、公共利益和人员生命安全”的侵害程度；
   3) 按照 6.4.4.6 提供的方法,判定对工业生产运行安全的侵害程度;按照 6.4.4.7 提供的方法，判定对公民、企业和其他组织的合法权益及重要财产安全的侵害程度；选择其中侵害程度高的作为对“国家安全、国家经济安全”的侵害程度；
   4) 按照 6.4.4.8 提供的方法,判定对工业控制系统及相关生产装置安全的侵害程度；
   5) 上述判定的对受侵害对象的侵害程度按照下列受侵害程度之一表示：
      ——造成一般损害；
      ——造成严重损害；
      ——造成特别严重损害。

c) 根据 a）判定的一个或几个受侵害对象，以及根据 b）判定的对相应受侵害对象的侵害程度，逐一按照本标准 5.2.2.1 的要求，分析工业控制系统受侵害后潜在影响的相关内容，分别依照表 3 得出工业控制系统受侵害潜在影响程度特征值，并选择

其中最高者作为工业控制系统受侵害潜在影响程度特征值。影响程度特征值取值范围是由低到高 1 至 5，共 5 个等级。

6.5 确定需抵御的信息安全威胁程度

6.5.1 评价面临的信息安全威胁

评价工业控制系统面临的信息安全威胁，包括：

a) 分析定级的工业控制系统可能面临的各种威胁，按照 5.2.3.2 所列出的常见威胁列表，还应查阅企业、行业、业务已有的威胁列表和统计数据，形成定级的工业控制系统可能面临所有威胁的列表；

b) 按照列表评价每个威胁的威胁程度及其特征值（取值范围为 1-5），形成完整的威胁列表。

6.5.2 评价信息安全事件可能性

评价信息安全事件可能性的目的是识别威胁和估算其发生可能性，应考虑来自事件和以往威胁评估的内部经验，注意相关威胁是持续变化的，特别是当业务环境或工业控制系统发生变化时。

a) 根据 6.5.1 形成的威胁列表，对确定存在每一种威胁逐一分析其发生的可能性，应考虑以下因素的影响：
   1) 工业控制系统资产的吸引力或可能影响；
   2) 工业控制系统受侵害后可造成影响或获得收益的容易度；
   3) 工业控制系统面临威胁发起者的技术能力和占有资源的强度；
   4) 工业控制系统固有脆弱性可被利用的难易程度；

b) 根据 5.2.3.3，对发生可能性高的威胁及其可利用的工业控制系统固有脆弱性组合进行分析，确定其可利用容易度：
   1) 应识别工业控制系统存在的固有脆弱性，即工业控制系统、相关生产装置以及所属企业或行业本身固有的，而非某个工业控制系统个体原因（如人为疏忽）造成的脆弱性；如：
      ——用于易燃易爆、强辐射、剧毒等危险品生产的工业控制系统；
      ——用于野外或难以监管的工业控制系统；
      ——受行业生产条件限制或技术水平限制，存在一定缺陷的业工业控制系统；
   2) 应识别可被威胁利用的工业控制系统固有脆弱性，按照被威胁利用的容易程度排序；
   3) 应关注工业控制系统固有脆弱性可利用容易度的变化，当环境变化、技术变化、系统部件的故障，替换部件的不可用、人员流动、以及更高级的威胁出现的影响，一个最初只包含有限固有脆弱性的工业控制系统，可能会变得更易受攻击；

c) 分析出现信息安全事件的可能性，应注意以下因素：
   1) 工业控制系统所属企业或行业对威胁可能性的经验和适用的统计数据；
   2) 对故意的威胁：随时间而变的动机和能力，潜在攻击者可用的资源，以及潜在攻击者对资产吸引力和脆弱性的感知；
   3) 对意外的威胁或环境的威胁：地理因素、极端天气情况的可能性、可能导致人为错误或设备故障的因素；
   4) 工业控制系统所属企业或行业固有的单个和聚集的脆弱性。

d) 根据工业控制系统所属企业或行业通常对待安全事件可能性的敏感程度，或对安全事件发生的可接受程度进行判断，确定是否可以容忍一定概率的信息安全事件发生；

e) 根据以上分析，对威胁列表的每个威胁给出信息安全事件的可能性“高”或“低”的评价。

6.5.3 评价需抵御的信息安全威胁程度

评价工业控制系统需抵御的信息安全威胁程度，包括：

a) 根据 6.5.2 形成的威胁列表，选择所有信息安全事件的可能性“高”的威胁作为定级的工业控制系统需抵御的信息安全威胁；

b) 比较定级的工业控制系统需抵御的所有的信息安全威胁，选择其中威胁程度特征值（取值范围为 1-5）最高的，判定为定级的工业控制系统需抵御的信息安全威胁程度特征值。

6.6 确定工业控制系统信息安全等级

根据5.1的要求，用已确定的工业控制系统资产重要程度特征值、受侵害潜在影响程度特征值、工业控制系统信息安全威胁程度特征值，在表1中查找对应的级别，即可确定基于工业控制系统信息安全风险的工业控制系统信息安全等级。

附 录 A 全面性等级定义

A.1 域全面性等级及相应目标

安全管理目标	
为安全考虑建立一个总体基础	1 / 最低
建立基线安全措施	2 / 临时
促进安全能力的实施	3 / 一致
设定一个明确的治理结构和流程	4 / 正规
安全实现目标	
使得可用的安全控制措施得到使用	1 / 最低
根据已知的使用场景实施安全控制	2 / 临时
采用内置的和额外的机制来覆盖已知的风险	3 / 一致
建立程序，以最佳方式处理风险	4 / 正规
安全加固目标	
应用公认的网络卫生的做法	1 / 最低
根据其需求和优先级改善系统保护	2 / 临时
采用公认的方法和工具，使其具有可信度	3 / 一致
建立支持可信度目标的持续过程	4 / 正规

A.2 子域的全面性等级及相应目标

策略与管理需要：	
愿景、范围和安全目标	1 / 最低
最合适的最佳实践	2 / 临时
被公认的方法和标准	3 / 一致
支持业务流程、法律、运营和其他问题	4 / 正规
威胁模型与风险评估需要：	
审查当前的威胁状况	1 / 最低
了解系统和技术的脆弱性	2 / 临时
对相关风险的全面描述	3 / 一致
整体和系统的风险管理方法	4 / 正规
供应链和外部依赖性管理需要：	
对供应商和承包商进行信誉检查	1 / 最低
供应链的最低安全保证工件	2 / 临时
由受信任的机构提供证书和其他保证	3 / 一致
控制供应商和承包商可能造成的危害	4 / 正规
身份和访问控制需要：	
支持基本使用场景下的基本实体	1 / 最低

区分一般访问场景下的行为者	2 / 临时
采用最佳实践来支持复杂的访问场景	3 / 一致
全面保护，防止与未经授权的访问有关的风险	4 / 正规
资产保护需要：	
对数字和实物资产的使用进行核算	1 / 最低
基于用例对资产进行监控	2 / 临时
管理和保护各种类型的资产	3 / 一致
保证资产管理政策的执行	4 / 正规
数据保护需要：	
普遍维护数据的保密性和完整性	1 / 最低
对某些数据的保密等级提高	2 / 临时
实施公认的数据保护政策和方法	3 / 一致
保证关键业务信息在传输和静止状态下得到保护	4 / 正规
漏洞与补丁管理需要：	
保持系统的最新状态避免被攻击	1 / 最低
对关键组件执行定期更新政策	2 / 临时
支持特殊场景配置自动更新	3 / 一致
计划定期更新过程和关键 0day 的应急方案	4 / 正规
态势感知需要：	
保持对安全相关事件的最低限度的了解	1 / 最低
对某些类型的安全事件的特别关注	2 / 临时
全面监测和定期分享安全相关信息	3 / 一致
提供和管理所有与可信度方面有关的信息	4 / 正规
应急响应与业务连续性需要：	
检查事故后的系统恢复情况	1 / 最低
确保独立的系统组件或程序的恢复	2 / 临时
在可能的情况下支持自动恢复程序并适当报告	3 / 一致
通过技术和组织手段，对事件作出迅速反应，减少对业务的损害	4 / 正规

A.3 实践的全面性等级及相应目标

安全方案管理目标：	
描述一般的安全规定	1 / 最低
参考相关的安全目标以及解决方案	2 / 临时
涵盖公认的安全管理标准的一般主题	3 / 一致
实施明确的计划，及时提供和控制安全活动	4 / 正规
合规管理目标：	
注意合规性的驱动因素	1 / 最低
考虑一些可选的合规性要求的实施	2 / 临时
实施强制性的合规要求	3 / 一致
监测不断变化的标准要求	4 / 正规
威胁模型目标：	

将一般的 IT 安全问题称为威胁	1 / 最低
以临时的方式识别和描述威胁	2 / 临时
以准确（可选择正式）的方式对威胁进行描述和分类	3 / 一致
揭示并明确描述可能使系统处于风险中的已知和特定的 IT 因素	4 / 正规
风险态度的目标：	
非正式地定义风险的概念	1 / 最低
区分风险的重要性	2 / 临时
衡量并适当地管理风险	3 / 一致
使用风险管理框架和程序	4 / 正规
产品供应链风险管理目标：	
监控所提供的部件的漏洞和补丁	1 / 最低
对所提供的组件实施一些安全测试	2 / 临时
为基本组件获得证书或其他安全保证文件	3 / 一致
应用供应链风险管理政策	4 / 正规
第三方服务依赖管理目标：	
监测承包商的信誉	1 / 最低
通过合同协议规定服务的质量	2 / 临时
获得服务质量的第三方证据	3 / 一致
对承包商适用统一的可信度管理政策	4 / 正规
实体建立和维护目标：	
以相同或非常相似的方式维护一个或几个账户	1 / 最低
为几组人、系统或事物管理身份	2 / 临时
利用自动机制支持各种不同的身份	3 / 一致
在人、系统和事物的整个生命周期中维护和控制其身份的使用	4 / 正规
访问控制的目标：	
只限制外部代理访问系统的能力	1 / 最低
考虑主体的角色并控制适当的访问权限	2 / 临时
使用具有适当级别的可用访问控制政策	3 / 一致
严格按照业务需求和限制条件来维护授权计划	4 / 正规
资产、变更和配置管理的目标：	
追踪资产和配置的非经常性变化	1 / 最低
遵循一些特定的规则来管理系统的可能变化	2 / 临时
支持资产和/或配置数量的变更管理程序	3 / 一致
规范资产的生命周期，从提供到更换的过程，包括紧急变更	4 / 正规
物理保护的目标：	
通常限制对实物资产的访问	1 / 最低
定制访问限制，考虑物理访问的时间和方式	2 / 临时
使用特定的身份令牌，自动进行可调整的物理访问控制	3 / 一致
解决物理安全和安全的所有方面，防止盗窃，并确保持续的安全运行	4 / 正规
数据的安全模型和策略目标：	
声明数据应受到保护，防止未经授权的访问	1 / 最低
设置简单的数据分类和适当的约束	2 / 临时
定义特定的方法和角色/属性来控制对数据的访问	3 / 一致

根据相关人员的要求，对数据进行分类和持续保护	4 / 正规
数据保护控制实施的目标：	
利用内置的保护控制（操作系统、网络、服务）	1 / 最低
配置内置控制，并确保其使用符合数据保护目标	2 / 临时
根据公认的标准，支持数据控制的正确应用	3 / 一致
确保每个数据项目在传输和静止时都得到所需的保护	4 / 正规
漏洞评估的目标：	
考虑广为人知的漏洞是否与系统有关	1 / 最低
检查指定的组件是否容易受到攻击	2 / 临时
获得一个客观的第三方对漏洞和暴露的评估	3 / 一致
定期执行深度定制的安全检查	4 / 正规
补丁管理的目标：	
考虑供应商发布的安全公告，并安装适当的修补程序	1 / 最低
检查指定的组件是否受到保护，防止最可能的攻击	2 / 临时
尽可能建立自动更新程序	3 / 一致
执行系统政策，保证持续保护，防止已知攻击	4 / 正规
实践监控的目标：	
不时地检查系统日志以进行诊断	1 / 最低
定期检查表明关键进程执行得如何的事件	2 / 临时
使用内置和专门设计的工具收集和分析与安全有关的信息	3 / 一致
作为持续系统保护的催化剂和能力建设者	4 / 正规
态势感知与信息共享的目标：	
临时获得一些相关的外部信息	1 / 最低
使人员能够持续使用相关的外部信息反馈	2 / 临时
根据情况考虑与当局和社区共享内部数据	3 / 一致
在整个行业内建立一个双向的 0day 和事件共享	4 / 正规
事件检测与响应计划的目标：	
界定具体的事件和反应的基本行动	1 / 最低
为关键部件提供关于如何检测和应对事件的指导	2 / 临时
设置自动执行响应程序基础	3 / 一致
建立检测事件的控制措施，分配进行调查，并根据需要进行升级	4 / 正规
补救、恢复和业务连续性的目标：	
给予系统恢复的基本指示	1 / 最低
处理已知的事件，并检查系统是否完全恢复	2 / 临时
实现补救和恢复程序的自动执行	3 / 一致
支持技术和组织措施的结合，促进系统快速恢复	4 / 正规