附件:

# 工业控制系统信息安全防护能力评估方法

## 1.适用范围

1.1 本方法提出了工业控制系统信息安全防护能力评估的基本概念、实施流程和工作形式。

1.2 本方法适用于规范对企业按照《工业控制系统信息安全防护指南》建立的工控安全防护能力开展的综合评价活动。

1.3 本方法适用于评估工业控制系统的应用企业。

## 2. 规范性文件

2.1 法律法规、指导性文件

《中华人民共和国网络安全法》

《国家网络空间安全战略》

《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）

《国务院关于印发〈中国制造 2025〉的通知》（国发〔2015〕28 号）

《国务院关于积极推进“互联网+”行动的指导意见》（国发〔2015〕40 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）

《工业控制系统信息安全防护指南》（工信部信软〔2016〕338号）

《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）

2.2 标准和技术规范

GB/T 32919－2016 《信息安全技术 工业控制系统安全控制应用指南》

GB/T 20984－2007 《信息安全技术 信息安全风险评估规范》

## 3. 术语与定义

下列术语和定义适用于本方法。

3.1 工业控制系统

工业生产控制各业务环节涉及的有关人员、软硬件系统和平台的集合。包括但不限于：可编程逻辑控制器（PLC）、分布式控制系统（DCS）、数据采集与监控系统（SCADA）等工业生产控制系统；紧急停车系统（ESD）、安全仪表系统（SIS）等工业控制过程安全保护系统；制造执行系统（MES）、企业资源计划系统（ERP）等工业生产调度与管理信息系统；工业云平台、工业大数据平台等工业服务应用系统。

3.2 工业控制系统信息安全防护

通过实施管理和技术措施，避免工业控制系统遭到非授

权或意外的访问、篡改、破坏及损失。

3.3 工业控制系统信息安全防护能力评估

从综合评价的角度，运用科学的方法和手段，系统地分析和诊断工业控制系统所面临的威胁及其存在的脆弱性，评估企业工业控制系统安全防护水平，提出有针对性的抵御威胁的防护对策和整改措施，为最大限度地保障信息安全提供科学依据。

3.4 工业控制网络

企业管理层之下的网络，包括现场设备层、生产控制层、制造执行层等所在的网络区域。

3.5 工业主机

工业生产控制各业务环节涉及组态、操作、监控、数据采集与存储等功能的主机设备载体，包括工程师站、操作员站、历史站等。

3.6 工业控制设备

工业生产过程中用于控制执行器以及采集传感器数据的装置，包括 PLC、DCS、远程测控终端（RTU）等。

3.7 资产

工业生产过程中具有价值的信息或资源，是安全防护的对象。

3.8 信息安全风险

人为或自然的威胁利用工业控制系统及其管理体系中

存在的脆弱性导致安全事件的发生及其对企业造成的影响。

3.9 威胁

可能导致对工业控制系统或企业危害的不希望事故潜在起因。

3.10 脆弱性

可能被威胁所利用的资产或若干资产的薄弱环节。

3.11 工业控制系统配置清单

包含工业控制系统正常运行所需配置的硬件、软件、文档、组件等信息的清单。

3.12 安全配置

工业控制系统为实现特定的安全防护功能而执行的配置策略。

3.13 物理安全防护区域

为保护工控系统不受人为或自然因素危害，需采取门禁、安防、人工值守等物理安全手段的特殊区域。

3.14 评估报告

评估机构根据评估方法的要求，在履行必要的评估程序后，对被评估对象出具的书面工作报告，是评估机构履行评估任务或评估委托的成果。

3.15 评估结论

评估机构在评估报告中作出的总体性判断意见。判断意见分为优秀（90 分以上）、良好（80~89.5）、一般（70~79.5）、

基本合格（60~69.5）、不合格（60 分以下）。

## 4. 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、组建评估技术队伍、制定评估工作计划、开展现场评估工作、现场评估情况反馈、企业自行整改、开展复评估工作和形成评估结论八个部分。

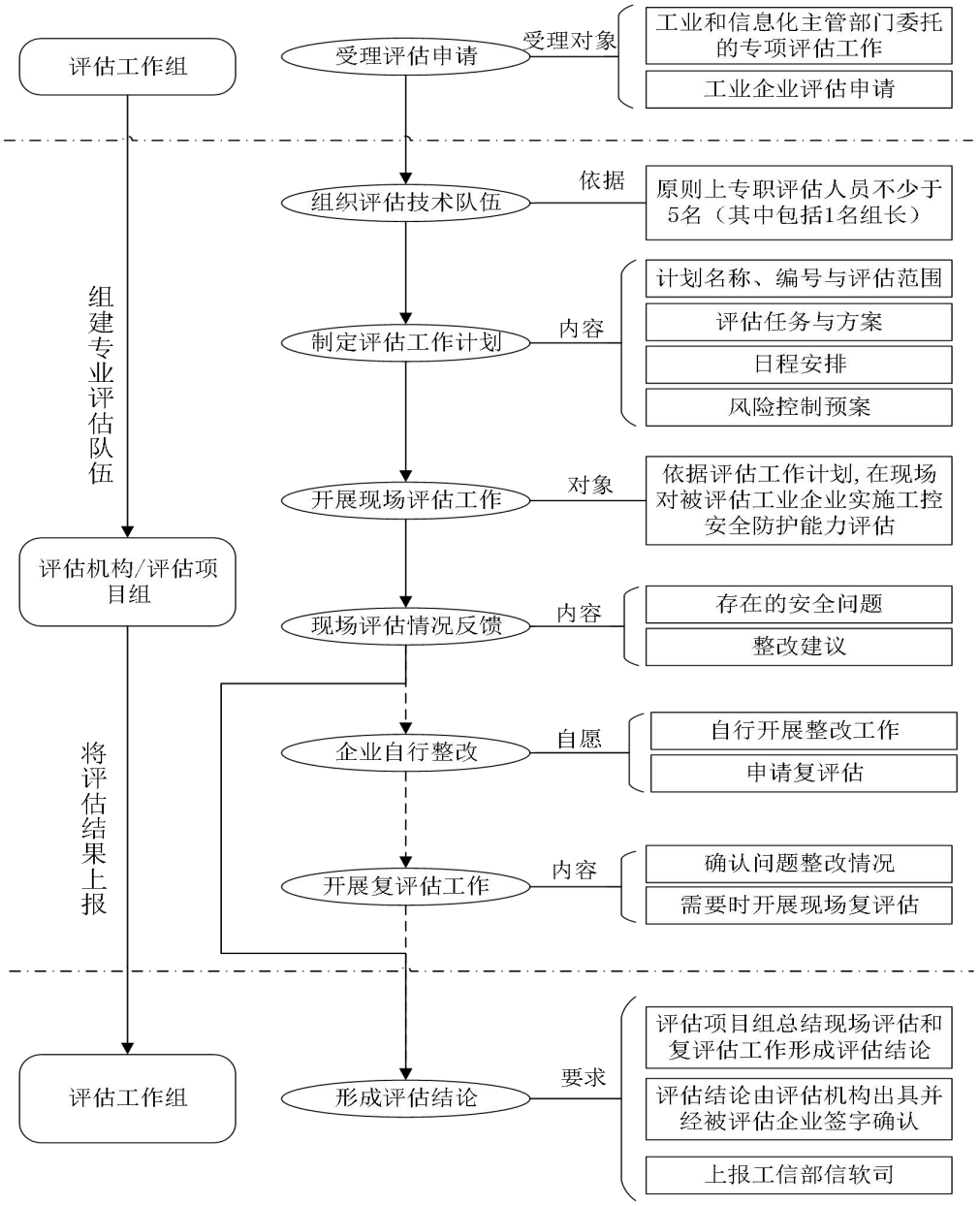


图 1 工业控制系统信息安全防护能力评估工作程序图

## 5. 评估工作实施

5.1 受理评估申请

评估工作组受理工业和信息化主管部门委托的专项评估工作，各评估机构可自行受理市场化的评估工作委托，并在评估工作组备案。

5.1.1 主管部门工作委托

工业和信息化主管部门，通过任务函等方式委托评估工作组开展工业控制系统信息安全防护能力评估专项工作。评估专项工作任务指定的被评估企业，应按要求向评估工作组提供 5.1.2 中（2）-（5）所需的评估材料。评估工作组根据工作任务量、地理位置等综合因素统筹确定评估机构，委托开展评估工作。

5.1.2 企业评估申请受理

企业可自行委托评估机构开展工业控制系统信息安全防护能力评估工作。申请企业需向评估机构提交以下评估申请材料：

（1）工业控制系统信息安全防护能力评估备案表；

（2）申请企业加注统一社会信用代码的的营业执照；

（3）申请企业简介、企业工业生产控制系统简介；

（4）围绕《工业控制系统信息安全防护指南》已实施的安全防护措施介绍；

（5）其它与评估工作有关的必要文件。

各评估机构对申请企业提交的材料进行审理，并根据申请企业申请的评估范围、完成评估所需时间及其他影响评估活动的因素，综合确定是否受理评估申请。如评估机构确定受理，需将材料（1）递交至评估工作组备案。

5.2 组建评估技术队伍

5.2.1 评估协议签订

评估机构应及时与被评估企业沟通，并签订书面的评估委托协议（或评估合同），以规范评估工作的顺利开展，保障企业的安全生产运行和数据安全。

5.2.2 评估技术队伍组建

评估机构应根据工业控制系统信息安全防护能力评估范围所覆盖的专业领域选择具备相关能力的评估人员和技术专家，组建评估项目组。评估项目组原则上应具备不少于5名专职评估人员，其中包括1名评估项目组组长。

评估项目组组长由评估机构指定经验丰富的骨干评估人员担任，负责统筹安排评估工作分工，推进评估工作开展，组织完成评估结论、编写评估报告。

评估项目组成员由评估机构根据该项评估的工作量及涉及的工业行业特征、专业需求等综合因素，确定成员数量和成员搭配。

5.3 制定评估工作计划

评估项目组应与被评估企业的管理人员和技术人员应

当充分沟通，明确被评估范围和评估对象，制定评估工作计划。被评估企业和评估项目组共同确认上述工作计划后，再开展实施具体评估工作。

5.3.1 建立评估项目文档

在评估工作开展过程中，评估机构应对评估工作相关文件进行统一编号，并规范管理。

5.3.2 梳理基本情况

在被评估企业的配合下，评估项目组对企业工业控制系统及相关信息进行梳理，以便针对性地开展评估工作。

（1）梳理企业基本信息

了解被评估企业的发展历程、主要业务范围、业务规模，分析企业对于国家、社会、人民生命财产的重要性。

（2）梳理企业生产资产基本信息

了解企业被评估工业控制系统所涉及的资产类型、规模、位置、重要程度、产品、数量、厂商、投产时间、责任人、网络拓扑及其运营维护等情况。

（3）梳理企业工控安全防护基本情况

了解被评估企业的工控安全管理机制建设情况，初步掌握企业已部署的工控安全防护措施。

5.3.3 确定评估范围

与被评估企业沟通，根据评估专项工作要求或企业自身需求确定评估范围。评估范围可以是企业的一套或多套工业

生产系统。

5.3.4 确定评估方案

评估机构在前期梳理工业控制系统基本情况、确定评估范围的基础上，结合评估工作实际，参照 5.4 相关内容，制定该企业评估方案。

评估方案涉及的评估方式至少包括：（1）人员访谈。评估项目组对相关人员进行访谈，核实已落实防护措施情况。（2）文档查阅。评估项目组查阅已落实防护措施形成的相关文档等证明材料。（3）人工核查。评估项目组通过手动方式核查部分已落实防护措施情况。（4）工具检测。评估项目组通过专用工具检测防护措施实际落实情况及其有效性。

5.3.5 确定评估工作日程安排

评估项目组与被评估企业充分沟通，梳理评估工作重要时间节点，合理设置评估时间，确定评估工作日程安排。

5.3.6 确定评估工具

评估项目组根据评估工作实际需求，并与被评估企业沟通确认后，参照附录 B，选择相对应的专项评估工具用于现场评估工作。

5.3.7 确定应急预案

评估项目组与被评估企业充分沟通，确定评估工作应急预案。应急预案应至少包括确定恢复点目标与恢复措施、按照事件分类等级制定应急响应保障措施等方面。

5.3.8 其它工作要求

评估机构应当与被评估企业充分沟通评估工作计划，按照尽量不影响企业正常生产和工控系统正常运行的原则，科学有序地开展评估工作。评估工作结束后，应及时清除评估过程中形成的测试数据。

5.4 开展现场评估工作

为确保工业控制系统信息安全防护能力评估工作规范全面开展，依据《工业控制系统信息安全防护指南》主要内容，应从如下方面开展评估工作。

5.4.1 安全软件选择与管理防护评估

**（一）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，只允许经过企业自身授权和安全评估的软件运行。**

**1.安全要求**

a)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服务的运行；

b）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测试验证,确保其不会对工业控制系统的正常运行造成影响。

**2.评估内容及方法**

a)查阅工业主机上安装防病毒软件或应用程序白名单软

件的证明材料（如采购合同、服务协议等），评估其来源是否安全正规；

b）核查其工业主机防病毒软件或应用程序白名单软件是否已安装运行、病毒库或白名单规则是否及时升级（原则上3个月内）。若未及时升级，查阅不适合升级病毒库的分析报告；

c)查阅防病毒软件或应用程序白名单软件已在离线或测试环境中充分测试验证的技术报告，评估其是否影响工业控制系统正常运行。

**（二）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。**

**1. 安全要求**

a)企业应建立工业控制系统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）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。

**2.评估内容及方法**

a)查阅企业已建立防病毒和恶意软件入侵管理机制的证明材料（如入侵管理章程等），评估其内容是否完备、合理；

b）访谈企业相关人员对该入侵管理机制的知悉程度，或采用人工核查方式，评估入侵管理机制是否被严格贯彻执

行；

c）查阅企业临时接入工控系统的设备查杀登记记录文档，并通过现场核验等方式，核查企业工业主机防病毒软件查杀历史记录。

5.4.2 配置和补丁管理防护评估

**（一）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。**

**1. 安全要求**

a）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策略配置，确保工业控制系统相关安全配置的有效性；

b）企业应建立工业控制系统安全策略配置清单，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)企业应定期自行对工业控制系统安全配置进行核查审计，避免因调试或其它操作导致配置变更后，未及时更新配置清单。

**2.评估内容及方法**

a）核查企业工业控制网络安全配置（如网络分区、端口禁用等）、工业主机安全配置（如远程控制管理、默认账户管理等）、工业控制设备安全配置（如口令策略合规性等）是否落实，评估其安全配置是否存在安全风险隐患；

b）查阅工业控制系统安全配置清单；

c）查阅企业工业控制系统安全配置清单审计记录（如配置核对表）。

**（二）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。**

**1.安全要求**

a）企业应在发生重大安全配置变更（如重新划分网络）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）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。

**2.评估内容及方法**

a）检查企业安全配置变更计划相关文档材料(如影响分析报告等)，确定其是否明确变更时间、变更内容、变更责任人、变更审批、变更验证等事项，评估其配置变更计划是否会降低企业工业控制系统安全防护水平、是否会影响工业控制系统正常运行；

b）检查企业安全配置变更前开展安全测试的测试验证报告，确定其是否包含风险分析等内容，评估配置变更测试验证是否有效规避安全风险、不会影响工业控制系统正常运行。

**（三）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。**

**1.安全要求**

a)企业应密切关注重大工控安全相关漏洞和可能影响工控安全的主机软硬件漏洞，及时跟踪补丁发布，并一定时间内（原则上不超过 180 天）及时开展补丁升级或消减措施，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）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。

**2.评估内容及方法**

a)查阅企业印发的重大工控安全相关漏洞和可能影响工控安全的主机软硬件漏洞的风险通报及补丁升级通知，评估企业是否密切关注重大工控安全漏洞及补丁发布；

b）核查企业工控安全漏洞补丁升级记录，评估企业工业控制系统是否已安装最新版补丁程序；

c)查阅企业补丁安装前进行安全评估测试的相关证明材料（如安全评估测试方案、测试报告等），评估其是否进行补丁安全测试。

5.4.3 边界安全防护评估

**（一）分离工业控制系统的开发、测试和生产环境。**

**1.安全要求**

a）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。

**2.评估内容及方法**

a）人工核查或工具检测的方式，检查企业为工业控制系统开发、测试和生产环境是否分离（如网络是否相连、生产环境是否存在测试账户/数据等）。

**（二）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。**

**1.安全要求**

a）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）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。

**2.评估内容及方法**

a）以人工核查或工具检测的方式，检查工业控制网络是否在无防护状态下直接连接互联网；

b）查阅企业工业控制网络拓扑结构、网络边界防护设备的部署情况相关材料，分析是否在不同网络边界之间部署边界安全防护设备，评估有效实现安全访问控制、阻断非法

网络访问等功能；

c）以人工核查或工具检测的方式，核实企业工业控制网络边界防护设备部署是否与企业提供材料相一致，检查安全防护设备配置策略，评估其部署实施情况的真实性。

**（三）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。**

**1.安全要求**

a)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）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。

**2.评估内容及方法**

a）查阅企业工业控制网络拓扑结构等相关文档，并通过人工核查评估其是否依据区域重要性和业务需求合理划分工业控制网络安全区域；

b）查阅企业工业控制网络安全防护设备部署实施相关证明材料（如网络拓扑结构图、网络安全防护设备采购合同、安全防护设备配置策略等），评估其是否依据工业控制网络安全区域实施逻辑隔离安全防护以满足企业网络边界防护需求；

c）以人工核查或工具检测等方式，检查工业控制网络安全防护设备部署实施实际情况，检查安全防护设备配置策

略，确定其与企业提供材料的一致性。

5.4.4 物理和环境安全防护评估

**（一）对重要工程师站、数据库、服务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。**

**1.安全要求**

a）企业应自行基于重要工程师站、数据库、服务器等核心工业控制软硬件明确重点物理安全防护区域；

b)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。

**2.评估内容及方法**

a）以人工核查等方式，检测企业是否明确划分重点物理安全防护区域；

b）查阅企业针对重要工业控制系统资产所在区域采用适当物理安全防护措施的相关文档材料（如物理安全防护措施规章制度等），以评估企业是否严格实施相关规章制度以及该规章制度是否满足企业安全需求；

c）查阅人员值守记录，并以人工核查等方式，现场核查企业是否针对重要资产区域开展安全防护，评估其是否严格落实安全措施规章制度。

**（二）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。**

**1.安全要求**

a）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，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，以避免未授权的外设终端接入。

**2.评估内容及方法**

a）人工核查企业是否拆除或封闭工业主机上不必要的 USB、光驱、无线等接口；

b）人工核查或工具检测工业主机是否存在 USB 等外设接口使用痕迹，检查是否有未授权的外设终端接入记录；

c）查阅企业主机外设接口管理制度，在适用时，人工核查、工具检测等方式验证企业主机外设安全管理技术手段实施情况，以技术手段评估企业是否落实管理技术手段。

5.4.5 身份认证防护评估

**（一）在工业主机登录、应用服务资源访问、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。**

**1.安全要求**

a）企业应在工业主机登录、应用服务资源访问、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）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。

**2.评估内容及方法**

a）查阅企业身份认证管理制度，以人工核查、人员访谈等方式，检查企业身份认证管理技术实施情况，评估身份认证方式是否满足企业安全要求；

b）若企业存在关键设备、系统和平台，以人工核查等方式，审核是否采用多因素认证方式，评估身份认证方式是否满足安全强度要求。

**（二）合理分类设置账户权限，以最小特权原则分配账户权限。**

**1.安全要求**

a）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）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)企业需定期自行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。

**2.评估内容及方法**

a）人工核查、文档查阅等方式，检查企业是否根据不同业务需求、岗位职责等，分类设置账户，并评估其合理性；

b）查阅企业系统账户权限分配规则，评估其是否按照最小特权原则进行权限分配；

c）人工核查或工具检测等方式，评估工业控制系统账户分配规则是否严格贯彻执行；

d）查阅企业工业控制系统账户权限分配情况的定期审计记录（如账户权限核对表），评估审计工作是否按时有效执行。

**（三）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。**

**1.安全要求**

a）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）企业应定期更新口令。

**2.评估内容及方法**

a）人工核验、工具检测等方式，核查企业的工业控制设

备、SCADA 软件、工业通信设备等登录账户及密码设定情况，账户密码管理制度，评估其强度及管理制度是否满足需求；

b）以人工核验、工具检测等方式，核实企业的工业控制设备、SCADA 软件、工业通信设备未使用默认口令或弱口令；

c）以人工访谈方式，核实企业是否定期更新口令。

**（四）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。**

**1.安全要求**

a）适用时，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。

**2.评估内容及方法**

a）人员访谈了解企业身份认证证书技术实现方式，对已使用身份认证证书的企业，核查其传输、存储方式是否安全。

5.4.6 远程访问安全防护评估

**（一）原则上严格禁止工业控制系统面向互联网开通 HTTP、FTP、Telnet 等高风险通用网络服务。**

**1.安全要求**

a）适用时，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 等高风险通用网络服务。

**2.评估内容及方法**

a）人员访谈企业工业控制系统是否面向互联网开通HTTP、FTP、Telnet等高风险通用网络服务；

b）通过人工核查或工具检测等方式，验证工业控制系统是否面向互联网开通HTTP、FTP、Telnet等高风险通用网络服务。

**（二）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。**

**1.安全要求**

a）企业应采用数据单向访问控制、VPN、堡垒机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）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。

**2.评估内容及方法**

a）以人工核查或工具检测等方式，检查企业是否采用数据单向访问控制等策略对远程访问进行安全加固，评估其安全加固措施是否满足企业安全和业务需要；

b）通过文档查阅、工具检测或人工核查等方式，评估企业是否针对远程访问控制采用时限控制或锁定策略等方式确保远程访问的安全可控。

**（三）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。**

**1.安全要求**

a）适用时，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）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。

**2.评估内容及方法**

a）通过人工核查等方式，核查企业远程维护通道是否采用 VPN 等远程接入方式；

b）查阅企业远程接入账户管理制度相关文档，核查其是否对接入账户实行专人专号，评估其账户申请、使用、收回等流程是否规范。

**（四）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。**

**1.安全要求**

a)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）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。

**2.评估内容及方法**

a）查阅工业控制系统访问日志相关文档材料、定期备份

材料，评估其访问日志及定期备份日志是否能记录工业控制系统访问情况，并满足企业安全审计需要；

b）查阅企业审计制度相关文档，评估企业审计制度是否合理，是否定期开展审计工作。

5.4.7 安全监测和应急预案演练防护评估

**（一）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。**

**1.安全要求**

a）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。

**2.评估内容及方法**

a）通过人员核查、文档查阅等方式，核查企业是否在工业控制网络部署了网络安全监测设备；

b）以人工核查或工具检测等方式，评估该监测设备是否可及时可发现、报告网络攻击或异常行为；

c）以人工核查等方式，核查该监测设备是否具备处理异常行为的功能。

**（二）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。**

**1.安全要求**

a）企业应根据自身情况，明确重要工业控制设备清单；

b）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。

**2.评估内容及方法**

a）适用时，查阅重要工业控制设备清单；

b）适用时，通过人工核查或工具检测等方式，检查企业部署深度包分析和过滤功能防护设备的实施情况，并核查安全防护设备配置策略，评估其是否满足限制违法操作的安全要求。

**（三）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。**

**1.安全要求**

a）企业应专门制定工控安全事件应急响应预案，确保企业正确应对安全事件；

b）适用时，当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。

**2.评估内容及方法**

a）人员访谈、查阅企业工控安全事件应急响应预案相关文件，评估其科学性、合理性；

b）查阅企业是否明确具有保护现场和调查取证相关流程和要求，适用时，查阅相关执行记录；

c)查阅企业工业控制系统信息安全威胁事件报送机制相关流程及要求，适用时，查阅相关执行记录。

**（四）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。**

**1.安全要求**

a)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）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。

**2.评估内容及方法**

a)人员访谈、查阅企业应急响应预案演练相关记录文档，评估是否定期组织相关人员开展应急响应预案演练及演练是否覆盖应急预案的全部内容；

b）查阅企业应急预案修订记录，评估其是否及时对其应急响应预案进行修订。

5.4.8 资产安全防护评估

**（一）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。**

**1.安全要求**

a）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）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。

**2.评估内容及方法**

a）查阅企业工业控制系统资产清单相关文档材料，评估资产信息是否完整和准确，并通过工具检测验证资产实际情况与资产清单的一致性；

b）查阅企业工业控制系统资产责任人相关材料（如资产登记表等），评估资产责任人是否明确，访谈资产责任人是否知悉其相关责任；

c）查阅企业资产使用处置规则、处置记录文档等，评估处置规则是否得到有效执行。

**（二）对关键主机设备、网络设备、控制组件等进行冗余配置。**

**1.安全要求**

a）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）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（如双机冷/热备等），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。

**2.评估内容及方法**

a）查阅企业关键主机设备、网络设备、控制组件清单；

b）以人工核验等方式，核查企业是否针对关键主机设备、网络设备、控制组件等实行了“一主一备”冗余配置。

5.4.9 数据安全防护评估

**（一）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。**

**1.安全要求**

a）企业应明确识别重要工业数据清单（如通过 OPC 采集的生产数据、历史站存储的数据等）；

b）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)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）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。

**2.评估内容及方法**

a）查阅企业是否建立重要工业数据清单；

b）通过人工核查或工具检测等方式，核查企业是否针对静态存储重要工业数据进行加密存储、访问控制等防护，评估其能否满足企业静态存储数据的安全防护要求；

c）通过人工核查或工具检测等方式，检查企业是否采取加密传输、VPN 等方式保护动态传输过程中重要工业数据，评估其能否满足企业动态传输数据的安全防护要求；

d）查阅企业数据管理相关文档材料，评估其是否建立数据分级分类管理制度，通过人工核查的方式，评估企业是否严格实施数据分级分类管理制度。

**（二）定期备份关键业务数据。**

**1.安全要求**

a）企业应建立关键业务数据清单（如生产工艺、生产计划、组态文件、调度管理等数据）；

b）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）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。

**2.评估内容及方法**

a）查阅企业是否建立关键业务数据清单（如工业参数、配置文件、设备运行数据、生产数据、控制指令等）；

b）检查企业关键业务备份数据、数据备份日志文件，评估其是否对关键业务数据进行了定期备份；

c）核查备份方式、备份周期等策略是否满足企业数据备份需求；

d）核查相关恢复测试记录文档，评估是否定期开展恢复测试，并判断恢复测试的有效性。

**（三）对测试数据进行保护。**

**1.安全要求**

a）企业应对测试过程中产生的数据进行保护，以确保企业测试数据的安全；

b）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。

**2.评估内容及方法**

a）以人工核查或工具检测等方式，对企业测试过程中产生的数据保护进行审核，评估测试数据是否存在被未授权获取及使用的风险；

b）以人员访谈等方式，评估企业是否使用实际生产数据等敏感数据进行测试；

c）适用时，以人员访谈、工具检测等方式，评估企业测试数据是否去除所有敏感细节和内容。

5.4.10 供应链管理防护评估

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

**1.安全要求**

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

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

**2.评估内容及方法**

a）查阅企业与工业控制系统服务商签署的合同等资料，评估其是否以明文条款的方式约定服务商在服务过程中应当承担的信息安全责任和义务；

b）查阅工业控制系统服务商已向企业提供的相关证明材料（如工控安全合同、工控安全防护案例、验收报告等），评估服务商是否具有工控安全防护经验且专业可靠。

**（二）以保密协议的方式要求服务商做好保密工作，防范敏感信息外泄。**

**1.安全要求**

a)企业应与服务商签订保密协议，确保敏感信息不外泄。

**2.评估内容及方法**

a）查阅企业与服务商签订的保密证明材料（如保密协议等），审核协议中是否约定保密内容、保密时限、违约责任等内容，评估是否存在工业控制系统敏感信息外泄的风险。

5.4.11 落实责任防护评估

**（一）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。**

**1.安全要求**

a）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）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）企业应在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。

**2.评估内容及方法**

a）查阅企业工业控制系统安全管理机制等文档（如人员工控安全培训制度、应急响应与演练制度、风险评估制度等），评估其指导工业控制系统安全管理工作的有效性；

b）查阅信息安全协调小组成立相关文档材料，评估小

组成员构成的合理性；同时通过人员访谈评估，评估小组成员对自身职责的熟悉程度；

c）访谈工控安全管理责任人，评估工控安全责任制和安全防护措施的落实情况。

5.5 现场评估情况反馈

现场评估工作结束后，评估项目组应在 1 个工作日内对评估过程及评估记录进行梳理、汇总，针对现场评估工作形成书面现场评估情况反馈表，描述存在的安全问题及整改建议。

5.6 企业自行整改

企业在收到反馈表后 30 日内，可根据自身实际情况，按照反馈表内容开展整改工作，并根据整改情况向评估机构或评估项目组申请复评估。

5.7 开展复评估工作

评估机构在收到企业复评估的请求后，根据需要对现场评估反馈表中的问题进行确认。必要时，采取现场复评估方式对整改企业所采取的整改措施的有效性进行验证。

5.8 形成评估结论

5.8.1 评估项目组形成结论

根据现场评估和复评估工作情况，评估项目组形成企业工控安全防护能力评估结论，并编制《工业控制系统信息安全防护能力评估报告》。评估报告由评估机构盖章出具并由

评估项目组组长、责任审核人签字。评估报告应准确、清晰地描述评估活动的主要内容，并附必要的证明相关事实的证据或记录。

5.8.2 评定报告的审定

评估机构形成的评估报告需上报评估工作组。评估工作组组织对评估过程中生成的文件和记录的合规性进行审查，确认相关材料完整规范。通过合规性审查的评估报告，由评估工作组报备工业和信息化部信息化和软件服务业司，并在一定范围内予以公示。未通过审核的评估报告予以驳回，评估机构需及时补充及完善相关材料，并再次由评估工作组进行合规性审查。

根据各评估机构提交的评估报告数量，评估工作组不定期委托评估专家委员会对评估结论开展必要的抽查与复核活动（包括到企业现场复核形式），未通过抽查与复核的评估结论予以撤销。

5.8.3 定期评估要求

按照《网络安全法》第 38 条要求，重要工业企业原则上宜每年进行一次评估，以适应企业控制系统不断变化的要求。评估所形成的评估得分及报告，仅是对评估时工控系统安全防护状况的表述。建议其他工业企业每年至少进行 1 次自评估或委托第三方评估。

# 附录 A 工业控制系统信息安全防护能力评分标准

本部分依据《工业控制系统信息安全防护指南》以及本方法中的评估内容及方法，明确了具体的评分方式，评价企业工业控制系统信息安全的防护能力的情况，并给出量化的评分标准。本评分标准从 11 个方面设置了 30 个大项，61 个小项，129 个评分细项。

## A.1 评分方法及原则

1）评分方法。评估标准满分为 100 分，评分采用扣分制，评分细项的分值作为评分的最小单元。

2）高风险项。高风险项共 25 小项，其分值相对较高。高风险项是企业工控安全防护中基础和关键的项，高风险项不满足可能造成较大信息安全风险，建议限期整改。

3）基于证据的方法。为了保证评估结果的公正和客观，评分的判断须有充分的证据，证据包括负责人谈话、制度文件、运行记录、核查结果和测试报告等。

## A.2 评分操作方法

见附表：评分操作方法表。

附表：

# 评分操作方法表

| 项目 | | | 评分细则 | 分值 | 备注 |
|---|---|---|---|---|---|
| 一、安全软件选择与管理（4 项 9 分） | （一）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，只允许经过企业自身授权和安全评估的软件运行。 | a）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服务 | 1.工业主机未安装防病毒软件或应用程序白名单软件，扣 4 分；（若本项成立，略过第 2-4 项）<br>2.防病毒软件或应用程序白名单软件的来源不安全正规，扣 1 分；<br>3.病毒库或白名单规则未及时更新，扣 1 分。 | 4 | 高风险项 |
| | | b）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测试验证,确保其不会对工业控制系统的正常运行造成影响 | 4.防病毒软件或应用程序白名单软件未在离线环境测试，扣 1 分。 | | |
| | （二）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）企业应建立工业控制系统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 | 5.未建立工业控制系统防病毒和恶意软件管理制度，扣 3.5 分；（若本项成立，略过第 6-8 项）<br>6.防病毒和恶意软件管理制度不完备、合理；扣 1 分；<br>7.企业人员对制度缺乏了解，扣 1 分；<br>8.制度没有执行或缺乏执行记录，扣 1 分。 | 3.5 | 高风险项 |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | | b）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 | 9.未定期对工业控制系统进行查杀，扣 0.5 分；<br>10.未对临时接入工业控制系统的设备进行查杀，扣 1 分。 | 1.5 | |
| 二、配置和补丁管理<br>（7 项 13.5 分） | （一）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）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策略配置，确保工业控制系统相关安全配置的有效性 | 11.未建立工业控制网络的安全策略配置，扣 1 分；(若本项成立，略过第 12 项)<br>12.工业控制网络的安全策略配置不合理，扣 0.5 分；<br>13.未建立工业主机的安全策略配置，扣 1 分；（若本项成立，略过第 14 项)<br>14.工业主机的安全策略配置不合理，扣 0.5 分；<br>15.未建立工业控制设备的安全策略配置，扣 1 分；(若本项成立，略过第 16 项)<br>16.工业控制设备的安全策略配置不合理，扣 0.5 分。 | 3 | 高风险项 |
| | | b）企业应建立工业控制系统安全策略配置清单，确保该清单满足企业工业控制系统安全可靠运行的需要 | 17.未建立工业控制系统安全策略配置清单，扣 4 分；(若本项成立，略过第 18-20 项)<br>18.工业控制系统安全策略配置清单不全面、不合理，扣 1 分。 | 4 | 高风险项 |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | | c）企业应定期自行对工业控制系统安全配置进行核查审计，避免因调试或其它操作导致配置变更后，未及时更新配置清单 | 19.未定期对配置清单进行更新和维护，扣 1 分；<br>20.未定期审计配置清单，扣 1 分。 | | |
| | （二）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）企业应在发生重大安全配置变更（如重新划分网络）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 | 21.企业未明确定义重大安全配置变更，扣 0.5 分；<br>22.发生重大变更时未制定变更计划，扣 0.5 分；<br>23.重大变更前未进行影响分析和评估，扣 0.5 分。 | 1.5 | 高风险项 |
| | | b）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 | 24.在变更实施前未进行测试，扣 1.5 分；（若本项成立，略过第 25 项）<br>25.必要时，未在离线环境中进行安全验证，扣 0.5 分。 | 1.5 | |
| | （三）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 | a）企业应密切关注重大工控安全相关漏洞和可能影响工控安全的主机软硬件漏洞，及时跟踪补丁发布，并一定时间内（原则上不超过 180 天）及时开展补丁升级或消减措施，确保工业 | 26.未印发或传达重大工控安全相关漏洞和可能影响工控安全的主机软硬件漏洞及补丁升级通知，扣 1 分；<br>27.未及时对重大工控安全相关漏洞和可能影响工控安全的主机软硬件漏洞进行补丁升级，扣 1 分。 | 2 | 高风险项 |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | 全评估和测试验证。 | 控制系统及时针对已知安全漏洞采取安全防护措施 | | | |
| | | b）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 | 28.补丁安装前，未对补丁进行安全评估测试，扣 1.5 分；（若本项成立，略过第 29 项）<br>29.未制定详细的安全评估测试方案及报告，扣 0.5 分。 | 1.5 | |
| 三、边界安全防护<br>（5 项 8.5 分） | （一）分离工业控制系统的开发、测试和生产环境。 | a）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 | 30.工业控制系统的生产环境未与开发、测试环境分离，扣 1.5 分。 | 1.5 | 高风险项 |
| | （二）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。**（注：如被评** | a）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 | 31.在工业控制网络与企业网边界未部署安全防护设备，扣 1.5 分；（若本项成立，略过第 32 项）<br>32.边界安全防护设备未按安全要求进行配置，或功能不满足，扣 1 分。 | 1.5 | 高风险项 |
| | | b）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 | 33.没有防护的工业控制网络与互联网连接，扣 2.5 分。 | 2.5 | 高风险项 |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | **估企业因国家相关保密要求，生产网络与办公网络实现物理隔离，此项不适用）** | | | | |
| | （三）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。**（注：若工业企业已做好工业控制网络的区域划分，且区域之间不可互联互通，则此项不适用）** | a）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 | 34.未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，扣 1.5 分。 | 1.5 | 高风险项 |
| | | b）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 | 35.安全区域隔离策略不满足企业网络边界防护需求，或防护功能不满足，扣 1 分；<br>36.安全防护设备配置策略与企业提供材料不一致，扣 0.5 分。 | 1.5 | |
| 四、物理和环境安全防护（4 项 6.5 分） | （一）对重要工程师站、数据库、服务器等核心工业控制软硬件所在区域采取访问控制、视频 | a）企业应自行基于重要工程师站、数据库、服务器等核心工业控制软硬件明确重点物理安全防护区域 | 37.未明确划分重点物理安全防护区域，扣 1 分。 | 1 | |
| | | b)企业应对重点物理安全防护区域采 | 38.未建立物理安全防护措施，扣 1.5 分；(若本项成 | 1.5 | 高风险 |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | 监控、专人值守等物理安全防护措施。 | 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 | 立，略过第 39-40 项）<br>39.物理安全防护措施不能满足企业安全需求，扣 0.5 分；<br>40.未提供物理安全防护措施落实的记录，扣 0.5 分。 | | 项 |
| | （二）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）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 | 41.未拆除或封闭工业主机上不必要的 USB、光驱、无线等接口，扣 1 分；<br>42.有未授权的外设终端或设备接入记录，扣 1.5 分。 | 2.5 | 高风险项 |
| | | b）在确需使用工业主机外设接口时，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，以避免未授权的外设终端接入 | （企业确需使用工业主机外设接口时，需要评估第 43-44 项）<br>43.未建立企业工业主机外设接口管理制度，扣 1 分；<br>44.企业工业主机外设安全管理技术手段未落实，扣 0.5 分。 | 1.5 | |
| 五、身份认证（8 项 12 分） | （一）在工业主机登录、应用服务资源访问、工业云平台访问等过程中使用身份认证管理。对 | a）企业应在工业主机登录、应用服务资源访问、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），<br>45.未建立工业主机登录、应用服务资源访问、工业云平台访问等身份认证管理制度，扣 1 分；<br>46.身份认证管理制度未落实，扣 1 分。 | | 2 | 高风险项 |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | 于关键设备、系统和平台的访问采用多因素认证。 | 以确保访问过程安全可控 | | | |
| | | b）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 | 47.没有建立关键设备、系统和平台清单，扣 0.5 分；<br>48.没有采用多因素认证方式，对关键设备、系统和平台进行身份认证，扣 0.5 分。 | 1 | |
| | （二）合理分类设置账户权限，以最小特权原则分配账户权限。 | a）企业应根据不同业务需求、岗位职责等，合理分类设置账户 | 49.没有根据不同业务需求和岗位职责分类设置账户，扣 2 分；（若本项成立，略过第 50 项）<br>50.账户分类设置不合理，扣 1 分。 | 2 | |
| | | b）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 | 51.未执行工业控制系统账户分配规则，扣 1 分；<br>52.工业控制系统未按照最小特权原则进行权限分配，扣 1 分。 | 2 | 高风险项 |
| | | c）企业需定期自行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 | 53.未提供工业控制系统账户权限分配情况的定期审计记录，扣 1 分。 | 1 | |
| | （三）强化工业控制设备、SCADA 软件、工业 | a）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 | 54.企业的工业控制设备、SCADA 软件、工业通信设备等登录账户及密码强度不满足需求，或使用默认口令 | 2 | 高风险项 |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | 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。 | 足够强度的登录密码，并妥善管理，避免使用默认口令和弱口令，以降低对设备未授权登录和操作的可能性； | 和弱口令，扣 1 分。<br>55.企业未妥善管理密码，扣 1 分。 | | |
| | | b）企业应采定期更新口令 | 56.企业的工业控制设备、SCADA 软件、工业通信设备没有定期更新口令，扣 1 分。 | 1 | |
| | （四）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，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 | 57.身份认证证书传输、存储方式不满足安全要求，扣 1 分。 | 1 | |
| 六、远程访问安全<br>（7 项 11 分） | （一）原则上严格禁止工业控制系统面向互联网开通 HTTP、FTP、Telnet 等高风险通用网络服务。 | a）适用时，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 等高风险通用网络服务 | 58.工业控制系统面向互联网开通不必要的 HTTP、FTP、Telnet 等高风险通用网络服务，扣 2 分。 | 2 | 高风险项 |
| | （二）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， | a）企业应采用数据单向访问控制、VPN、堡垒机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 | （如企业确需存在远程访问的情况，需要评估第 59-65 项）<br>59.没有采用数据单向访问控制、VPN、堡垒机等策略 | 2 | 高风险项 |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | 对访问时限进行控制，并采用加标锁定策略。 | 授权操作 | 对远程访问进行安全加固，扣 1 分；<br>60.安全加固措施不能满足企业安全和业务需要，扣 1 分。 | | |
| | | b）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 | 61.未对远程访问控制采用时限控制，扣 0.5 分；<br>62.未采用加标锁定策略等方式控制远程访问的安全，扣 0.5 分。 | 1 | |
| | （三）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，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 | 63.企业远程维护通道未采用 VPN 等远程接入方式，扣 1.5 分。 | 1.5 | |
| | | b）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 | 64.未建立远程接入账户管理制度，扣 1.5 分；（若本项成立，略过第 64 项）<br>65.接入账户的申请、使用、收回等流程不规范，扣 0.5 分。 | 1.5 | 高风险项 |
| | （四）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）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 | 66.工业控制系统访问日志未进行保留或日志内容不完善，扣 1 分；<br>67.未定期备份工业控制系统访问日志，扣 0.5 分。 | 1.5 | |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | | b）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 | 68.未建立日志审计制度，扣 1 分；<br>69.未定期开展日志审计工作，扣 0.5 分。 | 1.5 | |
| 七、安全监测和应急预案演练（7 项 10 分） | （一）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）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 | 70.未在工业控制网络部署通过国家相关部门认证的网络安全监测设备，扣 1.5 分；(若本项成立，略过第 71-72 项)<br>71.已部署网络安全监测设备不具备发现、报告并处理网络攻击或异常行为功能，扣 0.5 分；<br>72.未对网络安全监测设备进行恰当的配置，扣 0.5 分。 | 1.5 | |
| | （二）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）企业应根据自身情况，明确重要工业控制设备清单 | 73.未形成重要工业控制设备清单，扣 0.5 分；<br>74.重要工业控制设备清单不完整、不准确，扣 0.5 分。 | 1 | |
| | | b）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，具备阻断不符合协议标准结构的 | 75.未部署深度包分析和过滤功能防护设备，扣 1.5 分；（若本项成立，略过第 76 项）<br>76.未恰当配置深度包分析和过滤功能防护设备的策略（如是否开启阻断不符合协议标准结构的数据包、 | 1.5 | |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | | 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 | 不符合正常生产业务范围的数据内容等功能），不能满足限制违法操作的安全要求，扣 1 分。 | | |
| | （三）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）企业应专门制定工控安全事件应急响应预案，确保企业正确应对安全事件 | 77.未制定工控安全事件应急响应预案，扣 2 分；（若本项成立，略过第 78 项）<br>78.制定的工控安全事件应急响应预案不科学或不合理，扣 1 分。 | 2 | 高风险项 |
| | | b）适用时，当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 | （若企业工业控制系统未因信息安全威胁出现过异常或故障，则执行 79 条）<br>79.被访谈相关人员不能正确回答应急响应措施，扣 2 分；<br>（若企业工业控制系统因信息安全威胁出现过异常或故障，则执行 80-82 条）<br>80.未采取紧急防护措施防止事态扩大，扣 0.5 分；<br>81.未报送至属地相关工业和信息化主管部门，扣 0.5 分；<br>82.保护现场和调查取证相关流程和要求未执行或缺乏执行记录，扣 0.5 分。 | 2 | |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | （四）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)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，确保紧急事件发生时应急预案被有效执行 | 83.未定期开展应急响应预案演练，扣 1.5 分；(若本项成立，略过第 84 项)<br>84.应急响应预案演练未覆盖应急预案的相关内容，扣 0.5 分。 | 1.5 | |
| | | b)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 | 85.未对应急预案进行评审和修订，扣 0.5 分。（没有应急预案同样扣分） | 0.5 | |
| 八、资产安全（4 项 5.5 分） | （一）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）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 | 86.未建立工业控制系统资产清单，扣 1.5 分；(若本项成立，略过第 87 项)<br>87.工业控制系统资产清单不完整、不准确，扣 0.5 分。 | 1.5 | |
| | | b）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 | 88.未明确资产责任人，扣 1 分；(若本项成立，略过第 89 项)<br>89.资产责任人对其职责不清楚，扣 0.5 分；<br>90.未形成资产使用处置规则，扣 1 分；(若本项成立，略过第 91 项)<br>91.资产使用处置规则未得到有效执行，扣 0.5 分。 | 2 | |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | （二）对关键主机设备、网络设备、控制组件等进行冗余配置。 | a）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 | 92.未制定关键主机设备、网络设备、控制组件清单，扣 1 分。 | 1 | |
| | | b）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（如双机冷/热备等），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 | 93.关键主机设备、网络设备、控制组件未实施冗余配置，扣 1 分。 | 1 | |
| 九、数据安全（9 项 11 分） | （一）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）企业应明确识别重要工业数据清单（如通过 OPC 采集的生产数据、历史站存储的数据等） | 94.未建立重要工业数据清单，扣 1 分；（若本项成立，略过第 95 项）<br>95.重要工业数据清单不完整、不准确，扣 0.5 分。 | 1 | |
| | | b）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 | 96.未对静态存储的重要工业数据进行防护，扣 2 分；（若本项成立，略过第 97 项）<br>97.对静态存储的重要工业数据进行防护的手段不满足安全防护要求，扣 1 分。 | 2 | 高风险项 |
| | | c）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 | 98.未对动态传输的重要工业数据进行防护，扣 1.5 分；（若本项成立，略过第 99 项） | 1.5 | |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | | 护，确保动态传输过程中重要工业数据的安全性 | 99.对动态传输的重要工业数据进行防护的手段不满足安全防护要求，扣 1 分。 | | |
| | | d）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 | 100.未建立工业数据分级分类管理制度，扣 1 分；(若本项成立，略过第 101 项)<br>101.未按照分级分类管理制度对重要工业数据进行管理，扣 0.5 分。 | 1 | |
| | （二）定期备份关键业务数据。 | a）企业应建立关键业务数据清单（如生产工艺、生产计划、组态文件、调度管理等数据） | 102.未建立关键业务数据清单，扣 1 分；(若本项成立，略过第 103 项)<br>103.关键业务数据清单不完整、不准确，扣 0.5 分。 | 1 | |
| | | b）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 | 104.未定期备份关键业务数据，扣 2 分；(若本项成立，略过第 105-106 项)<br>105.关键业务数据的备份方式、备份周期等策略不合理，扣 1 分；<br>106.对关键业务数据的备份方式、备份周期等策略的执行不满足要求，扣 0.5 分。 | 2 | 高风险项 |
| | | c）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 | 107.未定期对所备份的关键业务数据进行恢复测试，扣 0.5 分。 | 0.5 | |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | | 用性 | | | |
| | （三）对测试数据进行保护。 | a）企业应对测试过程中产生的数据进行保护，以确保企业测试数据的安全 | 108.未采取措施保护测试过程中产生的数据，扣 1 分；（若本项成立，略过第 109 项）<br>109.未采取适宜、有效的保护措施，扣 0.5 分。 | 1 | |
| | | b）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 | 110.在测试环境中发现实际生产数据或通过访谈了解到使用实际生产数据进行测试的情况，扣 0.5 分；<br>111.测试数据中包含敏感细节和内容，扣 0.5 分。 | 1 | |
| 十、供应链管理（3 项 4 分） | （一）在选择工业控制系统规划、设计、建设、运维或评估等服务商时，优先考虑具备工控安全防护经验的企事业单位，以合同等方式明确服务商应承担的信息安全责任和义务。 | a）企业应以合同等方式明确工业控制系统产品和服务提供商承担的信息安全责任和义务，确保提供的产品和服务满足信息安全要求 | 112.与工业控制系统服务商签署的合同中未约定服务商在服务过程中应当承担的信息安全责任和义务，扣 2 分；（若本项成立，略过第 113 项）<br>113.企业与工业控制系统服务商签署的合同中约定的服务商在服务过程中应当承担的信息安全责任和义务不完整、不合理，扣 1 分。 | 2 | 高风险项 |
| | | b）企业在选择工业控制系统规划、设计、建设、运维或评估服务商时，应优先考虑具备工控安全防护经验的企 | 114.在服务商选择流程及要求中未明确提出应优先考虑具备工控安全防护经验的企事业单位，扣 0.5 分；<br>115.选择的服务商均不具备工控安全防护经验，扣 | 1 | |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | | 事业单位 | 0.5 分。 | | |
| | （二）以保密协议的方式要求服务商做好保密工作，防范敏感信息外泄。 | a）企业应与服务商签订保密协议，确保敏感信息不外泄 | 116.未与服务商签订保密协议，扣 1 分；(若本项成立，略过第 117 项)<br>117.保密协议中未明确保密内容、保密时限、违约责任等内容，扣 0.5 分。 | 1 | |
| 十一、落实责任（3 项 9 分） | 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）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 | 118.未建立工业控制系统安全管理机制，扣 3 分；(若本项成立，略过第 119-121 项)<br>119.工业控制系统安全管理机制不完备、合理，扣 1 分；<br>120.企业相关人员对工业控制系统安全管理机制缺乏了解，扣 0.5 分；<br>121.无法提供制度执行的证明材料，扣 0.5 分。 | 3 | 高风险项 |
| | | b）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 | 122.未成立信息安全协调小组，扣 3 分；(若本项成立，略过第 123-125 项)<br>123.协调小组的工业控制系统信息安全职责未明确，扣 1 分；<br>124.协调小组成员未包含信息化、生产管理、设备管 | 3 | 高风险项 |

| 项目 | | | 评分细则 | 分值 | 备注 |
| --- | --- | --- | --- | --- | --- |
| | | | 理等相关部门，扣 0.5 分；<br>125.协调小组成员对其职责不清楚，扣 0.5 分。 | | |
| | | c）企业应在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 | 126.未明确工控安全管理责任人，扣 3 分；(若本项成立，略过第 127-129 项)<br>127.工控安全管理责任人的职责不明确，扣 1 分；<br>128.工控安全管理责任人未有效落实工控安全责任制，扣 0.5 分；<br>129.工控安全管理责任人未及时部署工控安全防护措施，扣 0.5 分。 | 3 | 高风险项 |
| 合计 | 30 项 | 61 项 | 129 项 | 100 | 25 项 |

# 附录 B 防护评估工具

## B.1 防护评估工具的安全要求

评估机构应使用来源可靠、安全稳定的评估工具，并要求相关人员严格遵守操作流程，防止引入新的风险。防护评估工具应确保来源安全可靠，并经国家相关质检机构严格测试和校验，确保不对企业工控系统运行造成影响。未通过检测和校验的评估工具不得应用于评估工作。

## B.2 防护评估工具的使用要求

评估机构应确保评估人员可熟练使用相关工业控制系统信息安全防护评估工具，并在现场评估过程中安全、规范、合理的使用评估工具。

使用防护评估工具对工业控制系统进行测试时应慎重实施，尽量避免在企业的业务高峰期进行技术测试。

## B.3 常用防护评估工具

常用防护评估工具包括：工业控制系统信息安全防护指南评估工具、工业控制系统脆弱性扫描工具、工业控制系统主机安全检查工具、工业控制系统配置核查工具等。