ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37934—2019

信息安全技术　工业控制网络安全隔离与信息交换系统安全技术要求

Information security technology—Security technical requirements of industrial control system security isolation and information ferry system

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。

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这些专利的责任。

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:公安部第三研究所、公安部网络安全保卫局、北京神州绿盟信息安全科技股份有限公司、珠海市鸿瑞软件技术有限公司、中国电子科技网络信息安全有限公司、中国信息安全研究院有限公司、北京天融信网络安全技术有限公司、济南华汉电气科技有限公司、北京匡恩网络科技有限责任公司、北京力控华康科技有限公司、中国电子技术标准化研究院。

本标准主要起草人:邹春明、陆臻、田原、沈清泓、范春玲、陆磊、俞优、刘瑞、顾健、刘智勇、陈敏超、兰昆、杨晨、张大江、龚亮华、雷晓锋、叶晓虎、王晓鹏、周文奇、范科峰、姚相振、李琳、周睿康。

引　言

随着工业化与信息化的深度融合，来自信息网络的安全威胁正逐步对工业控制系统造成极大的安全威胁，通用网络安全隔离与信息交换系统在面对工业控制系统的安全防护时显得力不从心，因此需要一种能应用于工业控制环境的网络安全隔离与信息交换系统对工业控制系统进行安全防护。

应用于工业控制环境的网络安全隔离与信息交换系统与通用网络安全隔离与信息交换系统的主要差异体现在：

——通用网络安全隔离与信息交换系统除了需具备基本的五元组过滤外，还需要具备一定的应用层过滤防护能力。用于工业控制环境的网络安全隔离与信息交换系统除了具有通用网络安全隔离与信息交换系统的部分通用协议应用层过滤能力外，还需要具有对工业控制协议应用层的过滤能力。

——结合工业控制环境中当前的信息安全防护技术水平，以及信息安全防护不得影响系统功能的正常运行，通用网络安全隔离与信息交换系统所要求的强制访问控制要求还不能够适应于工业控制环境。

——工业控制环境下的网络安全隔离与信息交换系统比通用网络安全隔离与信息交换系统具有更高的可用性、可靠性、稳定性等要求。

信息安全技术　工业控制网络安全
隔离与信息交换系统安全技术要求

1　范围

本标准规定了工业控制网络安全隔离与信息交换系统的安全功能要求、自身安全要求和安全保障要求。

本标准适用于工业控制网络安全隔离与信息交换系统的设计、开发及测试。

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 20279—2015　信息安全技术　网络和终端隔离产品安全技术要求

GB/T 20438.3—2017　电气/电子/可编程电子安全相关系统的功能安全　第3部分：软件要求

GB/T 20438.4—2017　电气/电子/可编程电子安全相关系统的功能安全　第4部分：定义和缩略语

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 20279—2015、GB/T 20438.4—2017 和 GB/T 25069—2010 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；ICS

工业控制系统(ICS)是一个通用术语，它包括多种工业生产中使用的控制系统，包括监控和数据采集系统(SCADA)、分布式控制系统(DCS)和其他较小的控制系统，如可编程逻辑控制器(PLC)，现已广泛应用在工业部门和关键基础设施中。

[GB/T 32919—2016，定义 3.1]

3.2

工业控制协议　industrial control protocol

工业控制系统中，上位机与控制设备之间，以及控制设备与控制设备之间的通信报文规约。

注：通常包括模拟量和数字量的读写控制。

3.3

工业控制网络安全隔离与信息交换系统　industrial control system security isolation and information ferry system

部署于工业控制网络中不同的安全域之间，采用协议隔离技术实现两个安全域之间访问控制、协议转换、内容过滤和信息交换等功能的产品。

4 缩略语

下列缩略语适用于本文件。

MAC:媒体接入控制(Media Access Control)

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

5 产品描述

工业控制网络安全隔离与信息交换系统通常部署在工业控制网络边界,保护的资产为工业控制网络;或者部署在生产管理层与过程监控层之间,保护的资产为过程监控层网络及现场控制层网络。此外,工业控制网络安全隔离与信息交换系统本身及其内部的重要数据也是受保护的资产。

工业控制网络安全隔离与信息交换系统一般以二主机加专用隔离部件的方式组成,即由内部处理单元、外部处理单元和专用隔离部件组成。其中,专用隔离部件既可以是采用包含电子开关并固化信息摆渡控制逻辑的专用隔离芯片构成的隔离交换板卡,也可以是经过安全强化的运行专用信息传输逻辑控制程序的主机。工业控制网络安全隔离与信息交换系统中的内、外部处理单元通过专用隔离部件相连,专用隔离部件是两个安全域之间唯一的可信物理信道。该内部信道裁剪了 TCP/IP 等公共网络协议栈,采用私有协议实现公共协议隔离。专用隔离部件通常有两种实现方式:一是采用私有协议以逻辑方式实现协议隔离和信息传输;二是采用一组互斥的分时切换电子开关实现内部物理信道的通断控制,以分时切换连接方式完成信息摆渡,从而在两个安全域之间形成一个不存在实时物理连接的隔离区。

本标准将工业控制网络安全隔离与信息交换系统安全技术要求分为安全功能、自身安全要求和安全保障要求三个大类。安全功能要求、自身安全要求和安全保障要求分为基本级和增强级,与基本级内容相比,增强级中要求有所增加或变更的内容在正文中通过“**黑体**”表示。

6 安全技术要求

6.1 基本级安全技术要求

6.1.1 安全功能要求

6.1.1.1 访问控制

6.1.1.1.1 基于白名单的访问控制

产品应采用白名单的访问控制策略,即非访问控制策略明确允许的访问,需默认禁止。

6.1.1.1.2 网络层访问控制

产品应支持基于源 IP、源端口、目的 IP、目的端口、传输层协议等要求进行访问控制。

6.1.1.1.3 应用层访问控制

产品应支持应用层的访问控制:

a) 支持 HTTP、FTP、TELNET 等应用的识别与访问控制;

b) 至少支持一种工业控制协议的访问控制。

6.1.1.1.4 工业控制协议深度检查

产品应支持对工业控制协议内容进行深度分析和访问控制：

a) 对所支持的工业控制协议进行协议规约检查，明确拒绝不符合协议规约的访问；

b) 应支持对工业控制协议的操作类型、操作对象、操作范围等参数进行访问控制；

c) 若支持 OPC 协议：应支持基于控制点名称、读写操作等要素进行控制；

d) 若支持 ModbusTCP 协议：应支持基于设备 ID、功能码类型、读写操作、寄存器地址、控制值范围等要素进行控制。

6.1.1.2 协议隔离

所有主客体之间发送和接收的信息流均执行网络层协议剥离，还原成应用层数据，在两机之间以非 TCP/IP 的私有协议格式传输。

6.1.1.3 残余信息保护

在为所有内部或外部网络上的主机连接进行资源分配时，安全功能应保证其分配的资源中不提供以前连接活动中所产生的任何信息内容。

6.1.1.4 不可旁路

在与安全有关的操作（例如安全属性的修改、内部网络主机向外部网络主机传送信息等）被允许执行之前，安全功能应确保其通过安全功能策略的检查。

6.1.1.5 抗攻击

产品应具备抵御 SYN Flood 攻击、UDP Flood 攻击、ICMP Flood 攻击、Pingofdeath 攻击等典型拒绝服务攻击能力。

6.1.2 自身安全要求

6.1.2.1 标识和鉴别

6.1.2.1.1 唯一性标识

产品应保证任何用户都具有唯一的标识。

6.1.2.1.2 管理员属性定义

产品应为每个管理员规定与之相关的安全属性，如管理员标识、鉴别信息、隶属组、权限等，并提供使用默认值对创建的每个管理员的属性进行初始化的功能。

6.1.2.1.3 基本鉴别

产品应保证任何用户在执行安全功能前都要进行身份鉴别。

6.1.2.1.4 鉴别失败处理

产品应为管理员登录设定一个授权管理员可修改的鉴别尝试阈值，当管理员的不成功登录尝试超过阈值，系统应通过技术手段阻止管理员的进一步鉴别请求。

6.1.2.2 安全管理

6.1.2.2.1 接口及管理安全

产品应保证业务接口、管理接口、管理界面的安全：

a) 业务接口和管理接口采用不同的网络接口；

b) 管理接口及管理界面不存在中高风险安全漏洞。

6.1.2.2.2 安全状态监测

产品应能够监测产品自身及组件状态，包括对产品 CPU、内存、存储空间等系统资源使用状态进行监测。

6.1.2.3 数据完整性

安全功能应保护储存于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏。

6.1.2.4 时间同步

产品应支持与外部时间服务器进行时间同步。

6.1.2.5 高可用性

6.1.2.5.1 容错

产品应具备一定的容错能力：

a) 重要程序及文件被破坏时，设备重启后能够自恢复；

b) 重要进程异常终止时，能够自启动。

6.1.2.5.2 安全策略更新

进行访问控制安全策略应用时不应该影响正常的数据通信。

6.1.2.6 审计日志

6.1.2.6.1 业务日志生成

产品应对其提供的业务功能生成审计日志：

a) 访问控制策略匹配的访问请求，包括允许及禁止的访问请求；

b) 识别及防护的各类攻击行为。

6.1.2.6.2 业务日志内容

业务日志内容至少包括：

a) 日期、时间、源目的 MAC、源目的 IP、源目的端口、协议类型；

b) 工业控制协议的操作类型、操作对象、操作值等相关参数；

c) 攻击事件的类型及描述。

6.1.2.6.3 系统日志生成

产品应对与自身安全相关的以下事件生成审计日志：

a) 身份鉴别，包括成功和失败；
b) 因鉴别失败次数超过阈值而采取的禁止进一步尝试的措施；
c) 访问控制策略的增加、删除、修改；

6.1.2.6.4 系统日志内容

系统日志内容至少应包括日期、时间、事件主体、事件客体、事件描述等。

6.1.2.6.5 审计日志管理

应支持日志管理功能，具体技术要求如下：
a) 应只允许授权管理员能够对审计日志进行读取、存档、导出、删除和清空等操作；
b) 应提供能查阅日志的工具；
c) 审计事件应存储于掉电非易失性存储介质中，且在存储空间达到阈值时至少能够通知授权审计员。

6.1.3 安全保障要求

6.1.3.1 开发

6.1.3.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，技术要求如下：
a) 与产品设计文档中对安全功能的描述一致；
b) 描述与安全功能要求一致的安全域；
c) 描述产品安全功能初始化过程及安全措施；
d) 证实产品安全功能能够防止被破坏；
e) 证实产品安全功能能够防止安全策略被旁路。

6.1.3.1.2 功能规范

开发者应提供完备的功能规范说明，技术要求如下：
a) 完整描述产品的安全功能；
b) 描述所有安全功能接口的目的与使用方法；
c) 标识和描述每个安全功能接口相关的所有参数；
d) 描述安全功能接口相关的安全功能实施行为；
e) 描述由安全功能实施行为而引起的直接错误消息；
f) 证实安全功能要求到安全功能接口的追溯。

6.1.3.1.3 产品设计

开发者应提供产品设计文档，技术要求如下：
a) 根据子系统描述产品结构，并标识和描述产品安全功能的所有子系统；
b) 描述安全功能所有子系统间的相互作用；
c) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口。

6.1.3.2 指导性文档

6.1.3.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述要求如下：

a) 描述授权用户可访问的功能和特权，包含适当的警示信息；
b) 描述如何以安全的方式使用产品提供的接口；
c) 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e) 标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
f) 实现安全目的所应执行的安全策略。

6.1.3.2.2 准备程序

开发者应提供产品及其准备程序，技术要求如下：

a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b) 描述安全安装产品及其运行环境必需的所有步骤。

6.1.3.3 生命周期支持

6.1.3.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识；
b) 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识各配置项；
c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法。

6.1.3.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表至少包括产品、安全保障要求的评估证据和产品的组成部分。

6.1.3.3.3 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

6.1.3.3.4 支撑系统安全保障

开发者应明确产品支撑系统的安全保障措施，技术要求如下：

a) 若产品以软件形态提交，应在交付文档中详细描述支撑操作系统的兼容性、可靠性、安全性要求；
b) 若产品以硬件形态提交，应选取和采用安全可靠的支撑操作系统，以最小化原则选取必要的系统组件，并采取一定的加固措施。

6.1.3.3.5 硬件安全保障

若产品以硬件形态提交，开发者应采取措施保障硬件安全，技术要求如下：

a) 产品应采用具有高可靠性的硬件平台；

b) 若硬件平台为外购，应制定相应程序对硬件提供商进行管理、对采购的硬件平台或部件进行验证测试，并要求硬件提供商提供合格证明及必要的第三方环境适用性测试报告。

6.1.3.4 测试

6.1.3.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性。

6.1.3.4.2 功能测试

开发者应测试产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；

b) 预期的测试结果，表明测试成功后的预期输出；

c) 实际测试结果和预期的测试结果一致。

6.1.3.4.3 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

6.1.3.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗基本的攻击。

6.2 增强级安全技术要求

6.2.1 安全功能要求

6.2.1.1 访问控制

6.2.1.1.1 基于白名单的访问控制

产品应采用白名单的访问控制策略，即非访问控制策略明确允许的访问，需默认禁止。

6.2.1.1.2 网络层访问控制

产品应支持基于源 IP、源端口、目的 IP、目的端口、传输层协议等要求进行访问控制。

6.2.1.1.3 IP/MAC 地址绑定

产品应支持自动或管理员手工绑定与其进行通信的设备的 IP/MAC 地址，当通信的 IP、MAC 地址与绑定列表不符时，应阻止通信。

6.2.1.1.4 应用层访问控制

产品应支持应用层的访问控制：

a) 支持 HTTP、FTP、TELNET 等应用的识别与访问控制；
b) 至少支持两种工业控制协议的访问控制。

6.2.1.1.5 工业控制协议深度检查

产品应支持对工业控制协议内容进行深度分析和访问控制：
a) 对所支持的工业控制协议进行协议规约检查，明确拒绝不符合协议规约的访问；
b) 应支持对工业控制协议的操作类型、操作对象、操作范围等参数进行访问控制；
c) 若支持 OPC 协议：应支持基于控制点名称、读写操作等要素进行控制；
d) 若支持 ModbusTCP 协议：应支持基于设备 ID、功能码类型、读写操作、寄存器地址、控制值范围等要素进行控制。

6.2.1.2 协议隔离

所有主客体之间发送和接收的信息流均执行网络层协议剥离，还原成应用层数据，在两机之间以非 TCP/IP 的私有协议格式传输。

6.2.1.3 信息摆渡

设备双机之间应采用专用隔离部件，并确保数据传输链路物理上的时分切换，即设备的双机在物理链路上不能同时与专用隔离部件连通，并完成信息摆渡。

6.2.1.4 残余信息保护

在为所有内部或外部网络上的主机连接进行资源分配时，安全功能应保证其分配的资源中不提供以前连接活动中所产生的任何信息内容。

6.2.1.5 不可旁路

在与安全有关的操作（例如安全属性的修改、内部网络主机向外部网络主机传送信息等）被允许执行之前，安全功能应确保其通过安全功能策略的检查。

6.2.1.6 抗攻击

产品应具备一定的抗拒绝服务攻击能力：
a) SYN Flood 攻击、UDP Flood 攻击、ICMP Flood 攻击、Pingofdeath 攻击等；
b) **TearDrop 攻击、Land 攻击等。**

6.2.1.7 双机热备

产品应具备双机热备的能力，当主设备出现故障时或者主设备链路故障时，备用设备应能及时接管进行工作。

6.2.2 自身安全要求

6.2.2.1 标识和鉴别

6.2.2.1.1 唯一性标识

产品应保证任何用户都具有唯一的标识。

6.2.2.1.2 管理员属性定义

产品应为每个管理员规定与之相关的安全属性，如管理员标识、鉴别信息、隶属组、权限等，并提供使用默认值对创建的每个管理员的属性进行初始化的功能。

6.2.2.1.3 管理员角色

产品应为管理角色进行分级，使不同级别的管理角色具有不同的管理权限。各管理角色的权限应形成互相制约关系。

6.2.2.1.4 基本鉴别

产品应保证任何用户在执行安全功能前都要进行身份鉴别。若其采用网络远程方式管理，还应对可管理的地址进行限制。

6.2.2.1.5 多鉴别

产品应能向管理角色提供除口令身份鉴别机制以外的其他身份鉴别机制（如证书、智能IC卡、指纹等鉴别机制）。

6.2.2.1.6 超时锁定或注销

当已通过身份鉴别的管理角色空闲操作的时间超过规定值，在该管理角色需要执行管理功能前，产品应对该管理角色的身份重新进行鉴别。

6.2.2.1.7 鉴别失败处理

产品应为管理员登录设定一个授权管理员可修改的鉴别尝试阈值，当管理员的不成功登录尝试超过阈值，系统应通过技术手段阻止管理员的进一步鉴别请求。

6.2.2.2 安全管理

6.2.2.2.1 接口及管理安全

产品应保证业务接口、管理接口、管理界面的安全：

a) 应支持业务接口和管理接口采用不同的网络接口；

b) 管理接口及管理界面不存在中高风险安全漏洞。

6.2.2.2.2 管理信息传输安全

产品需要通过网络进行管理时，产品应能对管理信息进行保密传输。

6.2.2.2.3 安全状态监测

产品应能够监测产品自身及组件状态，包括：

a) 对产品CPU、内存、存储空间等系统资源使用状态进行监测；

b) 对产品的主要功能模块运行状态进行监测。

6.2.2.3 数据完整性

安全功能应保护储存于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏。

6.2.2.4 时间同步

产品应支持与外部时间服务器进行时间同步。

6.2.2.5 高可用性

6.2.2.5.1 容错

产品应具备一定的容错能力：

a) 重要程序及文件被破坏时，设备重启后能够自恢复；

b) 重要进程异常终止时，能够自启动。

6.2.2.5.2 安全策略更新

进行访问控制安全策略下装及应用时不应影响正常的数据通信。

6.2.2.6 审计日志

6.2.2.6.1 业务日志生成

产品应对其提供的业务功能生成审计日志：

a) 访问控制策略匹配的访问请求，包括允许及禁止的访问请求；

b) 识别及防护的各类攻击行为。

6.2.2.6.2 业务日志内容

业务日志内容至少包括：

a) 日期、时间、源目的 MAC、源目的 IP、源目的端口、协议类型；

b) 工业控制协议的操作类型、操作对象、操作值等相关参数；

c) 攻击事件的类型及描述。

6.2.2.6.3 系统日志生成

产品应对与自身安全相关的以下事件生成审计日志：

a) 身份鉴别，包括成功和失败；

b) 因鉴别失败次数超过阈值而采取的禁止进一步尝试的措施；

c) 访问控制策略的增加、删除、修改；

d) **管理员的增加、删除、修改；**

e) **时间同步；**

f) **超过保存时限的审计记录和自身审计日志的自动删除；**

g) **审计日志和审计记录的备份与恢复；**

h) **存储空间达到阈值报警；**

i) **其他事件。**

6.2.2.6.4 系统日志内容

系统日志内容至少应包括日期、时间、事件主体、事件客体、事件描述等。

6.2.2.6.5 审计日志管理

应支持日志管理功能，具体技术要求如下：

a) 应只允许授权管理员能够对审计日志进行读取、存档、导出、删除和清空等操作；

b) 应提供能查阅日志的工具，**支持多条件对审计日志进行组合查询**；

c) 审计事件应存储于掉电非易失性存储介质中，且在存储空间达到阈值时至少能够通知授权审计员；

d) **应支持以标准格式将审计日志外发到专用的日志服务器**。

6.2.3 安全保障要求

6.2.3.1 开发

6.2.3.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，技术要求如下：

a) 与产品设计文档中对安全功能的描述一致；

b) 描述与安全功能要求一致的安全域；

c) 描述产品安全功能初始化过程及安全措施；

d) 证实产品安全功能能够防止被破坏；

e) 证实产品安全功能能够防止安全策略被旁路。

6.2.3.1.2 功能规范

开发者应提供完备的功能规范说明，技术要求如下：

a) 完整描述产品的安全功能；

b) 描述所有安全功能接口的目的与使用方法；

c) 标识和描述每个安全功能接口相关的所有参数；

d) 描述安全功能接口相关的安全功能实施行为；

e) 描述由安全功能实施行为而引起的直接错误消息；

f) 证实安全功能要求到安全功能接口的追溯；

g) **描述安全功能实施过程中，与安全功能接口相关的所有行为**；

h) **描述可能由安全功能接口的调用而引起的所有错误消息**。

6.2.3.1.3 实现表示

开发者应提供全部安全功能的实现表示，技术要求如下：

a) **提供产品设计描述与实现表示实例之间的映射，并证明其一致性**；

b) **详细定义产品安全功能，达到无须进一步设计就能生成安全功能的程度**；

c) **实现表示以开发人员使用的形式提供**。

6.2.3.1.4 产品设计

开发者应提供产品设计文档，技术要求如下：

a) 根据子系统描述产品结构，并标识和描述产品安全功能的所有子系统；

b) 描述安全功能所有子系统间的相互作用；

c) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；

d) 根据模块描述安全功能，并提供安全功能子系统到模块间的映射关系；
e) 描述所有安全功能实现模块，包括其目的及与其他模块间的相互关系；
f) 描述所有模块的安全功能要求相关接口、与其他相邻接口的调用参数及返回值；
g) 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

6.2.3.2 指导性文档

6.2.3.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述要求如下：

a) 描述授权用户可访问的功能和特权，包含适当的警示信息；
b) 描述如何以安全的方式使用产品提供的接口；
c) 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e) 标识产品运行的所有可能状态(包括操作导致的失败或者操作性错误)，以及它们与维持安全运行之间的因果关系和联系；
f) 实现安全目的所应执行的安全策略。

6.2.3.2.2 准备程序

开发者应提供产品及其准备程序，技术要求如下：

a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b) 描述安全安装产品及其运行环境必需的所有步骤。

6.2.3.3 生命周期支持

6.2.3.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识；
b) 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识各配置项；
c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
d) 配置管理系统提供一种自动方式来支持产品的生成，并确保只能对配置项进行已授权的变更；
e) 配置管理文档包括配置管理计划，计划中需描述如何使用配置管理系统，并依据该计划实施配置管理；
f) 配置管理计划应描述配置项的变更(包括新建、修改、删除)控制程序。

6.2.3.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者，技术要求如下：

a) 产品、安全保障要求的评估证据和产品的组成部分；
b) 实现表示、安全缺陷报告及其解决状态。

6.2.3.3.3 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的各版本时，

交付文档应描述为维护安全所必需的所有程序。

6.2.3.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

6.2.3.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

6.2.3.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义的定义实现中所有语句的含义和所有依赖选项的含义。

6.2.3.3.7 支撑系统安全保障

开发者应明确产品支撑系统的安全保障措施，技术要求如下：

a) 若产品以软件形态提交，应在交付文档中详细描述支撑操作系统的兼容性、可靠性、安全性要求；

b) 若产品以硬件形态提交，应选取和采用安全可靠的支撑操作系统，以最小化原则选取必要的系统组件，并采取一定的加固措施。

6.2.3.3.8 硬件安全保障

若产品以硬件形态提交，开发者应采取措施保障硬件安全，技术要求如下：

a) 产品应采用具有高可靠性的硬件平台；

b) 若硬件平台为外购，应制定相应程序对硬件提供商进行管理、对采购的硬件平台或部件进行验证测试，并要求硬件提供商提供合格证明及必要的第三方环境适用性测试报告。

6.2.3.4 测试

6.2.3.4.1 测试覆盖

开发者应提供测试覆盖文档，技术要求如下：

a) 证实测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；

b) 证实功能规范中的所有安全功能接口都进行了测试。

6.2.3.4.2 测试深度

开发者应提供测试深度的分析，技术要求如下：

a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；

b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

6.2.3.4.3 功能测试

开发者应测试产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果

的任何顺序依赖性；

b） 预期的测试结果，表明测试成功后的预期输出；

c） 实际测试结果和预期的测试结果一致。

6.2.3.4.4 功能安全测试

开发者应按照 GB/T 20438.3—2017 中 7.9 的要求进行产品软件功能安全测试。

6.2.3.4.5 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

6.2.3.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗较强的攻击。