ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37954—2019

信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法

Information security technology—Technique requirements and testing and evaluation approaches for industrial control system vulnerability detection products

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:中国信息安全测评中心、中国电子技术标准化研究院、北京工业大学、北京匡恩网络科技有限责任公司、中国科学院沈阳自动化研究所、北京和利时系统工程有限公司、公安部第三研究所(国家网络与信息系统安全产品质量监督检验中心)、北京交通大学、解放军战略支援部队信息工程大学、中车株洲电力机车有限公司。

本标准主要起草人:张大江、胡仁豪、范科峰、周睿康、赖英旭、谢丰、邸丽清、叶润国、尚文利、赵剑明、陆臻、邹春明、谢安明、郑伟、魏强、安高峰、王春霞、梁猛、汪义舟、王弢、张胜、刘勇。

信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法

1 范围

本标准规定了针对工业控制系统的漏洞检测产品的技术要求，包括安全功能要求、自身安全要求和安全保障要求，以及相应的测试评价方法。

本标准适用于工业控制系统漏洞检测产品的设计、开发和测评。

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

3 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

漏洞 vulnerability

资产中能被威胁所利用的弱点。

3.2

测试用例 test case

为某个特定目标而编制的一组输入、执行条件以及预期结果，以核实是否满足某个特定需求。

3.3

测试集合 test set

测试用例的组合。

3.4

工业控制组态软件 industrial control configuration software

在控制系统监控层的软件平台和开发环境，使用灵活的方式为用户提供快速配置现场系统状态的软件工具。

4 缩略语

下列缩略语适用于本文件。

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

HTML：超文本标记语言(Hypertext Markup Language)

HTTP：超文本传输协议(HyperText Transfer Protocol)

FTP:文件传输协议(File Transfer Protocol)
IP:互联网协议(Internet Protocol)
OLE:对象连接与嵌入(Object Linking and Embedding)
OPC:用于过程控制的 OLE(OLE for Process Control)
RTU:远程控制终端(Remote Terminal Unit)
SNMP:简单网络管理协议(Simple Network Management Protocol)
TCP:传输控制协议(Transmission Control Protocol)
UDP:用户数据报协议(User Datagram Protocol)

5 产品描述

工业控制系统漏洞检测的目的是检查和分析系统的安全脆弱性,发现可能被入侵者利用的漏洞,并提出防范和补救措施。工业控制系统漏洞检测产品可以用于离线环境、工业控制系统试运行期间或工业系统维修期间,能够对工业控制系统中的工业控制设备、通信设备、安全保护设备以及工业控制软件等进行自动检测,发现存在的漏洞。为防止影响正常生产,不应在工业生产现场使用工业控制系统漏洞检测产品。

工业控制系统漏洞检测产品分为基本级和增强级。工业控制系统漏洞检测产品安全技术要求的分级及其要求条款见附录 A。工业控制系统漏洞检测产品测评方法的分级及其测评项见附录 B。

6 安全技术要求

6.1 安全功能要求

6.1.1 工业控制设备识别

漏洞检测产品应能自动识别工业控制设备。
漏洞检测产品应支持手动添加工业控制设备。

6.1.2 工业控制设备端口扫描

漏洞检测产品应能扫描所有 TCP 端口,检查其是否开启。
漏洞检测产品应能扫描所有 UDP 端口,检查其是否开启。
对于已开启的 TCP、UDP 端口,漏洞检测产品应能判断出与之对应的公开的工业控制通信协议。

6.1.3 工业控制设备通信协议漏洞检测

漏洞检测产品应能检测使用(包括但不限于)以下通信协议的工业控制设备的已知漏洞:

a) 工业以太网协议:Modbus/TCP 协议、OPC 协议、DNP3.0 协议、IEC-60870-5-104 协议、IEC-61850 MMS 协议、Siemens S7Comm 协议、PROFINET 协议、IEC-61850 GOOSE 协议、IEC-61850 SV 协议、EtherNet/IP 协议;
b) 互联网协议:HTTP 协议、FTP 协议、TELNET 协议、SNMP 协议;
c) 串口协议:Modbus RTU 协议、IEC-60870-5-101 协议;
d) 私有协议(包括行业专业协议)。

6.1.4 工业控制组态软件漏洞检测

漏洞检测产品应能检测工业控制组态软件的已知漏洞。

6.1.5 工业控制设备操作系统检测

漏洞检测产品应能检测工业控制设备操作系统的安全问题，检测项目应包括但不限于以下内容：

a) 操作系统类型和版本号识别；
b) 操作系统登录弱口令检测；
c) 操作系统已知安全漏洞检测。

6.1.6 工业控制数据库漏洞检测

漏洞检测产品应能检测工业控制数据库的已知漏洞。

6.1.7 工业控制网络通信设备漏洞检测

漏洞检测产品应能检测工业控制网络通信设备（例如，工业交换机等）的已知漏洞。

6.1.8 检测结果处理要求

漏洞检测产品应能满足以下要求：

a) 漏洞检测产品应能实时查看检测进度。
b) 漏洞检测产品应能实时查看测试用例的执行方法和每一方法的结果。
c) 漏洞检测产品应能监测工业控制设备的实时响应。
d) 检测任务应能随时暂停或者终止。
e) 漏洞检测产品应能保存检测结果。
f) 漏洞检测产品应能记录并追溯导致工业控制设备异常的数据报文。
g) 漏洞检测产品应能根据检测结果自动生成检测报告。检测报告应包括但不限于以下内容：
   1) 工业控制设备的信息列表，包括设备类型、固件版本、操作系统版本等；
   2) 漏洞的名称、漏洞编号、发布日期等；
   3) 潜在的漏洞；
   4) 被测设备的危险等级评估，明确标出扫描出的漏洞的危险等级。
h) 检测报告应以通用文档格式（例如，WPS、DOC、TXT、RTF、PDF、HTML 等）输出。
i) 测试过程异常终止时，漏洞检测产品应能生成已检测部分的报告，并说明测试过程异常终止。

注：被测设备的危险等级取决于扫描脆弱点的最高危险等级。危险等级的定义参见 GB/T 30279—2013 中 4.2。

6.1.9 管理控制功能要求

漏洞检测产品应能满足以下要求：

a) 漏洞检测产品应能针对不同的工业控制设备和系统设置相应的检测参数（例如，扫描地址范围、端口范围、漏洞类型、测试报文、测试次数、测试时间间隔等）。
b) 漏洞检测产品应支持以下测试方式：
   1) 依据工业控制通信协议将测试用例进行归类；
   2) 支持测试用例随机组合；
   3) 支持测试集合随机组合；
   4) 支持用户编写测试用例；
   5) 根据设备类型向用户推荐某类或某几类测试用例。
c) 漏洞检测产品应内置工业控制设备信息库并允许更新。
d) 漏洞检测产品应内置漏洞库。
e) 漏洞检测产品应能通过产品升级等方式更新漏洞库，添加新发现的安全漏洞。

f) 漏洞检测产品应内置测试用例库，包含测试用例和测试集合，用于检测已知漏洞和发现未知漏洞。

6.2 自身安全要求

6.2.1 用户管理与鉴别

漏洞检测产品应能满足以下要求：

a) 漏洞检测产品应支持用户管理，包括添加、删除、激活、禁止用户；
b) 漏洞检测产品应为每个用户设定标识、权限等安全属性；
c) 漏洞检测产品应在用户登录时进行鉴别；
d) 当用户鉴别尝试失败连续达到指定次数后，漏洞检测产品应阻止用户进一步的鉴别请求；
e) 漏洞检测产品应具有登录超时锁定或注销功能；
f) 若漏洞检测产品的控制台提供远程管理功能，应能对可远程管理的主机地址进行身份鉴别和访问控制，并保证传输数据的保密性和完整性。

6.2.2 产品升级

漏洞检测产品应能满足以下要求：

a) 漏洞检测产品应具有升级的功能(包括修复自身缺陷等)；
b) 漏洞检测产品应具有升级包校验机制，防止得到错误的或伪造的升级包。

6.2.3 日志管理

漏洞检测产品应能满足以下要求：

a) 漏洞检测产品应对相关安全事件生成安全日志，包括但不限于以下内容：
   1) 登录成功和退出、登录失败；
   2) 重启；
   3) 鉴别连续尝试不成功的次数超出了设定的限值；
   4) 增加、删除管理员角色和对管理员角色的属性进行修改的操作；
   5) 对上述审计事件的备份和删除；
   6) 升级；
   7) 检测操作。
b) 每一条安全日志应包括事件发生的日期、时间、用户标识、事件类型、事件描述和结果。若采用远程登录方式对漏洞检测产品进行管理还应记录管理主机的地址。
c) 漏洞检测产品应提供下列安全日志管理功能：
   1) 只允许授权管理员访问安全日志；
   2) 提供对安全日志的查询功能；
   3) 授权管理员应能保存或删除安全日志；
   4) 安全日志应能够以通用格式(例如，Excel)导出。

6.2.4 安全存储

漏洞检测产品应能满足以下要求：

a) 漏洞检测产品应只允许用户读取自己创建的测试任务数据；
b) 用户删除测试任务时，漏洞检测产品应删除与测试任务相关的数据；
c) 漏洞检测产品应允许用户导出或导入测试任务数据。

6.3 安全保障要求

6.3.1 配置管理

6.3.1.1 版本号

开发者应为产品的不同版本提供唯一的标识。

6.3.1.2 配置项

开发者应提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识产品的所有配置项并对配置项进行描述。

6.3.2 交付与运行

6.3.2.1 交付程序

开发者交付产品时应将交付过程文档化。

6.3.2.2 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

6.3.3 开发

6.3.3.1 功能规范

开发者应提供一个功能规范，功能规范应满足以下要求：

a) 描述产品安全功能及其外部接口；
b) 是内在一致的；
c) 描述所有外部接口的用途与使用方法；
d) 效果、例外情况和错误消息的细节；
e) 完备地表示产品安全功能。

6.3.3.2 高层设计

开发者应提供产品安全功能的高层设计，高层设计应满足以下要求：

a) 是内在一致的；
b) 按子系统描述安全功能的结构；
c) 描述每个安全功能子系统所提供的安全功能性；
d) 标识安全功能所要求的任何基础性的硬件、固件或软件；
e) 标识安全功能子系统的所有接口；
f) 标识安全功能子系统的哪些接口是外部可见的。

6.3.4 指导性文档

6.3.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a) 管理员可使用的管理功能和接口；

b） 安全地管理产品；
c） 在安全处理环境中应被控制的功能和权限；
d） 对与产品的安全操作有关的用户行为的假设；
e） 受管理员控制的安全参数；
f） 与管理功能有关的安全相关事件；
g） 与管理员有关的 IT 环境安全要求。

6.3.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。
用户指南应说明以下内容：
a） 产品的非管理员用户可使用的安全功能和接口；
b） 产品提供给用户的安全功能和接口的使用方法；
c） 用户可获取但应受安全处理环境所控制的所有功能和权限；
d） 产品安全操作中用户所应承担的职责；
e） 与用户有关的 IT 环境的所有安全要求。

6.3.5 测试

6.3.5.1 测试覆盖

开发者应提供测试覆盖的证据。
在测试覆盖证据中，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是对应的。

6.3.5.2 功能测试

开发者应测试安全功能，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，应标识要测试的安全功能，并描述测试的目标；
b） 测试过程，应标识要执行的测试，并描述每个安全功能的测试概况；
c） 预期的测试结果，应表明测试成功后的预期输出；
d） 实际测试结果，应表明每个被测试的安全功能能按照规定进行运作。

7 测评方法

7.1 安全功能测试

7.1.1 工业控制设备识别

对工业控制设备自动识别的测试方法与预期结果如下：
a） 测试方法：
在漏洞检测产品上输入 IP 地址，漏洞检测产品向该 IP 地址发送测试报文。
b） 预期结果：
1） 对于有效的 IP 地址，漏洞检测产品能够自动识别工业控制设备、正确显示设备厂商名称和设备类型，或提示用户手动添加工业控制设备；
2） 对于无效的 IP 地址，漏洞检测产品报错。

7.1.2 工业控制设备端口扫描

对工业控制设备端口扫描的测试方法与预期结果如下：

a) 测试方法：

漏洞检测产品向工业控制设备的所有 TCP 端口和 UDP 端口发送测试报文。

b) 预期结果：

1) 漏洞检测产品能够根据工业控制设备的响应报文识别出所有开启的 TCP 端口和 UDP 端口；

2) 对于已知的 TCP 端口、UDP 端口，漏洞检测产品能够显示出与之对应的工业控制通信协议。

7.1.3 工业控制设备通信协议漏洞检测

7.1.3.1 工业以太网协议漏洞检测

工业以太网协议漏洞检测的测试方法与预期结果如下：

a) 测试方法：

1) 漏洞检测产品逐一选取 6.1.3 a)中的工业以太网协议；

2) 漏洞检测产品向工业控制设备发送包含工业以太网协议已知漏洞的测试报文。

b) 预期结果：

1) 漏洞检测产品能够支持 6.1.3 a)中的全部工业以太网协议；

2) 漏洞检测产品能通过工业控制设备的响应来发现工业控制设备是否存在的已知漏洞；

3) 漏洞检测产品能够记录所发现的已知漏洞。

7.1.3.2 互联网协议漏洞检测

用于工业控制的互联网协议漏洞检测的测试方法与预期结果如下：

a) 测试方法：

1) 漏洞检测产品逐一选取 6.1.3 b)的互联网协议；

2) 漏洞检测产品向工业控制设备发送包含互联网协议已知漏洞的测试报文。

b) 预期结果：

1) 漏洞检测产品能够支持 6.1.3 b)中的互联网协议；

2) 漏洞检测产品能通过工业控制设备的响应来发现工业控制设备是否存在的已知漏洞；

3) 漏洞检测产品能够记录所发现的已知漏洞。

7.1.3.3 串口协议漏洞检测

用于工业控制的串口协议漏洞检测的测试方法与预期结果如下：

a) 测试方法：

1) 漏洞检测产品逐一选取 6.1.3 c)中的串口协议；

2) 漏洞检测产品向工业控制设备发送包含串口协议已知漏洞的测试报文。

b) 预期结果：

1) 漏洞检测产品能够支持 6.1.3 c)中的串口协议；

2) 漏洞检测产品能通过工业控制设备的响应来发现工业控制设备是否存在的已知漏洞；

3) 漏洞检测产品能够记录所发现的已知漏洞。

7.1.3.4 工业控制私有协议漏洞检测

工业控制私有协议漏洞检测的测试方法与预期结果如下：

a） 测试方法：

1） 漏洞检测产品逐一选取所支持的私有协议；

2） 漏洞检测产品向工业控制设备发送包含该协议已知漏洞的测试报文。

b） 预期结果：

1） 漏洞检测产品能通过工业控制设备的响应来发现工业控制设备是否存在的已知漏洞；

2） 漏洞检测产品能够记录所发现的已知漏洞。

7.1.4 工业控制组态软件漏洞检测

工业控制组态软件漏洞检测的测试方法与预期结果如下：

a） 测试方法：

在漏洞检测产品上运行针对工业控制组态软件漏洞的测试用例。

b） 预期结果：

1） 漏洞检测产品能通过工业控制设备的响应，来发现工业控制设备是否存在已知工业控制组态软件漏洞；

2） 漏洞检测产品能够记录所发现的已知漏洞。

7.1.5 工业控制设备操作系统检测

工业控制设备操作系统检测的测试方法与预期结果如下：

a） 测试方法：

1） 工业控制设备预置登录弱口令，并开放被测端口；

2） 在漏洞检测产品上运行弱口令测试用例；

3） 在漏洞检测产品上运行操作系统安全漏洞测试用例。

b） 预期结果：

1） 漏洞检测产品能够识别工业控制设备的操作系统类型和版本号；

2） 漏洞检测产品能够检测出登录弱口令；

3） 漏洞检测产品能够检测出并记录工业控制设备操作系统的已知安全漏洞。

7.1.6 工业控制数据库漏洞检测

工业控制数据库漏洞检测的测试方法与预期结果如下：

a） 测试方法：

漏洞检测产品向工业控制数据库服务器发送包含数据库已知漏洞的报文。

b） 预期结果：

漏洞检测产品能够检测出并记录工业控制数据库的已知漏洞。

7.1.7 工业控制网络通信设备漏洞检测

工业控制网络通信设备漏洞检测的测试方法与预期结果如下：

a） 测试方法：

漏洞检测产品向工业控制网络通信设备发送包含该型号设备已知漏洞的报文。

b） 预期结果：

漏洞检测产品能够检测出并记录工业控制网络通信设备存在的已知漏洞。

7.1.8 漏报测试

漏报测试方法与预期结果如下：

a） 测试方法：

1） 选取某型号具有已知安全漏洞的工业控制设备，记录其已知安全漏洞；

2） 使用检测产品对该设备进行漏洞检测；

3） 对比检测报告中列出的安全漏洞和该设备的已知安全漏洞。

b） 预期结果：

如果检测报告中列出的安全漏洞包括该设备的全部已知安全漏洞，则无漏报，否则有漏报。

注：该测试需要对多种类型的工业控制设备进行测试，以保证测试结论的有效性。

7.1.9 误报测试

误报测试方法与预期结果如下：

a） 测试方法：

1） 选取某型号具有已知安全漏洞的工业控制设备，记录其已知安全漏洞；

2） 使用漏洞检测产品对该设备进行漏洞检测；

3） 对比检测报告中列出的已知安全漏洞和该设备的已知安全漏洞。

b） 预期结果：

如果检测报告中列出的已知安全漏洞超出该设备的全部已知安全漏洞，或者将 A 漏洞判别为 B 漏洞，则有误报，否则无误报。

注：该测试需要对多种类型的工业控制设备进行测试，以保证测试结论的有效性。

7.1.10 检测结果处理

7.1.10.1 工业控制设备状态监测

工业控制设备状态监测的测试方法与预期结果如下：

a） 测试方法：

1） 在漏洞检测产品上运行测试集合；

2） 暂停或者终止测试集合。

b） 预期结果：

1） 能够在漏洞检测产品上实时查看检测进度；

2） 能够在漏洞检测产品上实时查看测试用例每一步骤的执行结果；

3） 能够在漏洞检测产品上监测工业控制设备的实时响应；

4） 能够在漏洞检测产品上随时暂停或者终止测试。

7.1.10.2 检测结果记录

检测结果记录的测试方法与预期结果如下：

a） 测试方法：

1） 检查漏洞检测产品是否具有记录检测结果的数据库或数据文件；

2） 检查漏洞检测产品的数据库或数据文件中是否包含导致工业控制设备异常响应的测试报文。

b） 预期结果：

1） 漏洞检测产品具有记录检测结果的数据库或数据文件；

2） 数据库或数据文件中包含导致工业控制设备异常响应的测试报文。

7.1.10.3 检测报告生成

检测报告生成的测试方法与预期结果如下：

a） 测试方法：

1） 查看漏洞检测产品的报告生成功能；

2） 查看报告的生成方式；

3） 查看报告的内容。

b） 预期结果：

1） 漏洞检测产品具有生成报告的功能；

2） 漏洞检测产品提供默认的模板以供快速生成报告；

3） 漏洞检测产品的报告可支持多种图形表格形式，并可生成日报、周报等汇总报告；

4） 漏洞检测产品的报告支持多种文档格式；

5） 漏洞检测产品的报告包括所有检测出的漏洞的名称、类型、编号、漏洞发布日期、漏洞概要描述等信息；

6） 漏洞检测产品的报告包括对被检测设备的危险等级评估，扫描脆弱点按风险严重程度分级，并明确标出。

7.1.10.4 检测中断时的报告生成

检测中断时的报告生成的测试方法与预期结果如下：

a） 测试方法：

1） 在漏洞检测产品上运行测试集合；

2） 随机终止测试。

b） 预期结果：

终止测试后，漏洞检测产品能生产成已检测部分的报告，并说明测试终止的情况。

7.1.11 管理控制功能

7.1.11.1 检测参数设置

检测参数设置的测试方法与预期结果如下：

a） 测试方法：

检查漏洞检测产品是否可以设置检测参数。

b） 预期结果：

漏洞检测产品能够设置检测参数（例如，扫描地址范围、端口范围、漏洞类型、测试报文、测试次数、测试时间间隔等）。

7.1.11.2 检测方式

检测方式的测试方法与预期结果如下：

a） 测试方法：

1） 检查漏洞检测产品是否能够依据工业控制通信协议将测试用例进行归类；

2） 检查漏洞检测产品是否支持测试用例随机组合；

3） 检查漏洞检测产品是否支持测试集合随机组合；

4） 检查漏洞检测产品是否支持用户编写测试用例；

5） 检查漏洞检测产品是否根据设备类型向用户推荐某类或某几类测试用例。

b） 预期结果：

1） 漏洞检测产品能够依据工业控制通信协议将测试用例进行归类；

2） 漏洞检测产品支持测试用例随机组合；

3） 漏洞检测产品支持测试集合随机组合；

4） 漏洞检测产品支持用户编写测试用例；

5） 漏洞检测产品能够根据设备类型向用户推荐某类或某几类测试用例。

7.1.11.3 设备信息库管理

设备信息库管理的测试方法与预期结果如下：

a） 测试方法：

1） 检查漏洞检测产品是否具有工业控制设备信息库；

2） 检查漏洞检测产品是否允许用户自定义及增删设备型号；

3） 检查漏洞检测产品是否能够添加新增设备的特征信息。

b） 预期结果：

1） 漏洞检测产品具有工业控制设备信息库；

2） 漏洞检测产品允许用户自定义及增删设备型号；

3） 漏洞检测产品能够添加新增设备的特征信息。

7.1.11.4 漏洞库管理

漏洞库管理的测试方法与预期结果如下：

a） 测试方法：

1） 检查漏洞检测产品是否具有漏洞管理库；

2） 检查是否能够在漏洞检测产品中添加新的安全漏洞。

b） 预期结果：

1） 漏洞检测产品具有漏洞管理库；

2） 漏洞检测产品能够添加新的安全漏洞。

7.1.11.5 测试用例库管理

测试用例库管理的测试方法与预期结果如下：

a） 测试方法：

1） 检查漏洞检测产品是否具有测试用例库；

2） 检查是否能够修改、增加、删除测试用例或测试集合。

b） 预期结果：

1） 漏洞检测产品具有测试用例库；

2） 库中包含测试用例和测试集合；

3） 检查漏洞检测产品允许用户修改、增加、删除测试用例或测试集合。

7.2 自身安全测试

7.2.1 用户管理与鉴别

7.2.1.1 用户管理

用户管理的测试方法与预期结果如下：

a） 测试方法：

1） 检查漏洞检测产品是否具有用户管理功能；
2） 检查漏洞检测产品是否能够为用户设置安全属性。

b） 预期结果：
1） 漏洞检测产品能够添加、删除、激活、禁止用户；
2） 漏洞检测产品能够设置用户的安全属性。

7.2.1.2 用户鉴别

用户鉴别的测试方法与预期结果如下：

a） 测试方法：
登录控制台，检查要求进行身份鉴别。

b） 预期结果：
1） 当用户登录对用户进行鉴别，拒绝未通过鉴别的用户登录；
2） 登录之前允许做的操作，仅限于输入登录信息、查看登录帮助等操作；
3） 允许用户在登录后执行与其安全功能相关的各类操作时，不再重复鉴别。

7.2.1.3 鉴别失败处理

鉴别失败处理的测试方法与预期结果如下：

a） 测试方法：
1） 检查漏洞检测产品的安全功能是否可定义用户鉴别尝试的最大允许失败次数；
2） 检查漏洞检测产品的安全功能是否可定义当用户鉴别尝试失败连续达到指定次数后，采取相应的措施、阻止用户进一步的鉴别请求；
3） 尝试多次失败的用户鉴别行为，检查到达指定的鉴别失败次数后，漏洞检测产品是否采取了相应的措施，并生成了审计事件。

b） 预期结果：
1） 漏洞检测产品具备定义用户鉴别尝试的最大允许失败次数的功能；
2） 当用户鉴别尝试失败连续达到指定次数后，漏洞检测产品能够锁定该账号，并将有关信息生成审计事件；
3） 最多失败次数仅由授权用户设定。

7.2.1.4 超时设置

超时设置的测试方法与预期结果如下：

a） 测试方法：
1） 检查漏洞检测产品是否具有用户登录超时重新鉴别功能；
2） 设定用户登录超时重新鉴别的时间段，检查登录用户在设定的时间段内没有任何操作的情况下，漏洞检测产品是否锁定或终止了会话，用户是否需要再次进行身份鉴别才能够重新管理和使用漏洞检测产品。

b） 预期结果：
1） 漏洞检测产品具有登录超时重新鉴别功能；
2） 任何登录用户在设定的时间段内没有任何操作的情况下，应被锁定或终止了会话，管理员需要再次进行身份鉴别才能够重新管理和使用漏洞检测产品；
3） 最大超时时间仅由授权管理员设定。

7.2.1.5 远程管理

远程管理的测试方法与预期结果如下：

a） 测试方法：

1） 通过控制台设置可以进行远程管理的主机地址；

2） 检查是否在执行所有功能之前要求首先进行主机地址；

3） 检查传输过程是否采用了保密性和完整性保护手段。

b） 预期结果：

1） 可以设置远程管理主机地址；

2） 在通过远程主机进行任何与安全功能相关的操作之前都应进行鉴别，拒绝未通过鉴别的管理请求；

3） 传输过程采用了保密性和完整性保护手段。

7.2.2 产品升级

7.2.2.1 升级功能

升级功能的测试方法与预期结果如下：

a） 测试方法：

1） 检查漏洞检测产品的升级方式；

2） 进行产品升级。

b） 预期结果：

1） 可以对漏洞检测产品进行升级；

2） 漏洞检测产品在升级的过程中可以正常工作；

3） 漏洞检测产品在升级后可以正常工作。

7.2.2.2 升级包校验

升级包校验功能的测试方法与预期结果如下：

a） 测试方法：

使用经过破坏性修改的升级包进行升级。

b） 预期结果：

漏洞检测产品无法升级并显示将完整性校验结果。

7.2.3 日志管理

7.2.3.1 安全日志生成

安全日志生成的测试方法与预期结果如下：

a） 测试方法：

1） 结合开发者文档，使用不同角色管理员模拟对漏洞检测产品进行访问、运行、修改、关闭以及重复失败尝试等相关操作，检查漏洞检测产品提供了对哪些事件的审计；

2） 审查安全日志的正确性。

b） 预期结果：

1） 漏洞检测产品至少为下述可审计事件产生安全日志：用户登录、用户退出、鉴别失败、设备重启、安全配置更改等重大事件，产品升级时间和版本号等；

2） 在每条安全日志中至少记录如下信息：事件发生的日期、时间、用户标识、事件类型、事件描述和结果、远程登录的管理主机的地址。

7.2.3.2 安全日志管理

安全日志管理的测试方法与预期结果如下：

a） 测试方法：

1） 模拟授权与非授权管理员访问安全日志，检查是否仅允许授权管理员访问安全日志；

2） 检查是否可以进行日志查询；

3） 检查是否可以修改日志；

4） 检查日志是否能够导出。

b） 预期结果：

1） 除了具有明确的访问权限的授权管理员之外，禁止所有其他用户对安全日志的访问；

2） 提供日志查询功能；

3） 允许授权管理员保存或删除安全日志；

4） 日志能够以通用格式导出。

7.2.4 安全存储

安全存储的测试方法与预期结果如下：

a） 测试方法：

1） 用户登录后，尝试读取其他用户创建的测试任务的数据；

2） 用户删除测试任务后，检查是否存在相关的测试数据；

3） 用户导出测试任务数据，用户导入测试任务数据。

b） 预期结果：

1） 用户无法读取其他用户创建的测试任务的数据；

2） 相关的测试数据已被删除；

3） 相关的测试任务数据可以被正确的导入和导出。

7.3 安全保障评估方法

7.3.1 配置管理

7.3.1.1 版本号

版本号的测试方法与预期结果如下：

a） 测试方法：

评价者应审查开发者提供的配置管理支持文件是否包含以下内容：版本号，要求开发者所使用的版本号与所应表示的产品样本完全对应，没有歧义。

b） 预期结果：

审查记录以及最后结果符合测试方法要求，开发者应提供唯一版本号。

7.3.1.2 配置项

配置项的测试方法与预期结果如下：

a） 测试方法：

评价者应审查开发者所提供的信息是否满足如下要求：

1） 配置管理功能应对所有的配置项定义唯一的标识。

2） 配置管理文档应包括配置清单、配置管理计划。配置清单用来描述组成系统的配置项。

3） 配置管理文档还应描述对配置项给出唯一标识的方法。

b) 预期结果：

审查记录以及最后结果符合测试方法要求，评价者审查内容至少包括测试方法中的 3 个方面。

7.3.2 交付与运行

7.3.2.1 交付程序

交付程序的测试方法与预期结果如下：

a) 测试方法：

评价者应审查开发者是否使用一定的交付程序交付系统，并使用文档描述交付过程，并且评价者应审查开发者交付的文档是否包含以下内容：在给用户方交付系统的各版本时，为维护安全所必需的所有程序。

b) 预期结果：

测试记录以及最后结果符合测试方法要求，开发者应提供完整的文档描述所有交付的过程（文档和程序交付）。

7.3.2.2 安装、生成和启动程序

安装、生成和启动程序的测试方法与预期结果如下：

a) 测试方法：

评价者应审查开发者是否提供了文档说明系统的安装、生成、启动和使用的过程。用户能够通过此文档了解安装、生成、启动和使用过程。

b) 预期结果：

审查记录以及最后结果符合测试方法要求。

7.3.3 开发

7.3.3.1 功能规范

功能规范的测试方法与预期结果如下：

a) 测试方法：

评价者应审查开发者所提供的信息是否满足如下要求：

1) 功能设计应描述产品安全功能与其外部接口；
2) 功能设计应是内在一致的；
3) 功能设计应描述使用所有外部产品安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和出错信息的细节；
4) 功能设计应完整地表示产品安全功能；
5) 评价者应确认功能设计是否是系统安全要求的精确和完整的示例。

b) 预期结果：

审查记录以及最后结果符合测试方法要求，评价者审查内容至少包括测试方法中的 4 个方面。开发者提供的内容应精确和完整。

7.3.3.2 高层设计

描述性高层设计的测试方法与预期结果如下：

a) 测试方法：

评价者应审查开发者所提供的信息是否满足如下要求：

1) 是内在一致的；

2） 按子系统描述安全功能的结构；
3） 描述每个安全功能子系统所提供的安全功能性；
4） 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
5） 标识安全功能子系统的所有接口；
6） 标识安全功能子系统的哪些接口是外部可见的。

b） 预期结果：
审查记录以及最后结果符合测试方法要求，评价者审查内容至少包括测试方法中的 6 个方面。开发者提供的高层设计内容应精确和完整。

7.3.4 指导性文档

7.3.4.1 管理员指南

管理员指南的测试方法与预期结果如下：

a） 测试方法：
评价者应审查开发者是否提供了供授权管理员使用的管理员指南，并且此管理员指南是否包括如下内容：
1） 产品可以使用的管理功能和接口；
2） 安全地管理产品；
3） 在安全处理环境中应进行控制的功能和权限；
4） 对与产品的安全操作有关的用户行为的假设；
5） 受管理员控制的安全参数，如果可能，应指明安全值；
6） 与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；
7） 与授权管理员有关的 IT 环境的安全要求。

b） 预期结果：
测试记录以及最后结果符合测试方法要求，评价者审查内容至少包括测试方法中的 7 个方面。开发者提供的管理员指南应完整。

7.3.4.2 用户指南

用户指南的测试方法与预期结果如下：

a） 测试方法：
评价者应审查开发者是否提供了供系统用户使用的用户指南，并且此用户指南是否包括如下内容：
1） 产品的非管理用户可使用的安全功能和接口；
2） 产品提供给用户的安全功能和接口的用法；
3） 用户可获取但应受安全处理环境控制的所有功能和权限；
4） 产品安全操作中用户所应承担的职责；
5） 与用户有关的 IT 环境的所有安全要求。

b） 预期结果：
测试记录以及最后结果符合测试方法要求，评价者审查内容至少包括测试方法中的 5 个方面。开发者提供的用户指南应完整。

7.3.5 测试

7.3.5.1 测试覆盖

测试覆盖的测试方法与预期结果如下：

a) 测试方法：

评价者应审查开发者提供的测试覆盖证据，在测试覆盖证据中，是否表明测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。

b) 预期结果：

审查记录以及最后结果符合测试方法要求，开发者提供的测试覆盖证据，应表明测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。

7.3.5.2 功能测试

功能测试的测试方法与预期结果如下：

a) 测试方法：

1) 评价开发者提供的测试文档，是否包括测试计划、测试规程、预期的测试结果和实际测试结果；

2) 评价测试计划是否标识了要测试的安全功能，是否描述了测试的目标；

3) 评价测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况(这些概况包括对其他测试结果的顺序依赖性)；

4) 评价期望的测试结果是否表明测试成功后的预期输出；

5) 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

b) 预期结果：

测试记录以及最后结果符合测试方法要求，评价者审查内容至少包括测试方法中的 5 个方面。开发者提供的内容应完整。

附 录 A
（规范性附录）
工业控制系统漏洞检测产品安全功能等级划分

工业控制系统漏洞检测产品的安全功能等级划分如表 A.1 所示。

表 A.1 安全功能等级划分

安全技术要求		基本级	增强级
安全功能要求	工业控制设备识别	6.1.1	6.1.1
	工业控制设备端口扫描	6.1.2	6.1.2
	工业控制设备通信协议漏洞检测	6.1.3 a)、b)	6.1.3 a)～d)
	工业控制组态软件漏洞检测	6.1.4	6.1.4
	工业控制设备操作系统检测	6.1.5	6.1.5
	工业控制数据库漏洞检测	6.1.6	6.1.6
	工业控制网络通信设备漏洞检测	6.1.7	6.1.7
	检测结果处理要求	6.1.8	6.1.8
	管理控制功能要求	6.1.9	6.1.9
自身安全要求	用户管理与鉴别	6.2.1 a)～d)	6.2.1 a)～f)
	产品升级	6.2.2	6.2.2
	日志管理	6.2.3	6.2.3
	安全存储	6.2.4	6.2.4
安全保障要求	配置管理	6.3.1	6.3.1
	交付与运行	6.3.2	6.3.2
	开发	6.3.3	6.3.3
	指导性文档	6.3.4	6.3.4
	测试	6.3.5	6.3.5

附 录 B
（规范性附录）
工业控制系统漏洞检测产品测评方法分级及其测评项

工业控制系统漏洞检测产品测评方法的分级及其测评项如表 B.1 所示。

表 B.1 工业控制系统漏洞检测产品测评方法分级及其测评项

安全技术要求		基本级	增强级
安全功能测试	工业控制设备识别	7.1.1	7.1.1
	工业控制设备端口扫描	7.1.2	7.1.2
	工业控制设备通信协议漏洞检测	7.1.3.1、7.1.3.2	7.1.3.1～7.1.3.4
	工业控制组态软件漏洞检测	7.1.4	7.1.4
	工业控制设备操作系统检测	7.1.5	7.1.5
	工业控制数据库漏洞检测	7.1.6	7.1.6
	工业控制网络通信设备漏洞检测	7.1.7	7.1.7
	漏报测试	7.1.8	7.1.8
	误报测试	7.1.9	7.1.9
	检测结果处理	7.1.10	7.1.10
	管理控制功能	7.1.11	7.1.11
自身安全测试	用户管理与鉴别	7.2.1.1～7.2.1.3	7.2.1.1～7.2.1.5
	产品升级	7.2.2	7.2.2
	日志管理	7.2.3	7.2.3
	安全存储	7.2.4	7.2.4
安全保障评估方法	配置管理	7.3.1	7.3.1
	交付与运行	7.3.2	7.3.2
	开发	7.3.3	7.3.3
	指导性文档	7.3.4	7.3.4
	测试	7.3.5	7.3.5

参 考 文 献

[1] GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件

[2] GB/T 20275—2013 信息安全技术 网络入侵检测系统技术要求和测试评价方法

[3] GB/T 20278—2013 信息安全技术 网络脆弱性扫描产品安全技术要求

[4] GB/T 30279—2013 信息安全技术 安全漏洞等级划分指南

[5] GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

[6] SSA-420 Vulnerability Identification Test (VIT) Policy Specification