ICS 25.040
N 10

中华人民共和国国家标准

GB/T 30976.2—2014

工业控制系统信息安全
第2部分：验收规范

Industrial control system security—Part 2: Acceptance specification

2014-07-24 发布　　2015-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 30976《工业控制系统信息安全》分为两个部分：

——第1部分：评估规范；

——第2部分：验收规范。

本部分为GB/T 30976的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量和控制标准化技术委员会(SAC/TC 124)和全国信息安全标准化技术委员会(SAC/TC 260)归口。

本部分起草单位：机械工业仪器仪表综合技术经济研究所、中国电子技术标准化研究院、北京和利时系统工程有限公司、北京钢铁设计研究总院、中国电力科学研究院、清华大学、浙江大学、西南大学、重庆邮电大学、华中科技大学、中国核电工程有限公司、上海自动化仪表股份有限公司、东土科技股份有限公司、北京奥斯汀科技有限公司、西门子(中国)有限公司、施耐德电气(中国)有限公司、罗克韦尔自动化(中国)有限公司、三菱电机自动化(中国)有限公司、中国仪器仪表学会、中国科学院沈阳自动化研究所、无线网络安全技术国家工程实验室、西安西电捷通无线网络通信股份有限公司、中央办公厅电科院、北京海泰方圆科技有限公司、青岛多芬诺信息安全技术有限公司、北京国电智深控制技术有限公司、北京力控华康科技有限公司、横河电机(中国)有限公司北京研发中心、中标软件有限公司、华北电力设计院工程有限公司、华为数字技术(成都)有限公司、广东航宇卫星科技有限公司。

本部分主要起草人：丁露、唐一鸿、罗安、夏德海、高昆仑、王雪、冯冬芹、刘枫、王浩、周纯杰、吕冬宝、张建军、薛百华、陈小枫、隋爱芬、陈小淙、华镕、龚明、张莉、宋岩、李琴、胡亚楠、王雄、胡伯良、刘安正、田雨聪、方亮、杨磊、何佳、马欣欣、张建勋、杨应良、梅恪、王玉敏、王勇、杜佳琳、王亦君、陈日罡、张涛、王玉裴、刘利民、丁青芝、刘文龙、钱晓斌、朱镜灵、张智。

引　言

近年来，网络技术的飞速发展和各类信息安全事故的频繁发生，使得工业自动化和控制系统通信网络中的信息安全得到越来越多的关注。用于工业自动化系统的网络通信技术不同于办公环境使用的计算机网络技术。办公网络的信息安全通常采用杀毒软件和防火墙等软硬件方案解决安全问题。在工业应用环境，对网络安全有着更高要求，恶意软件的入侵将会造成生产线停车、人员伤害、信息泄漏，从而严重威胁到人员生命安全、工业生产运行安全、国家安全等严重后果。随着大型的工业自动化控制系统越来越广泛的应用，作为整个工业自动化控制网络的核心，其信息安全问题就成为重中之重。

本部分规定了对实施安全解决方案的工业控制系统信息安全能力进行验收的验收流程、测试内容、方法及应达到的要求。这些测试是为了证明工业控制系统在增加安全解决方案后满足对安全性的要求，并且保证其主要性能指标在允许范围内。本标准的各项内容可作为实际工作中的指导，适用于各种工艺装置、工厂和控制系统。

工业控制系统信息安全
第2部分:验收规范

1 范围

GB/T 30976的本部分规定了对工业控制系统的信息安全解决方案的安全性进行验收的流程、测试内容、方法及应达到的要求。该方案可以通过增加设备或系统提高其安全性。

本部分的各项内容可作为实际工作中的指导,适用于石油、化工、电力、核设施、交通、冶金、水处理、生产制造等行业使用的控制系统和设备。

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 2423.1—2008 电工电子产品环境试验 第2部分:测试方法 试验A:低温(IEC 60068-2-1:2007,IDT)

GB/T 2423.2—2008 电工电子产品环境试验 第2部分:测试方法 试验B:高温(IEC 60068-2-2:2007,IDT)

GB 3836.1 爆炸性环境 第1部分:设备 通用要求(GB 3836.1—2010,IEC 60079-0:2007,MOD)

GB 3836.2 爆炸性环境 第2部分:由隔爆外壳"d"保护的设备(GB 3836.2—2010,IEC 60079-1:2007,MOD)

GB 3836.4 爆炸性环境 第4部分:由本质安全型"i"保护的设备(GB 3836.4—2010,IEC 60079-11:2006,MOD)

GB 4793.1—2007 测量、控制和实验室用电气设备的安全要求 第1部分:通用要求(IEC 61010-1:2001,IDT)

GB/T 15153.1—1998 远动设备及系统 第2部分:工作条件 第1篇:电源和电磁兼容性(IEC 60870-2-1:1995,IDT)

GB/T 15153.2—2000 远动设备及系统 第2部分:工作条件 第2篇:环境条件(气候、机械和其他非电影响因素)(IEC 606870-2-2:1996,IDT)

GB/T 18018—2007 信息安全技术 路由器安全技术要求

GB/T 18268.1—2010 测量、控制和实验室用的电设备 电磁兼容性要求 第1部分:通用要求(IEC 61326-1:2005,IDT)

GB/T 18272.4—2006 工业过程测量和控制 系统评估中系统特性的评定 第4部分:系统性能评估(IEC 61069-4:1997,IDT)

GB/T 25068.3—2010 信息技术 安全技术 IT网络安全 第3部分:使用安全网关的网间通信安全保护(ISO/IEC 18028-3:2005,IDT)

GB/T 25069—2010 信息安全技术 术语

GB/T 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

3 术语和定义

GB/T 25069—2010 和 GB/T 30976.1—2014 界定的以及下列术语和定义适用于本文件。

3.1

实施 implementation

将一系列活动付诸实践的过程。

3.2

系统生命周期 system lifecycle

系统的各个生命阶段，包括规划阶段、设计阶段、实施阶段、运行维护阶段和废弃阶段。

3.3

识别 identify

对某一评估要素进行标识与辨别的过程。

3.4

风险处置 risk treatment

对风险进行处理的一系列活动，如接受风险、规避风险、转移风险、降低风险等。

3.5

验收 acceptance

风险评估活动中用于结束项目实施的一种方法，主要由被评估方组织，对评估活动进行逐项检验，以是否达到评估目标为接受标准。

3.6

买方 buyer

从供应商处直接购买控制系统并对其负责的企业，既可以是业主也可以是总承包商。

3.7

业主 owner

雇佣总承包商去建设诸如化工厂、石化厂这类工厂的企业。

3.8

总承包商 contractor

被业主雇佣承建诸如化工厂、石化厂这类工厂的企业。

3.9

供应商 vendor

自动化系统的制造商或分包商。

3.10

性能 performance

系统在规定条件下执行任务的准确性和速度。

3.11

实时性 real-time

在限定时间内完成指定任务的能力。

3.12

可靠性 reliability

在规定的条件下和在给定的时间间隔内，产品完成规定功能的能力。

[IEC 60050(191):1990 191-2-6]

3.13

精确度　accuracy

系统在规定条件下执行并实现的信息转换与规定的信息转换之间的一致程度。

3.14

响应时间　response time

在规定条件下，从信息转换开始至发生相关响应那一瞬间的时间间隔。

3.15

处理能力　capacity

在不至于影响系统特性的状态下，系统能够在规定的时间内执行指定信息转换的最大数量。

4　概述

4.1　验收的基本原则

在验收工业控制系统信息安全解决方案的安全性时，应依据业主提出的信息安全要求或能力等级要求。相关技术要求和等级分类见 GB/T 30976.1—2014。

对于在运行系统的验收测试，应采用最小影响原则，即首要保障系统的稳定运行。对于需要进行攻击性测试的工作内容，需与业主和供应商沟通并进行备份，尽量选择非运行时间进行。

4.2　验收流程

图 1 示出了验收活动顺序。根据业主提出的安全性要求给出信息安全解决方案，通过增加设备或系统来降低风险，并由业主最终决定是否通过验收。对其验收时如果没有通过，则进行整改，再重新验收，直至最后通过。

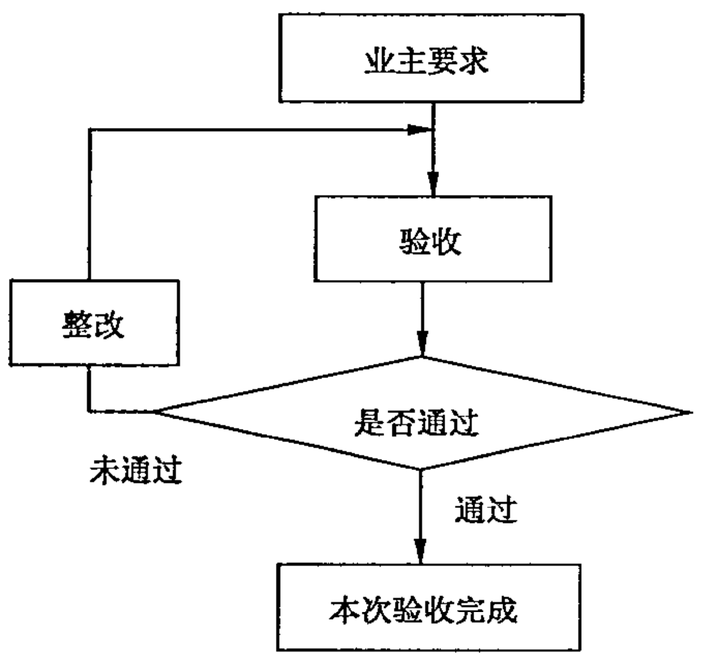

图 1　工业控制系统信息安全验收活动顺序示意图

验收过程划分为验收准备、风险分析与处置、能力确认三个阶段。

验收准备阶段工作是验收有效性的重要保证，是验收工作的开始，首先各参与方共同明确验收目标，核查相关文档。

风险分析与处置阶段是验收工作的核心内容，主要是结合评估阶段给出的评估结论和改进措施(如果涉及)，依据供应商出具的文档对新增加的安全保障系统可能产生的各类风险进行分析，判断是否有相应的风险处置，并提出解决方案。

能力确认阶段主要针对分析出的风险及其处置方法，判断选用的设备是否符合设定要求，以及设备集成到工控系统后整体信息安全和基本性能是否符合设定要求。能力确认阶段包括三个部分，即设备

离线测试、系统集成测试和确定验收结论。

附录 A 列出的清单有助于顺利实施验收活动。根据规范的说明，过程中发现的未完成工作或不符合规范的部分将记录在验收不符合项表中(参见附录 C)。

不符合项的处理归为如下几类：

a) 当场整改，然后继续进行验收测试；

b) 在验收过程中同时进行整改；

c) 需再次进行验收；

d) 在验收完成后进行整改。

当参与方根据验收程序和相关规范完成验收测试，并证实了除双方已认可的不符合项外，所有必须的功能已实现后，可认为系统成功通过验收。此时，买方的授权代表和供应商应共同在验收证书(参见附录 B)上签名。

4.3 验收测试进度表

参与方应共同制定一份包含测试项目和时间进度的测试进度表，表中应包括，但不仅限于以下内容：

项目	内 容
验收准备阶段	1. 启动会议
	2. 业主/总承包商、供应商文件检查
风险分析与处置阶段	3. 方案制定(风险分析、风险处置)
能力确认阶段	4. 软硬件清单核对
	5. 安装和接线检查
	6. 启动测试
	7. 系统常规功能检查
	8. 信息安全功能检查
	9. 复检，列出不符合项表
	10. 验收总结会议

4.4 验收的工作形式

验收的基本工作形式包括自验收和第三方验收。自验收是系统的拥有、运营或使用单位发起的对本单位系统进行的验收。第三方验收是委托第三方负责实施的验收。

5 验收准备阶段

5.1 确定验收目标和范围

由于工业控制系统生命周期各阶段中风险的内容、验收的对象、安全需求均不同，因此业主应首先根据当前实际情况确定在工控系统生命周期中所处的阶段，并以此来明确验收目标。

在确定验收目标后，应进一步明确验收工作的考核范围。在确定验收范围时，应结合已确定的验收目标和用户的实际系统建设情况，合理定义验收对象的范围边界，可以参考以下依据来作为验收范围边界的划分原则：

a) 业务系统的业务逻辑边界；

b) 网络及设备载体边界；

c) 物理环境边界；

d) 用户管理权限边界；

e) 其他。

验收的目标、范围和标准应得到利益相关方的认可。在实施对工控系统控制能力可能产生影响的任何附加安全解决方案之前，应征求控制系统原始设计方的意见。

5.2 文档准备

5.2.1 概述

在开始验收工作之前，供应商应已完成所有的内部测试，并提供可供复查的测试报告或有关机构的评估报告，准备好相关文件以备验收过程中使用。下面列出了常用文件的清单，该清单可根据工程项目的实际情况进行协商(包括文件提供方)、取舍和增减。

5.2.2 业主/总承包商通常准备的文件

——相关规范(如参考标准、管理规程等)；

——商定的相关协议(如安全性要求等)；

——功能规划；

——评估报告；

——改进要求；

——验收方案；

——验收测试指导书。

5.2.3 供应商通常准备的文件

——信息安全解决方案；

——工业控制系统或设备使用手册、系统数据资料、证书等；

——系统设计说明；

——硬件设计说明；

——软件设计说明；

——接口说明；

——操作画面说明；

——内部测试报告；

——测试计划。

6 风险分析与处置阶段

6.1 系统风险分析

系统风险分析主要是针对增加安全解决方案后可能产生的风险。风险分析阶段的关键控制点主要有以下两点：

a) 建立的风险分析模型及确定的风险计算方法，应能正确反应用户的行业安全特点，核心业务系统所处的内、外部环境安全状况；

b) 用户确认的信息、数据及相关文档资料应及时得到准确反馈。

风险分析报告是风险分析阶段的输出文档，是对风险分析阶段工作的总结。风险分析报告中需要

对建立的风险分析模型进行说明，并需要阐明采用的风险计算方法及风险评价方法。报告中应对计算分析出的风险给予详细说明，主要包括：风险对用户、业务及系统的影响范围、影响程度，依据的法规和证据，风险分析结论。

6.2 风险处置方案

风险处置依据风险分析报告进行风险处置。

风险处置的基本原则是根据用户可接受的处置成本将残余安全风险控制在可以接受的范围内。

依据国家、行业主管部门发布的信息安全建设要求进行的风险处置，应严格执行相关规定。实施的安全风险加固工作，应满足相应信息安全能力等级的安全技术和管理要求；对于因不能够满足该等级安全要求产生的风险则不能够适用适度接受风险的原则。对于有着行业主管部门特殊安全要求的风险处置工作，同样不适用该原则。

风险处置方式一般包括接受、消减、转移、规避等。在风险不适合转移或规避的情况下，通常采用安全整改进行风险消减。风险分析需提出安全整改建议。

安全整改建议需根据安全风险的严重程度、加固措施实施的难易程度、降低风险的时间紧迫程度、所投入的人员力量及资金成本等因素综合考虑。

a) 对于非常严重、需立即降低且加固措施易于实施的安全风险，建议用户立即采取安全整改措施。

b) 对于非常严重、需立即降低，但加固措施不便于实施的安全风险，建议用户立即制定安全整改实施方案，尽快实施安全整改；整改前应对相关安全隐患进行严密监控，并作好应急预案。

c) 对于比较严重、需降低且加固措施不易于实施的安全风险，建议用户制定限期实施的整改方案；整改前应对相关安全隐患进行监控。

7 能力确认阶段

7.1 设备要求

7.1.1 工业环境适应性要求

7.1.1.1 概述

用于工业现场的安全设备，应符合工业环境的相关要求。工业环境适应性要求包括：气候、电磁兼容、电气安全、机械适应性、外部电源和外壳防护要求。由于设备适用的行业不同，可增加行业特定的要求。

——气候环境要求主要包括温度、湿度、大气压力等。其中，温度要求为所有产品必须满足的条件，其余要求可根据实际应用环境由业主和制造厂商协商确定。

——电磁兼容要求包括对各类干扰的抗扰度及骚扰限值要求。

——电气安全要求包括绝缘电阻、绝缘强度要求。

——机械适应性要求包括正弦稳态振动、冲击和自由跌落要求。

——外部电源要求包括电源和接地要求。

——外壳防护要求包括防尘和防水要求。

如被测设备已通过相关测试，并获得认证证书，则可适当简化或跳过对应项目。

7.1.1.2 气候环境

设备在规定的工作温度范围内工作时，应符合其功能和性能规定。在规定的温度范围内贮存和运输时，不应发生裂痕、老化或其他损坏；当经受该温度范围后再恢复到工作温度范围时，设备应能正常

工作。

可能应用于温度快速变化场合的设备，在经受不超过 5 ℃/min 的温度变化时，应能正常工作。

工作温度、贮存、运输温度的要求见 GB/T 2423.1—2008 和 GB/T 2423.2—2008。

7.1.1.3 电磁兼容

对设备的电磁兼容性要求见 GB/T 18268.1—2010，包括电源电压暂降、电源电压短时中断、静电放电、射频电磁场辐射、电快速瞬变脉冲群、浪涌(冲击)、射频场感应的传导骚扰、工频磁场等。

7.1.1.4 电气安全

7.1.1.4.1 绝缘电阻

在一般试验大气条件下，设备的输入端子与外壳、输出端子与外壳、电源端子与外壳、输入端子与电源端子、输出端子与电源端子之间的绝缘电阻应不小于 20 MΩ。

7.1.1.4.2 绝缘强度(介电强度)

在一般试验大气条件下，设备的输入端子与外壳、输出端子与外壳、电源端子与外壳、输入端子与电源端子、输出端子与电源端子之间施加规定的试验电压，判定电流为 5 mA，保持 1 min，应不出现击穿或飞弧现象。

试验电压有效值应参照被试装置的额定电压(或绝缘电压)值和制造商规定的安全等级(Ⅰ或Ⅱ)加以确定。绝缘强度试验电压见 GB 4793.1—2007。

7.1.1.5 机械适应性

机械适应性要求见 GB/T 15153.2—2000。

7.1.1.6 外部电源

一般工业环境交流电源要求和直流电源要求见 GB/T 15153.1—1998，其中标称电压容差应为 10%～—10%。

7.1.1.7 外壳防护

设备外壳防护等级由制造厂商和业主协商确定。用于控制室内或机柜内的设备至少应达到 IP20 等级，用于现场的设备至少应达到 IP65 等级。

7.1.1.8 防爆性能

用于爆炸性危险场所的设备，其防爆性能应符合 GB 3836.1、GB 3836.2、GB 3836.4 的相关要求，并取得国家指定的防爆检验机构颁发的防爆合格证。

7.1.1.9 其他要求

7.1.1.9.1 外观

设备的结构件应有良好的表面处理，不应有镀层脱落、锈蚀、划伤、毛刺、锐角、玷污等痕迹；面板上的标志和文字应鲜明、清晰；显示屏显示亮度均匀，无异常现象。

7.1.1.9.2 连续工作性能

设备经 72 h 连续工作后，其基本误差仍应符合要求。

7.1.2 信息安全功能测试要求

7.1.2.1 对于控制设备的测试

7.1.2.1.1 健壮性测试

健壮性测试包括接口界面测试和协议特定健壮性测试。健壮性测试主要是针对基于 TCP/IP 的设备。如果对于非 TCP/IP 的设备，还需要针对其特定协议，进行通信健壮性测试。本健壮性测试适用以下测试项，但不限于这些项。

a) 接口界面测试

测试项 1：扫描所有 UDP 端口，确定哪些是开放的；

测试项 2：扫描所有 TCP 端口，确定哪些是开放的；

测试项 3：基于被测设备的功能来确定开放的端口；

测试项 4：扫描所有 IP 协议类型；

测试项 5：由于有些设备可能包含若干访问网络的接口，并可置于控制模式、组态模式、更新模式等多种模式中的任一种，如果被测设备支持若干操作模式，则应针对各种操作模式，在所有可访问网络的接口上进行 UDP 端口扫描、TCP 端口扫描和 IP 协议类型扫描；

测试项 6：高速率的端口和协议扫描。本测试项包括两个阶段，其中前述 UDP 端口扫描、TCP 端口扫描和 IP 协议类型扫描重复进行。第 1 阶段中，重复率较高，但低于设备标称值；第 2 阶段中，重复率首先设为网络可接受的最高速率，保持几秒后将发送率逐渐降低到零；

测试项 7：确定开放端口的方法应为可复制的。

如果被测设备在上述 7 项测试中仍能提供足够的基本服务，则认为该设备通过接口界面测试。

b) 协议特定健壮性测试

测试项 1：本健壮性测试项包括 3 个阶段。第 1 阶段，基线操作用于显示被测试的设备协议集在低负载的简单测试用例下操作适当；第 2 阶段，基本健壮性测试探查各特性对边界条件和特殊用例的敏感性，每次在一个报文中至多一个字段是错误的。基本健壮性测试应覆盖该协议报文的所有字段，并发送错误报文的序列来发现其对设备操作的累积影响；第 3 阶段，负载压力测试探查被测协议对高通信速率传输的有效协议数据单元的响应。

测试项 2：测试覆盖带冗余配置的设备。如果被测设备有冗余配置，则应在一个或多个冗余单元不可操作时，执行基本健壮性测试和负载压力健壮性测试。这些测试应覆盖各可能的可操作/不可操作单元数目。

测试项 3：测试覆盖字段值。基本健壮性测试应用一个良好定义的方法，通过产生通信数据来全面覆盖协议字段值。

测试项 4：应能绕过设备使用的 IP 地址黑名单等访问控制功能进行测试。当设备的防御机制会拒绝来自之前发送过可疑信息的某 IP 地址的通信，且该能力无法关闭时，适用该测试项。健壮性测试应能够产生用于测试的不同源 IP 地址的通信，以成功测试那些使用 IP 地址黑名单的设备。

测试项 5：测试设备应能支持一定范围的通信率。

如果设备能在上述 5 项测试下提供足够的上行和下行服务，并且满足其他针对该协议的通过条件，则认为该设备是通过协议特定健壮性测试。

适用场合：

——设备入网：验收将要上线的设备符合健壮性要求；

——健壮性测试不建议用于线上正在运行的设备。

7.1.2.1.2 基线检查

控制系统的一些在网设备不具备必要的安全功能，而且设备基础安全配置不够，如开放无用端口、口令安全，这是安全事件发生的重要原因之一。本标准从技术的角度提出设备应具备的安全功能和应实施的安全配置。任网络安全规范框架下，本系列标准属于测试、验收和运行环节的规范。

适用范围内设备应满足最低安全功能要求和推荐满足的安全功能要求。功能要求内容和具体厂家产品无关，可作为编制设备功能规范和入网测试的依据。适用范围内设备还应满足最低安全配置要求和推荐采用的安全配置要求。配置要求内容和具体产品自身特征相关，适用于工程验收和运行维护。功能要求是实现配置要求的基础。

安全功能和配置要求项应包括：

——账号管理、认证授权安全功能要求；

——日志安全功能要求；

——IP 协议安全功能要求；

——设备其他安全功能要求，例如依据业主要求进行已知恶意代码和已知漏洞的检测。

适用原则：具体设备的安全要求（功能、配置）应包括适用设备运行的操作系统、数据库和应用程序三个层面的最低要求，并依实际情况，选择部分增强要求。

适用场合：

——设备入网：保证新设备达到功能要求；

——工程验收：保证验收上线的设备符合配置要求；

——日常维护：保证在网设备持续符合配置要求。

7.1.2.2 对于边界防护设备的安全要求

7.1.2.2.1 概述

边界防护设备主要包括网关设备、路由设备、交换设备、防火墙、隔离部件等。健壮性测试和基线检查也适用于边界防护设备。

7.1.2.2.2 网关设备

对网关设备的安全要求见 GB/T 25068.3—2010，可参考 YD/T 1913—2009 、YD/T 2040—2009 和 YD/T 2241—2011 。

7.1.2.2.3 路由设备

对路由设备的安全要求见 GB/T 18018—2007，可参考：

——GB/T 20011—2005；

——YD/T 1358—2005；

——YD/T 1359—2005；

——YD/T 1439—2006；

——YD/T 1440—2006；

——YD/T 1906—2009；

——YD/T 1907—2009。

7.1.2.2.4 交换设备

对交换设备的安全要求可参考：

——GB/T 21050—2007；
——YD/T 1627—2007；
——YD/T 1628—2007。

7.1.2.2.5 防火墙

对防火墙设备的安全要求可参考：
——GB/T 20010—2005；
——GB/T 20281—2006。

7.1.2.2.6 隔离部件

对隔离部件的安全要求可参考：
——GB/T 20277—2006；
——GB/T 20279—2006。

7.2 系统测试

7.2.1 测试条件

测试条件包括：

a) 接入工业控制系统的全部现场设备，包括变送器、执行器、接线箱以及电缆等设备均应按照有关标准进行安装、调试、试运行并验收合格。
b) 工业控制系统的硬件和软件应按照制造厂的说明书和有关标准完成安装和调试，并已投入连续运行。可参考附录 A 中验证硬件结构、数量、尺寸等内容与相关文档的一致性。

7.2.2 系统安全测试

对于系统信息安全的测试主要针对系统能力。具体评估准则见 GB/T 30976.1—2014。不同于信息安全评估，本标准中的系统测试侧重于新增加的安全保障系统对原有系统的影响，以及对之前评估过程中提出的潜在风险和漏洞进行查验。可根据实际情况选择适用的条款进行测试。

管理人员应确保新系统的要求和准则被明确地定义、商定、形成文件并经过测试。在验收之前，需考虑下列项目：

a) 性能和计算机容量要求；
b) 差错恢复和重启规程以及应急计划；
c) 按照已定义标准，准备和测试日常的运行规程；
d) 确定的一组安全控制措施要到位；
e) 有效的人工操作规程；
f) 业务连续性安排；
g) 新系统的安装对现有系统无负面影响的证据；
h) 考虑新系统对用户总体安全影响的证据；
i) 新系统的操作或使用培训；
j) 易用性，这影响到用户使用，避免人员出错。

7.2.3 系统性能测试

加入信息安全保障措施后，应满足原有系统的实时性、可靠性、安全性的要求。可根据具体项目要求，选择相关重要参数，如精确度、响应时间、处理能力等，进行系统性能测试。具体要求和方法见

GB/T 18272.4—2006。

7.2.4 网络连接要求

工业控制系统同公共网络之间的连接，应采取防火墙、单向隔离、DMZ 等措施。企业内部控制网络与信息管理网络之间应采取必要的隔离措施。对于大型系统，宜考虑不同区域之间的隔离措施。

应授权、监视和控制无线网络对系统的访问，其中无线技术包括但不限于 wifi、Zigbee、GPRS/CDMA、蓝牙、微波、卫星。

7.2.5 应急灾备要求

在发生紧急情况下，系统的信息安全应急预案，必要的备机备件等容灾备份措施。

7.3 验收结论

7.3.1 验收文档

工业控制系统信息安全验收文档除准备阶段提供的文档外，还至少应包括下列内容：

a) 信息安全风险分析报告；
b) 测试记录或报告；
c) 验收结论；
d) 系统应急处理方案；
e) 信息安全维护手册；
f) 后续升级指南。

上述文挡除纸质文本外都应有电子文档，且与现场完全一致。

如涉及测试内容，各种测试报告应齐全，并有测试人、验收人签字。

7.3.2 验收结论的编制

7.3.2.1 编制原则

验收结论应依据整个验收过程中对相关要求的符合性做出判定。

7.3.2.2 基本要素

验收结论应包括以下几个方面：

a) 各阶段验收内容及结论(参见附录 A)；
b) 验收不符合项表(参见附录 C)；
c) 不符合内容对系统信息安全能力的影响分析；
d) 是否通过验收的建议。

附 录 A
（资料性附录）
验收检验表

A.1 文件检查

目的：

审查所有相关文件。

编号	查验文件	查验结果	备注
1	功能规划	□P □F □NA	
2	评估报告	□P □F □NA	
3	改进要求	□P □F □NA	
4	验收方案	□P □F □NA	
5	……	□P □F □NA	
注 1：不符合之处记录在不符合项表中，按启动会议确定的协议分类和处理。 注 2：P——合格；F——不合格；NA——不适用。			

签名：

A.2 软硬件检查

目的：

验证硬件结构、数量、尺寸等内容与相关文档的一致性。此外，也应检查软件授权许可、备品备件、耗材等内容。

参考文件：

- 软件手册；
- 经认可的供应商硬件图纸；
- 订货清单。

注：建议相关图纸的副本应由业主和其所聘的检验人员核对并签字确认。

编 号	说 明	查验结果
1	硬件检查	□P □F □NA
2	软件授权许可、版本(包括固件)检查	□P □F □NA
3	备品备件、耗材和工具检查	□P □F □NA

（续）

编　号	说　明	查验结果
4	……	□P　□F　□NA
注 1：不符合之处记录在不符合项表中，按启动会议确定的协议分类和处理。 注 2：P——合格；F——不合格；NA——不适用。		

签名：

A.3　启动测试和系统基本性能测试

目的：

检验系统能够正常启动，并能从典型安全故障中恢复。此外，还应检查系统运行时，其基本性能指标是否是在给定的限制范围内。

参考文件：

- 相关的产品文件；
- 系统基本性能参数限制范围说明。

编　号	说　明	查验结果
1	重新启动（从零点启动、停止/启动）	□P　□F　□NA
2	在线更改	□P　□F　□NA
3	系统负载（内存容量、存储容量等）	□P　□F　□NA
4	报警处理策略	□P　□F　□NA
5	数据流量	□P　□F　□NA
6	……	□P　□F　□NA
注 1：不符合之处记录在不符合项表中，按启动会议确定的协议分类和处理。 注 2：P——合格；F——不合格；NA——不适用。		

签名：

A.4　网络连接检查表

目的：

检查目标工业控制系统中网络连接和访问情况。

基本信息
业务： 位置： 现场技术：　　电话： 现场过程控制：　　电话： 最新更新：
请回答下面的问题：
目前制造和控制系统是应用于网站和企业局域网吗?： 知道和控制系统是从外围的 IACS 访问的吗?： 过程控制领域 可寻址 IP 节点的总数： 从外部过程控制领域访问的可寻址 IP 节点数目： 内部 IACS 领域在线人数： 内部 IACS 领域中有访问外部资源权限的在线人数： 外部 IACS 领域要求有访问过程控制资源的总应用人数： 外部 IACS 领域要求有访问过程控制资源的在线人数： IP 寻址(检查所有应用) DHCP：　　公用应用地址： 静态：　　私人应用地址： 在用网络安全屏障 类型(防火墙,路由器,虚拟墙等)： 支持预期的网络安全(检查所有应用) 网站资源： 外部： 现场网络(回答是/否) 目前网站网络提供最新的拓扑图吗?： 过程控制节点是在封闭的网络区段吗?： 网站信息安全政策是否到位?： 保卫处是否检查完毕?(是的话,日期:)： 网站是否使用认证?： 保卫处的风险评估是否完成?(是的话,日期:)： 远程访问要求(检查所有应用) 通过网站/公司局域网： 通过拨号调制解调器： 通过以太网： 通过本地拨号调制解调器直接联系到制造和控制节点

A.5　风险处置检查表

目的：

审查所有风险是否已处置,尤其是新增加的安全保障系统对原有系统的影响。

参考文件：

- 评估报告；
- 整改的措施和建议。

编号	潜在风险和漏洞	查验结果	备注
1	影响现有控制系统正常运行	□P □F □NA	
2	……	□P □F □NA	
注 1：不符合之处记录在不符合项表中，按启动会议确定的协议分类和处理。 注 2：P——合格；F——不合格；NA——不适用。			

签名：

附 录 B
（资料性附录）
验 收 结 论

基本信息：

业主名称			
工程项目名称		工程项目编号	
被测系统名称			
工厂/装置名称			
验收地点		验收结束日期	

验收结论：

通过 □ 不通过 □

无不合格项 □
有不合格项 □ 详见备注或所附清单
需要重新进行测试 □ 不需要重新进行测试 □
备注：

负责人/签章：

业 主		单 位	
第三方		单 位	
供应商		单 位	

附 录 C
（资料性附录）
验收不符合项表

参与者：

任何未完成的工作或者不符合项都应被记录在验收不符合项表中，并按照如下类型进行分类：

a） 当场整改，然后继续进行验收测试；

b） 在验收过程中同时进行整改；

c） 需再次进行验收；

d） 在验收完成后进行整改。

注：

编 号	说 明	责任方	类 型	是否完成
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

参 考 文 献

[1] GB/T 20010—2005 信息安全技术 包过滤防火墙评估准则

[2] GB/T 20011—2005 信息安全技术 路由器安全评估准则

[3] GB/T 20277—2006 信息安全技术 网络和终端设备隔离部件测试评价方法

[4] GB/T 20279—2006 信息安全技术 网络和终端设备隔离部件安全技术要求

[5] GB/T 20281—2006 信息安全技术 防火墙技术要求和测试评价方法

[6] GB/T 21050—2007 信息安全技术 网络交换机安全技术要求

[7] YD/T 1358—2005 路由器设备安全技术要求——中低端路由器(基于 IPv4)

[8] YD/T 1359—2005 路由器设备安全技术要求——高端路由器(基于 IPv4)

[9] YD/T 1439—2006 路由器设备安全测试方法——高端路由器(基于 IPv4)

[10] YD/T 1440—2006 路由器设备安全测试方法——中低端路由器(基于 IPv4)

[11] YD/T 1627—2007 以太网交换机设备安全技术条件

[12] YD/T 1628—2007 以太网交换机设备安全测试方法

[13] YD/T 1906—2009 IPv6 网络设备安全技术要求——核心路由器

[14] YD/T 1907—2009 IPv6 网络设备安全技术要求——边缘路由器

[15] YD/T 1913—2009 基于软交换的信令网关设备安全技术要求和测试方法

[16] YD/T 2040—2009 基于软交换的媒体网关安全技术要求

[17] YD/T 2241—2011 WAP 网关系统安全防护要求