ICS 25.040
N10

中华人民共和国国家标准

GB/T XXXX.1—XXXX

工业控制系统信息安全
第1部分：评估规范

Industrial control system security part 1: assessment specification

（报批稿）

（本稿完成日期：2013-04-15）

XXXX－XX－XX 发布　　XXXX－XX－XX 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/TXXXX《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/TXXXX 的第 1 部分。

本部分中未做说明的“安全”都是指“信息安全”。

本部分按照GB/T1.1-2009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/TC124）和全国信息安全标准化技术委员会（SAC/TC260）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所、北京和利时系统工程有限公司、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、中国电力科学研究院、清华大学、西门子（中国）有限公司、浙江大学、西南大学、重庆邮电大学、施耐德电气（中国）有限公司、北京钢铁设计研究总院、华中科技大学、北京奥斯汀科技有限公司、罗克韦尔自动化（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、西电捷通无线网络通信股份有限公司、中央办公厅电子科技学院、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、广东航宇卫星科技有限公司、华北电力设计院工程有限公司、华为技术有限公司、三菱电机自动化（中国）有限公司、中标软件有限公司、横河电机（中国）有限公司北京研发中心。

本部分主要起草人：王玉敏、唐一鸿、隋爱芬、罗安、吕冬宝、张建军、薛百华、陈小淙、高昆仑、王雪、冯冬芹、刘枫、王浩、周纯杰、陈小枫、华镕、张莉、宋岩、李琴、夏德海、胡亚楠、王雄、胡伯良、梅恪、刘安正、田雨聪、方亮、马欣欣、张建勋、杨应良、丁露、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、龚明、何佳、杨磊。

工业控制系统信息安全 第1部分：评估规范

1 范围

本部分规定了工业控制系统（SCADA、DCS，PLC，PCS等）信息安全评估的目标、评估的内容、实施过程等。

本部分适用于系统设计方、设备生产商、系统集成商、工程公司、用户、资产所有人以及评估认证机构等对工业控制系统的信息安全进行评估时使用。

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，仅所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 15851-1995 信息技术安全技术带消息恢复的安全技术要求

GB/T 17901 信息技术 安全技术 密钥管理 第 1 部分:框架（GB/ T 17901-1999，idt ISO/IEC 11770-1:1996）

GB/T 17902-1999 信息技术 安全技术 带附录的数字签名

GB/T 18336-2001 信息技术 安全技术 信息技术安全性评估准则

GB/T 19011-2003 质量和(或)环境管理体系审核指南（ISO 19011:2002，IDT）

GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则（ISO/IEC 27002：2005，IDT）

GB/T 28455-2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范

ISO/IEC 9798 信息技术 安全技术 实体鉴别

ISO/IEC 20009-2 信息技术 安全技术 匿名实体鉴别 第2部分 基于群组公钥签名的机制

IEC 62443-3-3 工业过程测量和控制安全-网络和系统安全 第 3-3 系统安全要求和安全保证等级（SAL）

3 术语、定义和缩略语

3.1 术语和定义

3.1.1

脆弱性 vulnerability

系统设计、实现或操作和管理中存在的缺陷或弱点，可被利用来危害系统的完整性或安保策略

3.1.2

识别 identify

对某一评估要素进行标识与辨别的过程。

3.1.3

评估目标 assessment target

评估活动所要达到的最终目的。

3.1.4

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机构，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。

3.1.5

风险处置 risk treatment

选择并且执行措施来更改风险的过程。

3.1.6

残余风险 residual risk
经过风险处置后遗留的风险。

3.1.7

风险接受 risk acceptance
接受风险的决定。

3.1.8

风险分析 risk analysis
系统地使用信息来识别风险来源和估计风险。

3.1.9

风险评估 risk assessment
风险分析和风险评价的整个过程。

3.1.10

风险管理 risk management
指导和控制一个组织机构相关风险的协调活动。

3.1.11

风险处置 risk treatment
选择并且执行措施来更改风险的过程。

3.1.12

工业控制系统 industrial control system（ICS）

对工业生产过程安全（safety）、信息安全(security)和可靠运行产生作用和影响的人员、硬件和软件的集合。

注：系统包括，但不限于：

1) 工业控制系统包括分布式控制系统（DCS）、可编程逻辑控制器（PLC）、智能电子设备（IED）、监视控制与数据采集（SCADA）系统，运动控制（MC）系统、网络电子传感和控制，监视和诊断系统。（在本标准中，不论物理上是分开的还是集成的，过程控制系统（PCS）包括基本过程控制系统和安全仪表系统（SIS））

2)相关的信息系统，例如先进控制或者多变量控制、在线优化器、专用设备监视器、图形界面、过程历史记录、制造执行系统（MES）和企业资源计划（ERP）管理系统。

3)相关的部门、人员、网络或机器接口，为连续的、批处理、离散的和其他过程提供控制、安全和制造操作功能。

3.1.13 安全 safety

免于不可接受的风险。

3.1.14 信息安全 security

a) 保护系统所采取的措施；
b) 由建立和维护保护系统的措施而产生的系统状态；
c) 能够免于非授权访问和非授权或意外的变更、破坏或者损失的系统资源的状态；
d) 基于计算机系统的能力,能够提供充分的把握使非授权人员和系统既无法修改软件及其数据也无法访问系统功能，却保证授权人员和系统不被阻止；
e) 防止对工业自动化和控制系统的非法或有害的入侵，或者干扰其正确和计划的操作。

注：措施可以是与物理信息安全（控制物理访问计算机的资产）或者逻辑信息安全（登录给定系统和应用的能力）相关的控制手段。

3.2 缩略语

CL	Capability level	能力等级
DCS	Distributed Control System	分布式控制系统

ERP	Enterprise Resource Planning	企业资源计划
FR	Foundational requirement	基本要求
HES	Health，enviroment and security	健康、环境和安全
ICS	Industrial control system	工业控制系统
IED	Intelligent Electronic Device	智能电子设备
MES	Manufacturing Execution System	制造执行系统
ML	Management level	管理等级
PCS	Process Control System	过程控制系统
RE	Requirement enhancement	增强要求
SLC	Programmalbe Logic Controller	可编程序控制器
SCADA	Supervisory Control And Data Acquisition	监视控制与数据采集系统
SIS	Safety Instrumented System	安全仪表系统
SL	Security level	信息安全等级
SR	System requirement	系统要求
VPN	Virtual private network	虚拟专用网

4 工业控制系统信息安全概述

4.1 总则

工业控制系统的信息安全特性取决于其设计、管理、健壮性和环境条件等各种因素。系统信息安全的评估应包括在系统生命周期内的设计开发、安装、运行维护、退出使用等各阶段与系统相关的所有活动。必须认识到系统面临的风险在整个生命周期内会发生变化。

评估系统信息安全特性时，应考虑以下各方面：

a) 危险引入点；
b) 危险后果的受体及其影响；
c) 传播途径；
d) 降低风险的措施；
e) 环境条件；
f) 组织机构管理。

注：在系统生命周期的不同阶段，由于某些新危险条件的出现，系统的安全等级会发生变化。

4.2 危险引入点

危险引入点是工业控制系统与非安全设备、系统和网络的接入点。危险源可能来自于工业控制系统系统外部，也可能来自于工业控制系统系统内部。安全威胁通过危险引入点并利用传播途径可能对受体造成伤害。危险引入点归结为以下几类，但不限于：

a) 网络和通信的连接点；

例如：远程技术支持和访问点；无线接入点；调制解调器网络连接；因特网或物联网连接；遥测网络连接；开放的工业控制系统网络连接；与工业控制系统专网互联的其他网络连接；配置不当的防火墙等；

b) 移动媒体；

例如：USB 设备、光盘、移动硬盘等；

c) 不当操作；

例如：恶意攻击、无意误操作等；

d) 受感染的现场设备等。

4.3 传播途径

危险源可能通过传播途径对受体造成伤害。通常，可识别单一的传播途径，但在多数情况下，一个完整的传播途径是由若干单一类型的传播途径组合而成。传播途径一般分为以下几类，但不限于：

a) 外部公共网络，如：因特网；

b) 内部信息网络；

c) 工控专网（点对点、无线）；

d) 移动存储装置。

4.4 危险后果的受体及其影响

危险后果的受体是指受到破坏时所侵害的客体,包括以下三个方面：

a) 人员；

b) 环境；

c) 资产。

对客体造成的侵害的程度归结为三种，分别对应于：

a) 造成特别严重的损害，A 级；

b) 造成严重损害，B 级；

c) 造成一般损害，C 级。

注：表 1 给出了后果造成侵害的级别。

表1 后果造成的侵害等级(上限及现等级的细化、核心数据的损失)

后果									
	风险区域								
	业务连续		信息安全			工业操作安全		环境安全	国家经济影响
级别	一个站点生产中断	多个站点生产中断	直接经济损失(亿元人民币)	刑事责任	社会影响	现场人员	非现场人员	环境	基础设施和服务
A(高)	＞7天	＞1 天	＞30	重罪刑事罪行	品牌形象损失	死亡	死亡或重大社会事件	大面积长期过度的重大损害	影响多个业务部门或扰乱社区服务
B(中)	＞2天	＞1 小时	＞3	轻罪刑事罪行	失去客户的信任	损失工作日或重大伤害	投诉或当地社区的影响	受地方机构通报	在超越一个公司的水平可能影响到业务部门，社区服务
C(低)	＜1天	＜1 小时	<3	无	无	急救	无投诉	可释放的极限	几乎无影响

4.5 工业控制系统信息安全评估的内容概述

4.5.1 组织机构管理评估

组织机构管理通常对构成管理体系的基本要素提出相应的要求和为满足这些要求需要实现或解决哪些方面的内容，而不提供如何去开发管理体系。工业控制系统管理机构（资产所有者）面对具有挑战性的新问题时，应当把信息安全作为一个关键内容融合到整个安全运行体系中。那么常见的工程方法是将问题分解成更小的子问题，按照分治方式解决每个子问题。这是解决ICS信息安全风险的合理途径。然而，在解决信息安全方面常犯的错误是，试图用一套系统一次解决所有的ICS信息安全问题。ICS信息安全是一个更大的挑战，需要考虑整个ICS以及环绕和利用ICS的政策、规程、实践和人员等各个方面。实施这样大范围的管理可能需要组织机构内部的文化变革。

在整个组织机构管理范围的基础上解决ICS信息安全管理是一项艰巨的任务。因为没有适合所有情况的工业控制系统信息安全实践。信息安全实际上是一个风险和成本的平衡。行业不同面对的情况有所不同。在某些情况下，风险可能与健康、安全、环境（HSE）因素有关而不是单纯的经济影响。风险可能带来不可恢复的后果而不仅仅是暂时性的财务损失。

组织机构管理评估基于GB/T 22081-2008标准制定，但是引入一个重要的概念，工业控制系统的信息安全风险对HSE影响，应与现有风险管理实践结合来应对这些风险。具体的评估内容见第5章和附录A。

4.5.2 工业控制系统能力（技术）评估

系统能力（技术）评估目的是保证系统能够在技术上免受攻击。对于一个运行很好的系统，他应该满足操作和安全两个要求。要提前决定的是什么时候开发项目测试以及供应商和集成商对于网络安全设备或系统的要求保证什么级别。对特殊设备或系统的保证的级别将决定系统能力实现的要求。供应商可能推荐测试方法对于特殊的设备和系统，但是用户将需要确定这些技术是否满足安全要求。

理想情况下，将系统所有状态都进行能力评估，以保证每个安全措施能够满足或可以知道其剩余的风险。尽管完整的系统评估理论上是可能的，但是由于财务和人为约束而不能获得大多数的认证。因此，现在面临的问题是决定可接受的风险等级，执行可接受风险的评估。本部分的内容主要见IEC62443-3-3，分别对于于本部分的第6章和附录B。

4.5.3 与其他安全措施的关联

在工业控制系统系统环境下，评估人员应该完全理解企业计算机安全政策、规程、与特定设施和/或工业操作相关的健康、安全、环境风险。应小心确保评估不会干扰由工业控制系统设备提供的控制功能，在评估实施前，可能需要使系统离线。

信息安全、物理安全和功能安全可能是密切相关的。在某些情况下，其他安全措施有可能为信息安全提供独立保护层，而附加的信息安全措施也有可能破坏其他安全措施的完整性。因此，在具体的风险评估活动中，应考虑三者潜在的相互作用及其影响后果。

4.5.4 过程环境制约因素

在评估工业控制系统信息安全特性时，应考虑过程环境条件的制约因素，特别是针对在用工业自化控制系统，应考虑现场测试和引入安全技术措施对正常生产过程的影响。在实施现场测试和引入安全技术措施之前，必须分析下列过程环境条件，以确保行动不会影响正常生产过程。

a) 工业控制系统或其子系统承担的任务；
b) 操作人员的能力；
c) 工业控制系统所连接的工业过程的特性；
d) 附加工具或系统对工业控制正常逻辑的影响；
e) 与工业控制系统连接的公用设施（气、电等）。

4.6 评估结果

4.6.1 风险可接受程度

信息安全采取的管理和技术措施建议采取最小影响的原则。

根据工业控制系统的组织机构管理以及系统（技术）能力评估系统的风险，针对风险产生的结果采用信息安全等级（security level, SL）来表示风险管理过程中的不同风险，这样的结果比较直观，根据SL来确定组织机构的整体安全策略和相应的技术防御措施。同时，组织机构应当综合考虑风险控制成本与风险造成的影响，提出一个可接受的风险范围。对某些资产的风险，如果风险计算值在可接受的范围内，则该风险是可接受的，即残余风险在系统允许风险之内说明系统是健壮的，应保持已经有的安全措施；如果风险评估值在可接受的范围外，但是低于不可接受范围的下限值，则该风险需要采取安全措

施降低、并控制风险到可接受的程度；如果评估的风险从经济，健康，安全和环境方面进行评估后发现风险是不可以接受的，那么就要对现有的系统重新设计信息安全程序。见图1。其中的风险评估的工具和方法参见附录C。

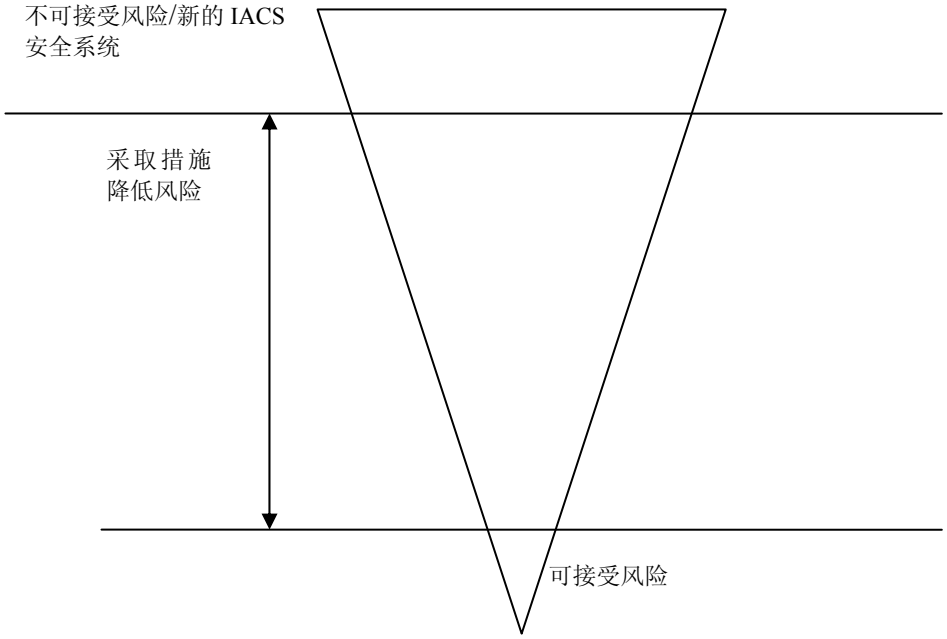

图1　风险可接受的程度

注1：工业控制系统是利用可供选用的各种配置的功能和元件执行要求的任务，系统的该特征难以仅通过评定每一个单独功能和元件的特征来综合评估一个系统的信息安全能力；
注2：工业控制系统信息安全评估的深度在很大程度上取决于系统的复杂程度和边界影响条件以及评估的目的；
注3：评估的范围可以采用汇总统计表的形式，在一个轴线上列出系统的特性另一轴线上列出需考虑的安全影响条件。统计表的方格可用于记录对于每一种系统特性哪一种安全影响条件需要加以考虑。

4.6.2　评估结果等级的划分

评估分为管理评估和系统能力（技术）评估。管理评估宜对照风险接受准则和组织机构相关目标，识别、量化并区分风险的优先次序。风险评估的结果宜指导并确定适当的管理措施及其优先级，评估风险和选择控制措施的过程需要执行多次，以覆盖组织机构的不同部门或各个工业控制系统。

管理评估分为三个级别，分别为管理等级（management level）的 ML1，ML2，ML3，由低到高分别对应低级、中级和高级。具体的评估内容见第 5 章，表格见附录 A。系统能力（技术）评估分为四个级别，由小到大分别对应系统能力等级（capability level）的 CL1，CL2，CL3 和 CL4，具体的评估内容见第 6 章，表格见附录 B。综合管理评估和系统能力评估的结果，得到工业控制系统的评估结果，亦即信息安全等级（SL1，SL2，SL3），见表 2。

表2　工业控制系统的评估结果

系统能力等级 / 信息安全等级 / 管理等级	CL1	CL2	CL3	CL4
ML1	SL1	SL1	SL1	SL1
ML2	SL1	SL2	SL2	SL3
ML3	SL1	SL2	SL3	SL4

(由于文件过大，服务器空间有限， 资料只能展示一部分)

更多资料请联系我司客服，我们将尽最大努力为您服务。