ICS 25.040
N 10

中华人民共和国国家标准

GB/T 33009.1—2016

工业自动化和控制系统网络安全 集散控制系统(DCS) 第1部分:防护要求

Industrial automation and control system security—
Distributed control system(DCS)—Part 1:Protection requirements

2016-10-13 发布　　2017-05-01 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 33009《工业自动化和控制系统网络安全　集散控制系统(DCS)》和GB/T 33008《工业自动化和控制系统网络安全　可编程序控制器(PLC)》等共同构成工业自动化和控制系统网络安全系列标准。

GB/T 33009《工业自动化和控制系统网络安全　集散控制系统(DCS)》分为4个部分：

——第1部分：防护要求；

——第2部分：管理要求；

——第3部分：评估指南；

——第4部分：风险与脆弱性检测要求。

本部分为GB/T 33009的第1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、控制和自动化标准化技术委员会(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：浙江大学、浙江中控研究院有限公司、机械工业仪器仪表综合技术经济研究所、重庆邮电大学、中国科学院沈阳自动化研究所、西南大学、福建工程学院、杭州科技职业技术学院、北京启明星辰信息安全技术有限公司、中国电子技术标准化研究院、国网智能电网研究院、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、清华大学、西门子(中国)有限公司、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、工业和信息化部电子第五研究所、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、北京和利时系统工程有限公司、中国石油天然气管道有限公司、北京匡恩网络科技有限责任公司、西南电力设计院、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、中国电子科技集团公司第三十研究所、深圳万讯自控股份有限公司、横河电机(中国)有限公司北京研发中心。

本部分主要起草人：冯冬芹、施一明、梅恪、王玉敏、王平、王浩、高梦州、徐珊珊、徐皑冬、刘枫、许剑新、陈平、杨悦梅、陈建飞、还约辉、黄家辉、贾驰千、梁耀、陆耿虹、刘大龙、刘文龙、吴彦彪、孟雅辉、范科峰、梁潇、王彦君、张建军、薛百华、许斌、陈小淙、华镕、高昆仑、王雪、周纯杰、张莉、刘杰、朱毅明、王骏、孙静、胡伯良、刘安正、田雨聪、方亮、马欣欣、王勇、杜佳琳、陈日罡、李锐、刘利民、孔勇、黄敏、朱镜灵、张智、张建勋、兰昆、张晋宾、成继勋、尚文利、钟诚、梁猛、陈小枫、卜志军、丁露、李琳、杨应良、杨磊。

工业自动化和控制系统网络安全 集散控制系统(DCS) 第1部分:防护要求

1 范围

GB/T 33009的本部分规定了集散控制系统在运行和维护过程中应具备的安全能力、防护技术要求和安全防护区域的划分,并对过程监控层、现场控制层和现场设备层的防护要点、防护设备以及防护技术提出了具体的要求。

本部分适用于涉及集散控制系统安全防护的电力、石油、化工、水利、冶金、建材等各关键基础设施领域,指导企业用户提高在役运行和新增集散控制系统的安全性,也可作为集散控制系统生产商和集成商的系统安全设计指导。

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 20984—2007 信息安全技术 信息安全风险评估规范

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、定义、缩略语

3.1 术语和定义

GB/T 20984—2007和GB/T 30976.1—2014界定的以及下列术语和定义适用于本文件。为了便于使用,以下重复列出了GB/T 20984—2007和GB/T 30976.1—2014中的一些术语和定义。

3.1.1

可用性 availability

数据或资源能被授权实体按要求访问和使用的特性。

[GB/T 20984—2007,定义3.3]

3.1.2

鉴别 authentication

验证实体所声称的身份的动作。

3.1.3

授权用户 authorized user

依据安全策略可以执行某项操作的用户。

3.1.4

业务战略 business strategy

组织为实现其发展目标而制定的一组规则或要求。

[GB/T 20984—2007,定义3.4]

3.1.5

保密性 confidentiality

数据所具有的特性，即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度。

[GB/T 20984—2007，定义 3.5]

3.1.6

控制系统网络安全 control system security

以保护控制系统的可用性、完整性、保密性为目标，另外也包括实时性、可靠性与稳定性。

3.1.7

人机界面 human machine interface

员工(用户)可以与特定的机器，设备，计算机程序或其他复杂工具(系统)互动的方法集。

注：在很多情况下，这些包含了视频或计算机终端，按钮，听觉反馈，闪烁的灯等。人机界面提供的方法包括：输入(允许用户控制机器)、输出(允许机器通知用户)。

3.1.8

识别 identification

对某一评估要素进行标识与辨别的过程。

[GB/T 30976.1—2014，定义 3.1.2]

3.1.9

网络安全风险 security risk

人为或自然的威胁利用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组织造成的影响。

[GB/T 20984—2007，定义 3.6]

3.1.10

完整性 integrity

保证信息及信息系统不会被非授权更改或破坏的特性。包括数据完整性和系统完整性。

[GB/T 20984—2007，定义 3.10]

3.1.11

制造执行系统 manufacturing execution system

生产规划和跟踪系统，用于分析和报告资源可用性和状态、规划和更新订单、收集详细的执行数据，例如材料使用、人力使用、操作参数、订单和装置状态及其他关键信息。

注 1：此系统访问材料清单、工艺路线和其他来自于基础企业资源规划系统的数据，典型用于实时车间作业报告和监视将活动数据反馈给基础系统的过程。

注 2：更多信息参见 GB/T 20720.1—2006。

3.1.12

组织 organization

由作用不同的个体为实施共同的业务目标而建立的结构。一个单位是一个组织，某个业务部门也可以是一个组织。

[GB/T 20984—2007，定义 3.11]

3.1.13

远程终端装置 remote terminal unit，RTU

集远程数据采集、传输、存储功能于一体的终端设备。

3.1.14

残余风险 residual risk

采取了安全措施后，信息系统仍然可能存在的风险。

[GB/T 20984—2007，定义 3.12]

3.1.15

安全事件 security incident

系统、服务或网络的一种可识别状态的发生，它可能是对安全策略的违反或防护措施的失效，或未预知的不安全状况。

[GB/T 20984—2007，定义 3.14]

3.1.16

网络安全措施 security measure

为保护资产、抵御威胁、减少脆弱性、降低安全事件的影响而实施的各种实践、规程和机制。

3.1.17

网络安全策略 security policy

规范或限定系统或组织如何为保护其资产提供网络安全服务的规则集合。

3.1.18

安全需求 security requirement

为保证组织业务战略的正常运作而在安全措施方面提出的要求。

[GB/T 20984—2007，定义 3.16]

3.1.19

网络安全区 security zone

共享通用网络安全需求的逻辑资产或物理资产的集合。

注 1：本文所用的“区域”是指网络安全区域。

注 2：一个区域与其他区域有明显的边界。一个网络安全区域的网络安全策略在其内部和边缘都要强制执行。一个网络安全区域可以包括多个不同等级的子区域。

3.1.20

敏感性 sensitivity

表征资源价值或重要性的特性，也可能包含这一资源的脆弱性。

3.1.21

威胁 threat

可能导致对系统或组织危害的不希望事故的潜在起因。

[GB/T 20984—2007，定义 3.17]

3.1.22

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。

[GB/T 30976.1—2014，定义 3.1.1]

3.2 缩略语

下列缩略语适用于本文件。

DCS：集散控制系统(Distributed Control System)

MES：制造执行系统(Manufacturing Execution System)

DoS：服务拒绝(Denial of Service)

4 DCS 安全防护概述

4.1 DCS 系统概述

4.1.1 通用 DCS 系统应用的网络结构

通常 DCS 系统应用是一种纵向分层的网络结构，自上到下依次为过程监控层、现场控制层和现场

设备层。各层之间由通信网络连接，层内各装置之间由本级的通信网络进行通信联系，其典型网络结构如图1所示。本部分主要对DCS系统中的过程监控层、现场控制层网络和现场设备层网络的安全要求进行了要求。各层的说明如下：

——过程监控层：以操作监视为主要任务，兼有部分管理功能。这一级是面向操作员和控制系统工程师的，因而这一级配备有技术手段齐备，功能强的计算机系统及各类外部装置，特别是显示器和键盘，以及需要较大存储容量的硬盘或软盘支持，另外还需要功能强的软件支持，确保工程师和操作员对系统进行组态、监视和操作，对生产过程实行高级控制策略、故障诊断、质量评估；

——现场控制层：现场控制层主要功能包括：采集过程数据，进行数据转换与处理；对生产过程进行监测和控制，输出控制信号，实现模拟量和开关量的控制；对I/O卡件进行诊断；与过程监控层等进行数据通信；

——现场设备层：现场设备层的主要功能包括：采集控制信号、执行控制命令，依照控制信号进行设备动作。

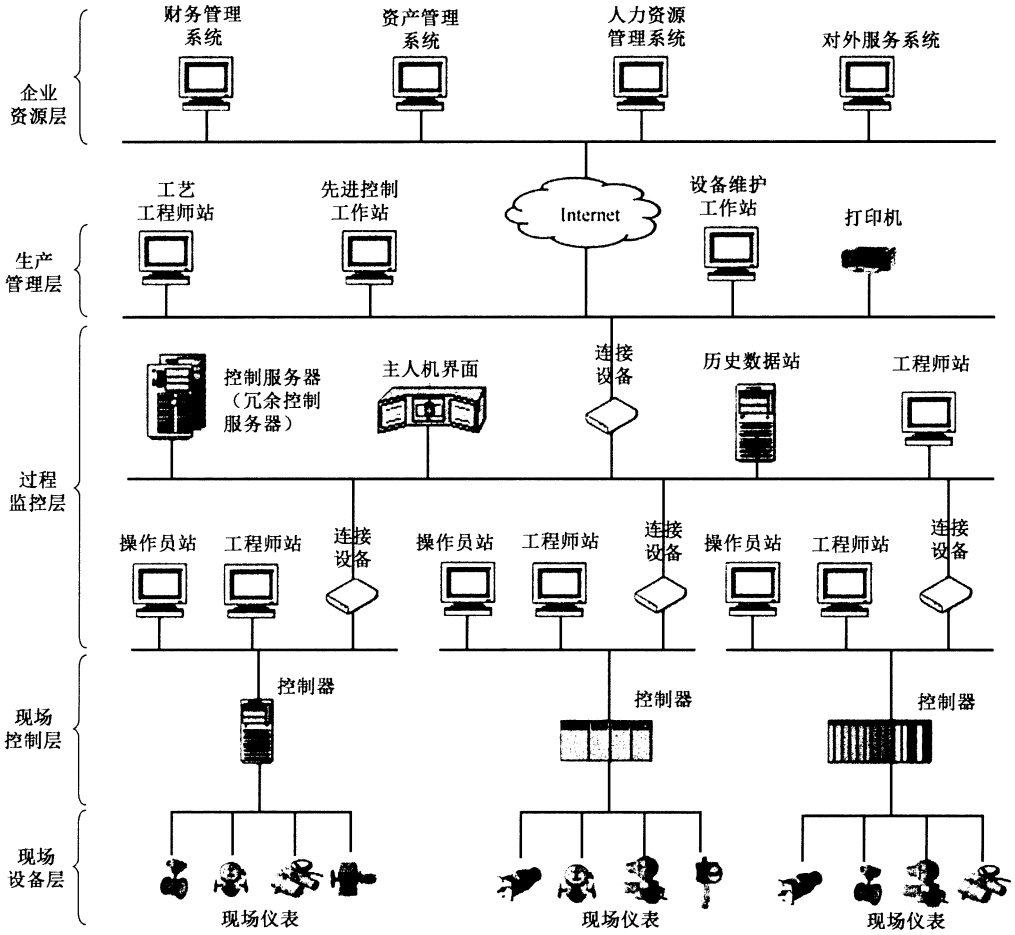

图1 典型DCS系统的网络结构示意图

注：将监控层以下的现场控制层网络进行细分，其中现场控制层网络主要包括DCS控制器和控制器通信模块、I/O模块等，现场设备层网络包括现场智能仪表、执行机构、传感器等现场设备和仪表。

4.1.2 DCS运行安全总体要求

4.1.2.1 实时性要求

DCS应具备实时响应能力，不允许存在不可接受的延迟和抖动。

4.1.2.2 可用性要求

DCS具有高可用性需求，一般不允许重启系统，所以部署前需要详尽的测试，在生产过程中的中断操作需要提前计划。

4.1.2.3 安全性要求

DCS具有安全性要求。DCS一般部署在重要的生产领域，系统不允许出现安全事故。

4.1.2.4 完整性要求

DCS具有完整性要求，不允许未授权用户或者恶意程序对信息和数据的修改。

4.1.2.5 稳定性要求

DCS具有稳定性要求。DCS一旦工作不稳定，将存在严重的威胁，导致大批的不合格产品流出，而且加剧设备的损耗等。

4.1.2.6 高可靠性要求

DCS具有可靠性要求。DCS能够在规定的条件下，长期正常执行其设定的控制功能，期间不允许发生停车，且具有很好的耐久性和可维修性。

4.2 DCS防护总体要求和原则

4.2.1 DCS安全要求

4.2.1.1 概述

DCS系统安全主要包括物理安全和网络安全等。本部分针对DCS系统定义总体要求、基本要求和加强要求等三类安全要求，其中总体要求是针对DCS系统整体的安全性和防护水平提出的安全要求；基本要求和加强要求是针对DCS系统中不同网络层次特点，在本部分的第5章、第6章、第7章和第8章分层进行了定义，其中DCS系统安全性要求不高的企业用户只需满足基本要求，对DCS系统安全要求高的企业用户可以结合企业特点和所用的DCS系统的特点，有选择的部署实现加强要求中的安全要点。加强要求分为常规加强要求和深度加强要求，常规加强要求主要用于普通企业用户，深度加强要求用于具有高安全要求的特殊行业。

4.2.1.2 外部网络隔离要求

DCS用户企业全网拓扑结构可采用分层的方式进行布局，如果DCS系统网络与外部网络（指企业管理层网络、互联网等DCS系统网络以外的其他网络）存在直接或间接互连时，DCS系统网络与外部网之间应使用物理或逻辑隔离技术措施进行防护。

4.2.1.3 网络链路要求

对部署于多地区并通过网络进行互联的DCS系统应用，应保证互联网络链路资源充足，即在企业业务量达最大峰值时，链路数据通信正常且网络延时仍能满足DCS系统应用要求。

对于网络互通性和稳定性要求较高的企业用户，可采取链路冗余技术和手段保证企业网络在网络出现故障时能够维持基本通信，保证在一条链路出现故障时另一条链路能够为企业的正常生产经营活动提供网络保障。

对于网络互通性和稳定性要求非常高的企业用户可采用物理线路冗余的方式部署企业的核心业务

网络、骨干网、核心控制网络，并且冗余线路网络可采用与主网络不同的网络构建方式。

4.2.1.4 数据备份要求

一般 DCS 系统应具有实时数据、OPC 数据、组态数据、控制方案等重要数据的实时备份和定期备份措施；对于数据安全性要求高的 DCS 系统应用，可以采用对系统正常运行的数据进行完整备份的措施，备份周期应不大于 3 个月；对于数据安全性要求非常高的 DCS 系统应用可以建立异地灾难数据备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备。

4.2.2 系统防护原则

在工业控制系统领域，工业控制系统强调的是工业自动化过程及相关设备的智能控制、监测与管理。它们在系统架构、设备操作系统、数据交换协议等方面与普通 IT 信息系统存在较大差异。而且更为关注系统的实时性与业务连续性。也就是说，工业控制系统对系统设备的可用性、实时性、可控性等特性要求很高，在考虑工业控制系统安全时要优先保证系统的可用性；其次，各组件之间存在固有的关联，因此完整性次之；而对于数据保密性来说，则由于工控系统中传输的数据通常是控制命令和采集的原始数据，需要放在特定的背景下分析上下文内容才有意义，而且多是实时数据，所以对保密性的要求较低。除此之外，控制系统还需保证实时性、可靠性和安全性等要求。因此工业控制系统的安全防护手段的部署和实施应结合上述 DCS 特点，遵循下列原则。

本部分以区域划分、纵深防御为基础进行防护，主要手段包括防护软件的部署、防护设备的部署、技术防护以及纵深防御。

a) 防护软件部署原则

防护软件部署主要是指在 DCS 系统的各个单元（如工作站、服务器等设备）上安装安全补丁、病毒防护、入侵监测、入侵防御等具有病毒查杀和阻止入侵行为的软件。

在部署上述防护软件前，应采用线下测试等手段确保其上线后不影响正常的 DCS 运行的可用性、实时性、可靠性和安全性；如果存在影响系统可用性、实时性、可靠性和安全性的较大风险，则撤销对系统造成影响的防护软件的部署。

b) 防护设备部署原则

防护设备部署主要是指在 DCS 系统网络上介入具有防护功能的设备，如防火墙、网闸、安全交换机、入侵检测系统、入侵防御系统等。

在部署防护设备前，应采用线下测试等手段确保其上线后不影响正常的 DCS 运行的可用性、实时性、可靠性和安全性；如果存在影响系统可用性、实时性、可靠性和安全性的较大风险，则撤销对系统造成影响的防护设备的部署。

c) 技术防护原则

技术防护主要是指以技术的手段进行 DCS 安全防护，如访问控制、边界管理、管道通信等。在防护技术应用前，应采用线下测试等手段在相同的 DCS 系统上进行严格的系统测试，确保其上线后不影响正常的 DCS 运行的可用性、实时性、可靠性和安全性；如果存在影响系统可用性、实时性、可靠性和安全性的较大风险，则撤销对系统造成影响的防护技术的使用。

d) 纵深防御原则

单一的安全产品、技术或者解决方案无法有效保护 DCS，所以需要一种包含两个或者多个不同机制的多层防护策略。本部分采用的纵深防御架构策略包含了防火墙的使用，安全分区的建立，有效的安全策略下的入侵检测能力，培训计划和应急响应机制。进行纵深防御架构的有效部署和实施，需要对 DCS 可能遭受的下列攻击和安全风险有全面的掌握，包括：

1) 网络边界的后门和漏洞；

2) 常见协议的漏洞；

3） 针对现场设备的攻击；
4） 针对数据库的攻击；
5） 通信劫持和“中间人”攻击。

在纵深防御技术各项设备或技术应用 DCS 前，应采用线下测试等手段确保其上线后不影响正常的 DCS 运行的可用性、实时性、可靠性和安全性；如果存在影响系统可用性、实时性、可靠性和安全性的较大风险，则撤销对系统造成影响的防护技术的使用。

5 物理访问控制要求

物理访问控制基本要求包括：

a） 机房（包括电子设备间）出入口应安排专人值守，控制、鉴别和记录进入的人员；
b） 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；
c） 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在进入重要区域前设置交付或安装等过渡区域；
d） 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

6 过程监控层网络安全

6.1 区域划分

6.1.1 基本要求

应根据过程监控层网络中各系统的安全等级划分成不同的安全区域，并按照方便管理和控制为原则为各安全功能区域分配网段地址。过程监控层各网段应相互隔离，原则上不直接连接在一起。

6.1.2 常规加强要求

6.1.2.1 加强要求

本项要求包括但不仅限于：

a） 重要设备不直接与外层网络相连
   1） 应在工程师站、操作员站与 MES 层网络间采用数据隔离措施。
   2） 不宜将工程师站与操作员站放置在同一物理区域内。
b） OPC 等其他数据服务器安全
   1） 不宜将不同安全等级的服务器软件安装在同一台主机上；如果需要安装在同一台主机上，需要考虑安全措施。
   2） 各个控制系统网段的服务器不宜直接连接在同一个网络上。
   3） 应在服务器与实时数据库通信处部署隔离设备。

6.1.2.2 深度加强要求

不要求。

6.2 访问与使用控制

6.2.1 基本要求

本项要求包括但不仅限于：

a) 应在过程监控层与上层网络边界部署访问控制设备，启用访问控制功能，设定访问控制策略，对从上层发起的访问进行源地址、目的地址、源端口、目的端口和协议等项目的检查，以允许/拒绝数据包的出入；

b) 提供账户分配管理功能，能够新建、添加、删除、修改账户信息的功能；

c) 应在会话处于非活跃时间或会话结束后终止会话，终止链接动作可以由被请求数据的设备或程序执行，也可以由防护设备执行。

6.2.2 加强要求

6.2.2.1 常规加强要求

本项要求包括但不仅限于：

a) 逻辑安全隔离

在过程监控层与上层网络通信处部署隔离设备或采用其他隔离技术手段，保证两个层次网络间的逻辑隔离。

b) 用户权限安全

应对多用户共同操作的主机进行用户权限划分，根据用户的工作职责分配相应的访问权限，授予用户所需的最小权限；并实现操作系统和数据库系统特权用户的权限分离。

c) 移动代码限制

对可能对系统造成破坏的移动代码技术（如 Java、VB script 等）的使用提供限制功能，包括防止移动代码的执行、对移动代码的源进行身份认证、限制移动代码与控制系统通信、监控移动代码的使用、对移动代码的完整性进行检查等。

6.2.2.2 深度加强要求

本项要求包括但不仅限于：

a) 物理安全隔离

在过程监控层与上层网络通信处部署隔离设备或采用其他隔离技术手段，保证两个层次网络间的物理隔离。

b) 应用协议检查

应对进出网络的协议数据内容进行过滤，实现对 HTTP、FTP、TELNET、SMTP、POP3 等通用协议以及其他工业协议的命令级控制，以允许/拒绝数据包的出入。

c) 敏感信息访问控制

应对工程师站、操作员站、OPC 服务器、实时数据库服务器等重要设备内的重要信息资源（如系统组态信息、控制程序、实时数据库用户及密码表项、OPC 服务器数据文件）设置敏感标记；应依据安全策略严格控制用户对有敏感标记重要信息资源的操作，如对组态信息、控制程序、实时数据库表项、OPC 服务器数据等文件的访问和修改操作进行监管，严格控制访问权限。

d) 基于角色的授权

应对用户组态软件、系统组态软件、图形化编辑软件、语言编程软件、流程图制作软件、实时监控软件、数据服务软件、数据通信软件、报警记录软件、趋势记录软件、OPC 数据通信软件、OPC 服务器软件、历史数据传输软件、网络文件传输软件等工控应用软件中的所有角色提供授权执行功能。

6.3 入侵防御

6.3.1 基本要求

宜在过程监控层与上层网络间部署入侵防护设备，能够监视边界处的常见网络攻击行为（包括端口

扫描攻击、强力攻击、木马后门攻击、DoS 攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫等），并能够在检测到攻击行为时实时记录攻击源 IP、攻击类型、攻击目标、攻击时间，并提供报警。

6.3.2 加强要求

6.3.2.1 常规加强要求

本项要求包括但不仅限于：

a） 系统最小化安装

工程师站、操作员站、OPC 服务器、实时数据库服务器、监控计算机等主机设备操作系统采用最小化系统安装原则，只安装与自身业务相关的操作系统组件及应用软件。

b） 重要系统病毒防护

在工程师站、操作员站、OPC 服务器、实时数据库服务器、监控计算机等重要系统部署经过验证的防病毒软件，病毒库和补丁的更新需在线下模拟系统中进行严格的验证，在不影响系统可用性、实时性和稳定性的前提下实施更新。

c） 移动存储接口管理

应对工程师站、操作员站、OPC 服务器、实时数据库服务器、监控计算机等系统的物理接口进行限制，禁止 USB 接口或使用 USB 端口设备绑定；部署文件拷贝中转设备，对通过存储介质中转的数据进行病毒和木马的查杀。

6.3.2.2 深度加强要求

本项要求包括但不仅限于：

a） 边界完整性监测

应能够对非授权设备私自连接到过程监控层网络的行为和内部网络用户私自连接到外部其他层次网络的行为进行检查，并对非法接入部位进行准确定位，进行有效隔离和阻断。

b） 系统完整性保护

应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式、长度符合系统要求；能够对组态软件（包括用户组态软件、系统组态软件、图形化编辑软件、语言编程软件、流程图制作软件等）和监控软件（包括实时监控软件、数据服务软件、数据通信软件、报警记录软件、趋势记录软件、OPC 数据通信软件、OPC 服务器软件、历史数据传输软件、网络文件传输软件等）的完整性进行检查，并在检测到完整性受到破坏后具有恢复的措施。

6.4 身份鉴别与认证

6.4.1 基本要求

本项要求包括但不仅限于：

a） 应对工程师站、操作员站、OPC 服务器、实时数据库服务器、监控计算机等所有设备提供用户身份登录认证功能，并提供用户身份信息修改、添加、删除等操作功能；

b） 应提供用户身份认证反馈功能，对身份认证结果向用户反馈；

c） 限制默认账户的访问权限，重命名系统默认账户，修改默认口令，禁止在工程师站、操作员站、OPC 服务器和实时数据库服务器使用默认账户；

d） 应及时删除多余的、过期的账户，避免共享账户的存在。

6.4.2 加强要求

6.4.2.1 常规加强要求

本项要求包括但不仅限于：

a) 密码强度

身份鉴别信息应不易被冒用，口令应有复杂度要求并定期更换。

b) 管理员地址限定

应对网络设备的管理员登录地址进行限制。

c) 登录失败处理

应具有用户登录失败处理功能，可采取结束会话、限制非法登录的次数、自动退出和当网络登录连接超时自动退出等措施。

6.4.2.2 深度加强要求

对重要系统（如历史数据库服务器等）应提供两种或两种以上的鉴别技术来进行身份鉴定，其中至少有一种身份鉴别信息是不易伪造的。

6.5 安全审计

6.5.1 基本要求

应对过程监控层网络中的网络设备运行状况、网络流量等进行审计，审计记录应包括日期和时间、类型、主体标识、客体标识等。

6.5.2 加强要求

6.5.2.1 常规加强要求

应对审计记录进行保护，严格控制审计记录的访问权限，降低被非法篡改的风险。

6.5.2.2 深度加强要求

本项要求包括但不仅限于：

a) 加强审计

应对工程师站、操作员站、OPC 服务器、实时数据库服务器等重要系统的操作系统用户、数据库用户和控制应用软件（用户组态软件、系统组态软件、图形化编辑软件、语言编程软件、流程图制作软件、实时监控软件、数据服务软件、数据通信软件、报警记录软件、趋势记录软件、OPC 数据通信软件、OPC 服务器软件、历史数据传输软件、网络文件传输软件等）的运行事件（包括用户登录事件、组态事件、编程事件、程序下载/上传事件、控制操控事件、系统进程事件、客户端请求事件、数据传输事件、OPC 服务器进程事件）、系统资源的异常使用和重要系统命令的使用等进行安全审计，并能生成审计报表进行分析。

b) 集中审计

应根据系统的统一安全策略，实现集中审计，并与时钟服务器同步。

6.6 资源控制

6.6.1 基本要求

应能够监视过程监控层网络与上层网络接口处的网络流量、连接数等网络资源信息，定义整体网络最大资源使用限定阈值，整体网络使用的资源超过此阈值时终止用户或网络的资源占用行为。

6.6.2 加强要求

6.6.2.1 常规加强要求

本项要求包括但不仅限于：

a) 网络资源控制

应通过设定终端接入方式、网络地址范围等条件限制终端登录，并根据安全策略设置登录终端的操作超时锁定。

b) 角色资源控制

应根据控制应用软件(包括用户组态软件、系统组态软件、图形化编辑软件、语言编程软件、流程图制作软件、实时监控软件、数据服务软件、数据通信软件、报警记录软件、趋势记录软件、OPC 数据通信软件、OPC 服务器软件、历史数据传输软件、网络文件传输软件等)用户的角色进行资源访问的限制，防止角色之间的交叉访问。

6.6.2.2 深度加强要求

本项要求包括但不仅限于：

a) 用户资源控制

应限制单个用户对系统资源的最大或最小使用限度，对单个账户的多重并发会话进行限制。

b) 主机资源控制

应对工程师站、操作员站、OPC 服务器、实时数据库服务器等重要系统进行监视，包括监视服务器的 CPU、硬盘、内存等资源的使用情况；对用户组态软件、系统组态软件、图形化编辑软件、语言编程软件、流程图制作软件、实时监控软件、数据服务软件、数据通信软件、报警记录软件、趋势记录软件、OPC 数据通信软件、OPC 服务器软件、历史数据传输软件、网络文件传输软件等软件进程占用的资源进行监视，分配最大限额和最小限额。

6.7 数据安全

6.7.1 常规加强要求

本项要求包括但不仅限于：

a) 必要信息保护

应能够检测过程监控层网络内所有的系统管理数据、控制指令数据、上传/下载程序数据、监控数据等在存储过程中是否受到破坏，并在检测到破坏时及时采取必要的恢复措施。

b) 剩余信息保护

1) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是内存中。
2) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。
3) 应保证工程组态文件、系统组态文件、控制程序文件等资源所在的存储空间在重新分配给其他用户前得到完全清除。

6.7.2 深度加强要求

本项要求包括但不仅限于：

a) 数据保密

应能够采用加密技术或其他有效的技术手段实现系统管理数据、现场实时数据、控制指令数据、上传/下载程序数据、监控数据在传输和存储过程中的保密性。

b) 数据备份及恢复

应对实时数据库服务器、OPC 数据库服务器、组态数据库服务器、历史数据库服务器等重要服务器设备进行硬件冗余。启用实时数据备份功能，保证当主服务器出现故障时冗余设备可以切换并恢复

数据。

c) 私有通信

应能够对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通信协议的攻击破坏数据的完整性。

7 现场控制层网络安全

7.1 区域划分

7.1.1 基本要求

应根据现场控制层的安全等级进行安全区域划分，并按照方便管理和控制为原则为各安全功能区域分配网段地址。

7.1.2 加强要求

7.1.2.1 常规加强要求

不宜将不同控制系统的数据服务器软件安装在同一台主机上；各个控制系统网段的数据服务器不宜直接连接在同一个网络上；应在数据服务器与实时数据库通信处部署隔离设备。现场控制层各网段相互隔离，原则上不直接连接在一起。

7.1.2.2 深度加强要求

不要求。

7.2 访问与使用控制

7.2.1 基本要求

应在现场控制层网络与过程监控层网络间具有访问控制措施，对从过程监控层发起的访问进行源地址、目的地址、源端口、目的端口和协议等项目的控制。

7.2.2 加强要求

7.2.2.1 常规加强要求

对于安全接入，应对接入现场控制层的设备进行身份认证，拒绝未经认证的设备访问网络；现场控制层网对于已使用的无线网络连接，应至少启用 MAC 地址过滤白名单功能。

应提供针对工程师站、操作员站、OPC 服务器、实时数据库服务器等用户发送的操作行为的授权验证功能，如读写数据、下载程序、用户组态、设备操控命令、设置配置等行为。

7.2.2.2 深度加强要求

本项要求包括但不仅限于：

a) 安全连接

在现场控制层和过程监控层网络的边界增加安全连接控制功能，无线网络连接，应启用 MAC 地址绑定功能。

在现场控制层内的安全区域间增加安全连接控制功能，建立区域安全访问路径，对各安全区域之间的访问进行连接控制。

b) 应用协议检查

应对进出网络的信息内容进行过滤，实现对应用层协议的命令级（包括数据上传服务、数据下载服务、读服务、写服务、控制指令执行服务等）的检查，对非法数据包的出入进行报警。

c） 敏感信息访问控制

应对 DCS 控制器内的配置信息、控制程序、数据块等重要信息资源设置敏感标记，并依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

d） 移动代码限制

对可能对系统造成破坏的移动代码技术（如 Java、VB script 等）的使用提供限制功能，包括防止移动代码的执行、对移动代码的源进行身份认证、限制移动代码与控制系统通信、监控移动代码的使用、对移动代码的完整性进行检查等。

e） 敏感文件使用限制

应对控制器内组态文件、控制程序代码、实时数据等关键敏感文件的访问进行限制。

7.3 入侵防御

7.3.1 常规加强要求

本项要求包括但不仅限于：

a） 控制器软件容错

控制器软件（如嵌入式软件）应提供数据有效性检验功能，对通过通信接口输入的数据格式、长度，功能码等进行实时检查，保证其符合系统要求，当控制器出现故障后能够自动保存当前所有状态，并采取恢复措施。

b） 通信检测

应能够对总线上的网络流量及网络负载进行监测，对现场控制层设备接入网络具有识别能力。

7.3.2 深度加强要求

本项要求包括但不仅限于：

a） 总线恶意服务指令识别与阻断

应在控制器入口端部署控制器防护功能和设备，能够识别针对控制器的操控服务指令（包括组态服务、数据上传服务、数据下载服务、读服务、写服务、控制程序下载服务、操控指令服务等），并能够根据安全策略要求对非法的服务请求进行报警。能在必要时断开非认证设备的连接。

b） 入侵监测

应在现场控制层与过程监控层间旁路部署入侵检测设备，能够监视边界处的常见网络行为（包括端口扫描攻击、暴露攻击、木马后门攻击、DoS 攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫等），并能够在检测到攻击行为时实时记录攻击源 IP、攻击类型、攻击目标、攻击时间，并提供报警。

7.4 身份鉴别与认证

7.4.1 常规加强要求

应对工程师站、操作员站、OPC 服务器、实时数据库服务器的网络地址进行限制，现场控制层网络可以根据网络标识对服务请求的发送方进行识别。

7.4.2 深度加强要求

采用身份标识手段，能够对工程师站、操作员站、OPC 服务器和实时数据库服务器发送的服务操作指令（包括数据读服务、数据写服务、程序上传服务、程序下载服务、开关控制指令等）发送方的角色身份进行验证和鉴别。

7.5 安全审计

7.5.1 常规加强要求

应对现场控制层网络中关键系统(如:控制核心生产工艺的系统)的网络设备运行状况、网络流量等进行审计,审计记录应包括日期和时间、用户、事件类型等。

7.5.2 深度加强要求

本项要求包括但不仅限于:

a) 审计记录保护

应对审计记录进行保护,应保证无法单独中断审计进程,无法删除、修改和覆盖审计记录。

b) 加强审计

应对嵌入式控制器内的修改事件(包括配置修改事件、算法修改事件、控制程序修改事件、关键变量修改事件等)和控制器服务事件(包括组态服务、数据块下载服务、程序下载服务、写服务等)进行安全审计,并生成审计报表进行分析。

c) 集中审计

应根据系统的统一安全策略,实现集中审计,注意审计任务时钟保持与系统主时钟同步。

7.6 资源控制

7.6.1 基本要求

应能够监视现场控制层网络与过程监控层网络接口处的网络流量、连接数等网络资源信息,并根据安全策略要求对流量、连接数进行限制。

7.6.2 加强要求

本项要求包括但不仅限于:

a) 网络资源控制

应通过设定设备接入方式、网络地址范围等条件限制设备接入网络。

b) 嵌入式控制器资源控制

应对嵌入式控制器的运行状态进行监控,包括系统的 CPU、内存、堆栈等,对存储于内存中的配置信息、控制程序、数据进行监控,限制对关键控制系统数据(包括控制程序代码、组态配置信息等)的访问。

7.7 数据安全

7.7.1 基本要求

应能够检测现场控制层网络内所有的用户组态数据、上传/下载程序数据等在传输过程中完整性是否受到破坏。

7.7.2 加强要求

7.7.2.1 常规加强要求

数据传输完整性:应保证数据在现场控制层传输过程中的完整性,包括防止数据包被插入、防止数据包被删除、防止数据包被超期延迟、防止数据包被重排序和重放。

7.7.2.2 深度加强要求

本项要求包括但不仅限于：

a) 控制器存储数据完整性

应保证存储于嵌入式控制系统内的数据完整性，包括静态数据保护、关闭无用端口、写保护、可执行代码保护、应用程序配置保护、应用程序语法检查、操作系统配置保护、可执行代码注入保护等。

b) 控制系统实时数据完整性

应能够检测现场控制层网络内所有的现场实时数据、控制指令数据、监控数据等在传输过程中完整性是否受到破坏。应具备利用密码技术或其他同等功效的技术检测数据包被修改的能力。

c) 点对点通信加密

应保证在点对点通信的过程中，会话的建立有相应的身份认证机制、会话过程中应提供加密机制或其他等效技术手段保证会话不会被窃听、在会话目的达到后及时关闭会话、在会话超时时提供会话超时响应功能，如可关闭会话也可重新进行会话认证。

8 现场设备层网络安全

8.1 区域划分

8.1.1 常规加强要求

应根据现场设备层的安全等级进行安全区域划分，并按照方便管理和控制为原则为各安全区域分配网络地址。

8.1.2 深度加强要求

应限制将不同安全等级的控制装置和现场设备连接到同一个安全区域内的现场总线网络。

8.2 访问与使用控制

8.2.1 常规加强要求

应在各安全区域之间部署安全网关设备，建立各区域之间的网关路径，保证各子区域之间访问的相对独立性。

应对危险区域、关键装置中的执行机构(压力执行机构、温度执行机构等)的操作行为进行限制，对装置的手动操作区域应采用物理防护措施进行防护，但不应影响紧急操作。

8.2.2 深度加强要求

应在现场控制层与现场设备层网络的边界部署访问控制设备，设定访问控制策略。对从现场控制层发起的访问，进行现场总线协议和服务功能等项目的检查，以允许/拒绝数据包的出入。

应提供对控制器发送操控指令的操作行为进行授权验证的功能，如开关操作、电磁阀操作等。

8.3 入侵防御

8.3.1 常规加强要求

a) 智能仪表软件检测

智能仪表嵌入式软件应对输入数据提供有效性检验功能，保证通过通信接口输入的数据格式、长度符合系统要求，当出现异常情况时能够提供异常处理功能。

b） 总线负载检测

应能够对现场总线上的网络流量及网络负载数量进行监测，当发现网络负载异常时能够提供报警信息。

8.3.2 深度加强要求

本项要求包括但不仅限于：

a） 控制指令识别

应能够对关键装置、关键执行机构（压力控制机构、温度控制机构、流量控制机构等）的控制指令进行识别。

b） 恶意指令防护

应在现场设备层与现场控制层网络的边界部署安全防护设备，并能够监视过滤网络中的恶意控制指令行为，根据安全策略对恶意指令进行阻断。

8.4 身份鉴别与认证

8.4.1 常规加强要求

能够对发送操作数据和指令的现场设备进行身份识别。

8.4.2 深度加强要求

不要求。

8.5 安全审计

8.5.1 常规加强要求

宜对现场设备层网络中的现场总线运行状况、网络流量等进行审计，审计记录应包括日期和时间、控制器、事件类型等。

8.5.2 深度加强要求

应对审计记录进行保护，应保证无法单独中断审计进程，无法删除、修改和覆盖审计记录。

8.6 数据安全

8.6.1 常规加强要求

应采用监测或管理手段保证现场设备层网络内所有的现场实时数据、控制指令数据、监控数据等在传输过程中完整性不受到破坏，如果数据被破坏能够及时发现。

8.6.2 深度加强要求

应保证数据在现场设备层传输过程中的完整性，包括防止数据被插入、防止数据被删除、防止数据被超期延迟、防止数据被重排序和重放；应具备利用密码技术或其他同等功效的技术检测数据被修改的能力。

参 考 文 献

[1] GB/T 20270—2006 信息安全技术 网络基础安全技术要求

[2] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

[3] GB/T 22240—2008 信息安全技术 信息系统安全保护等级定级指南

[4] IEC/TS 62443-1 Terminology, concepts and models

[5] IEC/TR 62443-2 Establishing an industrial automation and control system security program

[6] IEC/TR 62443-3 Operating a manufacturing and control systems security program

[7] IEC/TR 62443-4 Specific security requirements for manufacturing and control systems

[8] IEC 62443-5 Security technologies for industrial automation and control systems

[9] NIST SP 800-41—2009 Guidelines on Firewalls and Firewall Policy

[10] NIST SP 800-82—2011 Guide to Industrial Control Systems (ICS) Security