ICS 25.040
N 10

中华人民共和国国家标准

GB/T 33009.2—2016

工业自动化和控制系统网络安全 集散控制系统(DCS) 第2部分:管理要求

**Industrial automation and control system security—
Distributed control system(DCS)—
Part 2:Management 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 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义、缩略语 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 3
4　DCS 安全管理概述 …… 3
4.1　DCS 系统概述 …… 3
4.2　DCS 网络安全管理体系 …… 5
5　DCS 安全管理要素 …… 8
5.1　方针、策略与规程 …… 8
5.2　管理机构 …… 8
5.3　资产管理 …… 9
5.4　人员 …… 10
5.5　密码学 …… 10
5.6　物理和环境 …… 10
5.7　安全控制措施 …… 11
5.8　通信安全 …… 15
5.9　系统运营与维护 …… 15
5.10　供应商关系 …… 16
5.11　信息与文件管理 …… 17
5.12　业务连续性规划 …… 17
5.13　安全事件规划与响应 …… 18
5.14　符合性 …… 18
参考文献 …… 20

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、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：浙江中控研究院有限公司、浙江大学、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：施一明、冯冬芹、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、王芳、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、王弢、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2部分:管理要求

1 范围

GB/T 33009的本部分规定了集散控制系统网络安全管理体系及其相关安全管理要素的具体要求。

本部分适用于集散控制系统运行、维护过程中的安全管理。

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 22080—2008 信息技术 安全技术 信息安全管理体系 要求

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

ISO/IEC 27002:2013 信息技术 安全技术 信息安全控制实用规则(Information technology—Security techniques—Code of practice for information security controls)

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

用于验证用户所声称的身份。

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

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]

3.1.5

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。

3.1.6

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)。

3.1.7

识别 identify

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]

3.1.8

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]

3.1.9

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]

3.1.10

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：更多的信息参见 GB/T 20720.1—2006。

3.1.11

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]

3.1.12

残余风险 residual risk

采取了安全措施后，系统仍然可能存在的风险。

[GB/T 20984—2007，定义 3.12]

3.1.13

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]

3.1.14

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]

3.1.15

威胁 threat

可能导致对系统或组织危害的不希望事故潜在起因。

[GB/T 20984—2007,定义 3.17]

3.1.16

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]

3.1.17

资产 asset

对组织有价值的任何事物。

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)

DoS:服务拒绝(Denial of Service)

HSE:健康、安全和环境管理体系(Health Safety and Enviroment Management System)

SMS:网络安全管理系统(Security Management System)

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

PSM:工艺安全管理(Process Safety Management)

4 DCS 安全管理概述

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:现场控制层的主要功能包括: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。

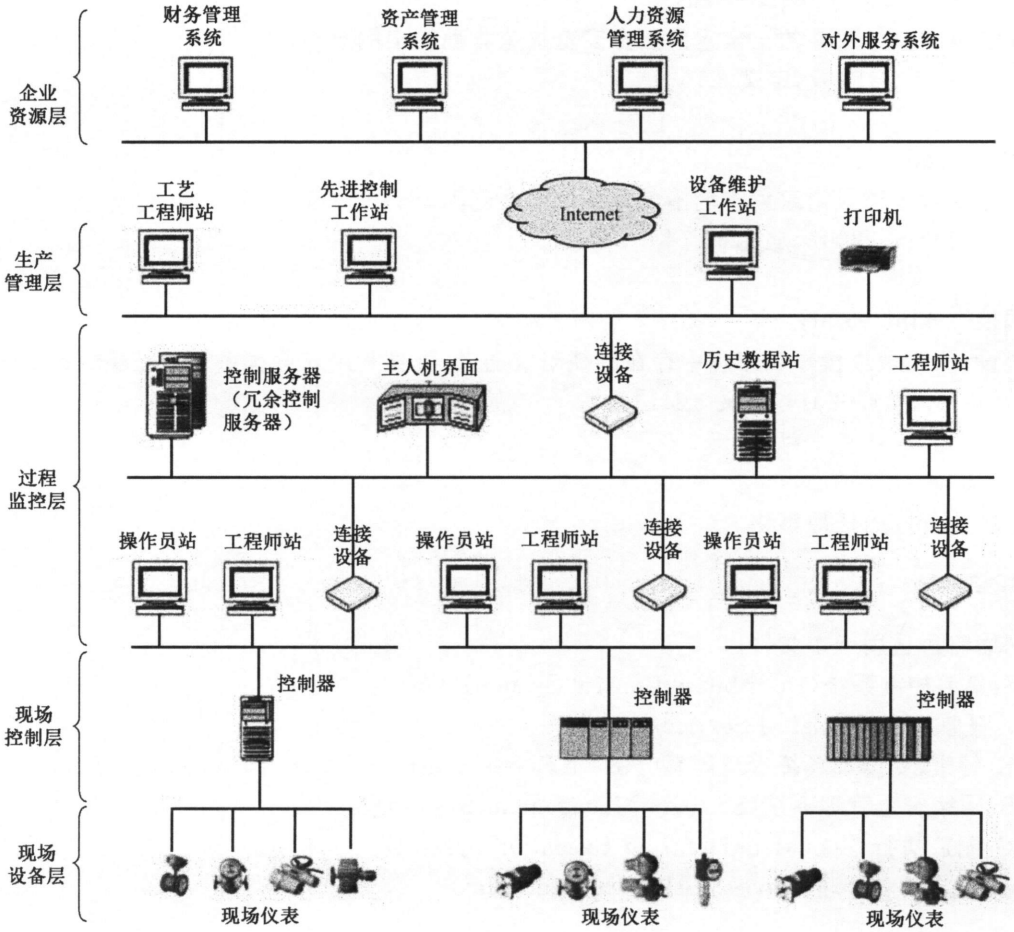

图 1　典型 DCS 系统应用的网络结构示意图

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网络安全管理体系

4.2.1 总要求

DCS网络安全管理的核心是网络安全管理体系的建立、维护和改进过程，宜按照GB/T 22080—2008建立相应的组织管理体系。本部分旨在指导DCS系统相关企业理解DCS网络安全管理体系的建立和运行过程。在第5章定义了DCS网络安全管理体系建立和运行过程中必要的管理要素和具体要求，用户应结合具体DCS应用实际情况选择执行。

DCS网络安全管理体系(Information Security Management System)旨在指导企业或组织在已有网络安全管理体系的框架或环境下，建立、实施、运行、监视、评审、保持与改进文件化的DCS网络安全管理体系(ISMS)。DCS网络安全管理体系应综合考虑资产重要性、资产地理位置、系统功能、控制对象和生产厂商等因素，将控制系统进行分区域管理。

本部分采用过程方法规定了文件化的ISMS的建立、实施、运行、监视、评审、保持和改进过程中的安全要求。DCS用户和DCS设备生产企业和系统集成企业应成立相关的组织承担相应的网络安全管理职责。

本部分提出的用于DCS网络安全管理的过程方法强调以下方面的重要性：

a) 分析理解企业或组织自身的工控网络安全需求和建立工控网络安全方针与目标；

b) 从整体业务风险的角度，实施和运行控制措施，管理DCS网络安全风险；

c) 监视和评审ISMS执行情况的有效性；

d) 基于客观测量的ISMS持续改进。

本部分采用“规划(Plan)-实施(Do)-检查(Check)-处置(Act)”(PDCA)模型来建立DCS系统的ISMS过程，如图2所示。

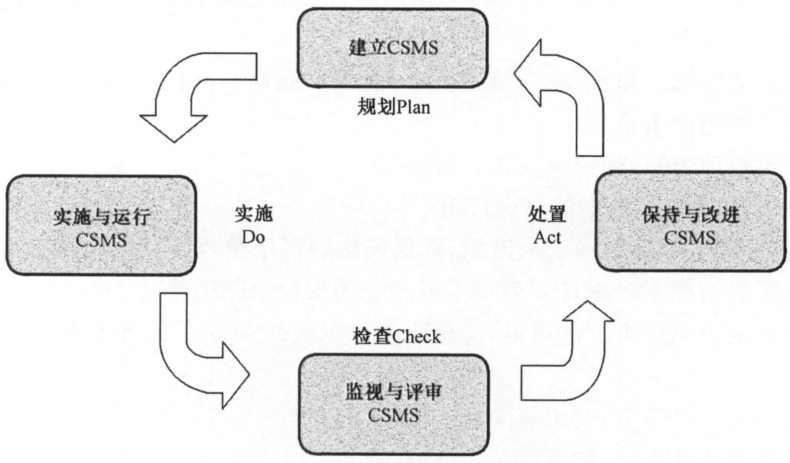

图2 应用于ISMS过程的PDCA模型

4.2.2 建立 DCS 的 ISMS

建立与管理 DCS 安全风险和改进 DCS 网络安全有关的方针、目标、过程和规程，提供与组织或企业总方针和总目标相一致的结果。应做以下几方面工作：

a) 根据 DCS 业务、组织机构、物理场所、价值资产和技术手段等方面的特性，确定 DCS 的 ISMS 的范围和边界；

b) 根据 DCS 业务、组织机构、物理场所、价值资产和技术手段等方面的特性，确立 DCS 的 ISMS 方针。DCS 的 ISMS 方针应：

1) 包括设定 DCS 网络安全目标的框架和建立 DCS 网络安全工作的总方向和原则；

2) 考虑 DCS 业务和相关法律法规的要求，及合同中的安全义务；

3) 在组织或企业的战略性风险管理环境下，设定 DCS 风险管理框架，建立和保持 DCS 的 ISMS；

4) 建立风险评价的准则，确定可接受风险的范围；

5) 获得组织或企业管理者的批准和支持。

c) 确定 DCS 的风险评估方法：

1) 选择适合 DCS 的 ISMS、已识别的业务网络安全和法律法规要求的风险评估方法，基于 DCS 资产的安全威胁、脆弱性以及影响后果来识别与分级风险；

2) 建立一套指标体系，用于 DCS 各业务流程与子系统在风险处理上的分级排序；制定接受风险的准则，识别可接受的风险级别。

选择的风险评估方法应确保风险评估产生可比较的、可再现的结果。

d) 识别 DCS 风险：

1) 创建 DCS 网络拓扑图，收集 DCS 资产信息，识别 ISMS 范围内的资产及其负责人；

注：负责人标识了已经获得管理者的批准，负责产生、开发、维护、使用和保证资产的安全的个人和实体，并非资产拥有者。

2) 识别 DCS 资产可能面临的威胁及威胁发生的可能性；

3) 识别 DCS 控制功能单元和工艺环节可能被威胁利用的脆弱点；

4) 识别丧失 DCS 实时性、可用性、可靠性、安全性时，对企业或组织的财产、人员及环境的影响。

e) 分析和评价 DCS 风险：

1) 在考虑丧失 DCS 的可用性、实时性、可靠性所造成的后果的情况下，评估安全失误可能对系统造成的影响；

2) 评估由主要威胁和脆弱点导致安全失误的可能性，对财产、人员及环境的影响，以及当前可采用的控制措施；

3) 估计风险的级别，确定风险是否可接受。

f) 识别和评价 DCS 风险处理的可选措施：

对于不可接受的 DCS 风险选择安全措施，降低风险到可接受范围。可能的措施包括：

1) 采用适当的控制措施，5.6 列举了可选择的安全控制措施；

2) 在满足企业或组织方针策略、安全要求和风险接受准则的情况下，可有意识地、客观地接受风险；

3) 调整相关风险环节，避免风险；

4) 转移相关业务风险，如保险公司、供应商等。

g) 为处理风险选择控制目标和控制措施：

选择和实施适用于 DCS 的控制目标和控制措施，以满足风险评估和风险处理过程中所识别的网络

安全要求。这种选择应考虑接收风险的准则以及法律法规和合同要求。控制措施的实施应以不影响DCS正常运行为前提。

h) 获得管理者对建议的残余风险的批准；

i) 获得管理者对实施和运行ISMS的授权；

j) 准备适用性声明，适用性声明的内容包括以下几方面：

1) 当前已有的安全目标和安全控制措施；

2) 在4.2.2 f)中的不可接受的风险及所选择的安全措施，以及选择的理由；

3) 其他需要增加或删减的安全措施及其增加/删减的理由。

4.2.3 实施与运行DCS的ISMS

实施和运行DCS的ISMS方针、控制措施、过程和规程，应做好以下几方面工作：

a) 为管理DCS网络安全风险，根据风险等级选择适当的管理措施、可用资源、职责分配和优先顺序，即制定DCS风险管理规程；

b) 建立DCS分区及分区目标安全等级，配置分区内设备，实施DCS风险管理规程，使DCS各分区达到目标安全等级和已识别的控制目标；

c) 实施5.6中所选择的控制措施，以满足控制目标风险管理与实施；

d) 确定如何测量所选择的控制措施或控制措施集的有效性，并指明如何评估控制措施的有效性及其对DCS系统性能的影响；

e) 开展培训和安全实施意识教育，确保参与ISMS工作的人员具备企业或组织要求的执行任务的能力；

f) 管理ISMS的运行；

g) 管理DCS的ISMS资源，包括资源的提供及人员管理；

h) 实施能够迅速检测DCS运行的安全事态的监控软件、响应安全事件的报警系统及其他控制措施。

4.2.4 监视与评审DCS的ISMS

对照ISMS方针、目标和实践经验，评估并测量ISMS过程的执行情况，包括验证是否按照文件化的流程执行以及所选择的控制措施是否部署，是否有效等，并将结果报告管理者以供评审，应包括：

a) 制定ISMS审计流程与方法；

b) 保持审计工作人员的独立性；对于特定DCS系统的审核，所要求的审计工作人员的能力范围应符合企业或组织的相关规定；

c) 实行ISMS定期审计，检测过程运行结果中的错误，识别试图的和得逞的安全违规和事件，确保所制定的网络安全策略与规程被正确执行以及DCS分区的网络安全目标得到满足；

d) 从组织机构、技术、DCS业务目标和工艺流程、已识别威胁、外部事态等方面考虑，监测DCS风险评估、风险处置的ISMS最佳实践，并定期进行DCS风险评估、残余风险和可容忍风险的评审；

e) 管理者应定期执行管理评审，包括对ISMS范围、ISMS控制措施状态、以往未强调的脆弱点威胁等的评审，确保ISMS持续的适宜性、充分性和有效性；

f) 建立符合性测量体系，应定义一套性能指标项(performance indicators)，每次定期审计的结果应能以各指标项表述，以此保证DCS的安全性能和安全态势；

g) 考虑监视和评审结果，以更新安全计划；

h) 建立审计文件跟踪记录，记录影响ISMS有效性和执行情况的措施和事态；

i) 设定惩罚性措施，应定义“违反符合性”的行为以及相关的惩罚措施。

4.2.5 保持与改进 DCS 的 ISMS

基于 ISMS 评审结果与其他外部相关信息，采取预防和纠正措施，持续改进 ISMS。应包括：

a) 建立专门负责管理 ISMS 改进及其实施的部门或团队(见 5.2)；
b) 实施已识别的 ISMS 改进与预防措施，调整 ISMS 以满足企业或组织的 DCS 网络安全目标；从其他组织和组织自身的安全经验中吸取教训；
c) 基于企业或组织的可容忍风险标准建立可能引起 ISMS 改进的触发(重大网络安全事件发生、法律法规的变动、DCS 重大结构变化等)，根据一系列触发重新评估并改进 ISMS；
d) 积极寻求 DCS 现场操作人员的安全建议反馈，并及时反馈给管理层。向所有相关方沟通措施和改进情况，其详细程度应与环境相适应。必要时，商议协定如何进行。

5 DCS 安全管理要素

5.1 方针、策略与规程

5.1.1 管理目标与范围

本项要求包括但不仅限于：

a) 应制定 DCS 网络安全工作的总体方针和安全策略，明确工控安全工作的总体目标、范围、原则和安全框架等；
b) 应对 DCS 安全管理活动中的各类管理内容建立安全管理制度；
c) 应对 DCS 各层管理人员或操作人员执行的日常管理操作建立操作规程；
d) 应形成由安全策略、管理制度、操作规程等构成的全面的工控网络安全管理制度体系。

5.1.2 制定与发布

本项要求包括但不仅限于：

a) 企业或组织应指定或授权专门的部门及其人员负责 DCS 安全管理制度的制定；
b) DCS 各项安全管理制度应具有统一的格式，并进行版本控制；
c) 应组织相关人员对制定的 DCS 安全管理制度进行论证和审定；
d) DCS 安全管理制度应以有效的方式在企业或组织内部正式进行发布；
e) DCS 安全管理制度应注明发布范围、对收发文件进行登记。

5.1.3 评审与修订

本项要求包括但不仅限于：

a) 应根据 DCS 安全管理制度的相应密级(如有要求)确定评审和修订的操作范围；
b) 应具有专门的部门与人员负责 DCS 安全管理制度的日常维护；
c) DCS 网络安全管理机构应负责定期组织相关部门与人员对 DCS 安全管理制度体系的合理性和适用性进行再评定，对存在不足或需要改进的地方进行再修订。

5.2 管理机构

5.2.1 安全机构

本项要求包括但不仅限于：

a) 应具备管理 DCS 安全的职能；
b) 应单独设立 DCS 安全管理的职能部门，设立安全主管、安全管理等负责人岗位；部门人员应由

跨物理安全、网络安全、工业控制等领域的人员组成，并定义各负责人职责；

c) 对于覆盖跨地区的企业或组织，总部应成立 DCS 安全管理委员会或 DCS 安全领导小组（统称 DCS 安全小组）。各下级单位应分别建立 DCS 安全领导小组，隶属总部 DCS 安全小组，下级单位的安全领导小组组长应由该单位主管领导委任或授权。

5.2.2 岗位设置

应设置系统管理员、安全管理员、安全审计员等岗位，并定义具体的岗位职责。

5.2.3 人员配备

本项要求包括但不仅限于：

a) 应根据 DCS 的各层规模合理配备管理与审计人员的数量；

b) 宜坚持岗位不可兼任原则，安全管理人员不能兼任网络管理员、操作员、数据库管理员、技术工程师等；

c) 对于 DCS 的主要站点，包括控制站、工程师站、操作员站、服务器等，应配备专人管理。

5.2.4 安全意识与培训

本项要求包括但不仅限于：

a) 在企业整体培训计划中，应包括工业控制系统网络安全方面的培训计划；

b) 培训种类包括针对全体员工的一般培训和针对特定岗位的培训，应包括安全责任、法律责任和业务控制措施等内容；

c) 针对特定岗位的培训，宜邀请网络安全领域的专家进行授课；

d) 在员工入职时安排培训，并在后续以固定周期进行；

e) 应能对工控网络安全培训的有效性进行评估；

f) 应具备对工控网络安全培训进行评审和改进的方法与规程。

5.2.5 沟通与合作

本项要求包括但不仅限于：

a) 应加强与企业或组织内部物理安全管理部门的沟通与合作；

b) 应在与外部供应商、第三方以及利益相关者等的商业合同中建立或改进 DCS 在物理与网络安全方面的流程与规程。

5.3 资产管理

本项要求包括但不仅限于：

a) 应清晰识别与 DCS 相关的资产，编制并保存资产清单，包括资产责任部门、重要程度和所处位置等内容；

b) 应建立资产安全管理制度，规定系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；

c) 应根据资产的重要程度、敏感度等对资产进行标识管理，根据资产的价值选择相应的管理措施；

d) 应按照企业或组织所采纳的分类机制建立和实施一组合适的资产标记和处理规程。资产标记应包括物理和资料格式的资产；

e) 应对系统相关的各种设备（包括备份和冗余设备）、网络等指定专门的部门或人员定期进行维护管理；

f) 应对控制站、工程师站、操作员站和服务器等设备的操作和使用进行规范化管理，按操作规程实现主要设备(包括备份和冗余设备)的启动/停止、上电/断电等操作。

5.4 人员

5.4.1 人员录用

本项要求包括但不仅限于：

a) 应对 DCS 重要岗位的内、外部应聘者进行背景审查，包括财务情况、犯罪记录、从业经历以及历史信用等；

b) 宜对 DCS 第三方合作的工作人员、供应商进行背景审查，包括财务情况、犯罪记录、从业经历以及历史信用等；

c) 如有必要，应对所有访问 DCS 的外部人员进行背景审查；

d) 如有必要，企业或组织应与利益相关者、供应商、第三方、顾客等外部方签署保密协议；

e) 在可能的情况下，录用人员应具有相应的资质，通过相关单位的认证。

5.4.2 人员考核与审查

本项要求包括但不仅限于：

a) 应明确定义员工的网络安全责任，同时与第三方合作单位人员、供应商等利益相关者明确合作中的网络安全责任；

b) 应定期对 DCS 工程师、各操作站点的系统管理员与操作人员进行相关的安全认知和安全技能的考核；

c) 如发现违反 DCS 网络安全有关规定的人员，应采取相应的惩罚措施。

5.4.3 人员离岗

本项要求包括但不仅限于：

a) 应立即中止企业或组织被解雇的、退休的、辞职的或其他原因离开的人员对 DCS 的所有物理或逻辑上的访问权限；

b) DCS 安全管理层和 DCS 关键岗位人员调离岗位，应根据离岗单位相关的保密管理要求和流程执行；

c) DCS 安全管理层和 DCS 关键岗位人员调离单位，应根据调离单位相关的保密管理要求和流程进行离岗安全审查，办理移交手续。

5.5 密码学

本项要求包括但不仅限于：

a) 应建立密码控制的使用管理方法，确保密码安全等级符合 DCS 安全保护级别；

b) 应使用加密技术保护经由移动设备，可移动介质或通信网络上传输的数据。

5.6 物理和环境

5.6.1 系统部署环境

本项要求包括但不仅限于：

a) 应指定专门人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；

b) 应配备机房安全管理人员，对出入机房、服务器的开机或关机等工作进行管理；

c) 应建立机房安全管理制度，规定有关机房物理访问，物品带进、带出机房和机房环境安全等方

面的管理要求；

d) 应规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态等。

5.6.2 系统资产与设备

本项要求包括但不仅限于：

a) 妥善安置或保护设备，尽量减少对工作区域的不必要访问，避免由环境威胁和危险所造成的各种风险以及未授权访问的机会；

b) 采取相应控制手段最小化潜在的物理威胁和风险，例如偷窃、火灾、爆炸等；

c) 应保护设备免受其他支持性设施（如电、供水、排污、空调）的失效而引起的电源故障和其他中断；

d) 应保护网络布缆免受未授权的窃听或损坏，分开电源电缆和通信电缆，防止互相干扰；

e) 应定期检查、正确维护设备，确保其持续的可用性、可靠性；

f) 应确保重要设备必须经过审批才能带离机房或办公地点。

5.6.3 数据存储介质

本项要求包括但不仅限于：

a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；

b) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；

c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；

d) 应对存储介质的使用过程、送出维修以及销毁等进行登记管理，对送出维修或销毁的介质应首先清除介质中的数据。

5.7 安全控制措施

5.7.1 访问控制

5.7.1.1 授权管理

本项要求包括但不仅限于：

a) 应初始化 DCS 验证器内容，包括令牌、密匙、口令卡、生物识别等；

b) 应对 DCS 的主要操作节点与控制节点分别实施逻辑与物理上的验证；

c) DCS 安装完成后应更改所有默认的验证器；

d) 应定期对所有 DCS 各操作节点的验证器进行更改；

e) 应能保护所有的验证器在存储与传输过程中不受到非授权的泄露或更改；

f) 对于 DCS 的软件过程与设备，应能提供硬件机制来保护相应的验证器；

g) 对 DCS 的重要操作域与控制域，应实行多重验证来实施访问控制；

h) 必要时，企业可根据不同的岗位和应用需求，定义相应的授权等级要求进行授权。

5.7.1.2 账户管理

本项要求包括但不仅限于：

a) 应建立 DCS 账户管理流程与策略，根据不同安全要求规定账户级别，规范 DCS 账户的使用流程；并定期对 DCS 账户管理流程与策略进行评审，如发现不足或有缺陷需重新修订该管理流程与策略；

b) 应根据 DCS 安全授权策略进行账户分类，并分配相应的访问权限，应具备统一账户管理的能力；
c) 应确保所有账户的授权、变动与终止均经过相应的授权管理；
d) 应对所有 DCS 操作节点的访问账户进行记录，包括使用人、被访问设备、权限以及管理者等；
e) 操作员站、工程师站等 DCS 操作节点与控制站/控制器的过程通信应进行安全账户管理；
f) 应及时停止或移除 DCS 各操作节点上不使用的账户；
g) 应定期对 DCS 各操作节点的所有账户进行检查；
h) DCS 首次安装建立的系统默认账户应及时移除。

5.7.1.3 身份鉴别

本项要求包括但不仅限于：

a) 应对 DCS 的主要操作节点，包括工程师站、操作员站、组态服务器、数据服务器、时钟同步服务器，以及连接在 DCS 的 MES 层网络和现场控制层网络上的人机会话接口等，所有使用者进行身份鉴别；
b) 对通过非信任网络访问 DCS 的使用者应实施多重鉴别策略；
c) 应对 DCS 主要操作节点、控制节点的软件过程与任务间通信实施鉴别控制，防止不安全的数据交换；
d) 应鉴别访问 DCS 设备与网络的便携式、可移动设备；
e) DCS 的组态管理与应用配置应启用高强度的鉴别方法；
f) 应记录对 DCS 主要操作节点与控制节点的设备或系统的所有访问尝试；
g) 应对 DCS 远程访问用户进行高强度的鉴别策略，应对远程登录与连接建立安全策略；
h) 当远程登录失败超过一定次数时，应能终止该账户对 DCS 设备或网络的访问；
i) 当长时间不启用的设备重新启用时，应重新鉴别远程访问该设备的用户身份；
j) 应能对 DCS 物理环境中无线通信的使用者、软件过程以及设备进行识别或鉴别(见 5.7.5)；
k) 应能对 DCS 中使用非授权的无线设备进行识别(见 5.7.5)。

5.7.2 使用控制

5.7.2.1 加强授权

本项要求包括但不仅限于：

a) 在 DCS 操作站与控制站的所有接口上，应能提供对所有用户的加强授权能力，以保证职责分离和最小特权原则；
b) 应设置某个授权用户或角色，能定义与修改所有用户的权限映射；
c) 应能支持高层管理者在特定时间或事件上对当前使用人使用权限的更改。

5.7.2.2 无线使用(见 5.7.5)

5.7.2.3 可移动设备、代码的使用

本项要求包括但不仅限于：

a) 应具有自动识别外部设备接入内部网络，并限制其使用的能力，如禁止便携式与移动设备接入 DCS 过程监控层网络、禁止移动代码等；
b) 便携式或移动设备在 DCS 不同分区层次和不同网络层次的使用，应考虑它们的接入是否满足接入分区或网络的安全要求，并根据安全要求实施不同级别的授权；
c) 应禁止从便携式设备上传代码与数据至 DCS 应用环境中，同时禁止从 DCS 应用环境中下载

代码与数据至便携式设备中；

d) 在保证系统功能正常可用的前提下，应禁止 Java、JavScript、ActiveX、PDF、Shockware movies 等移动代码在 DCS 各服务器中进行选择与使用，和在 DCS 各工作站中进行下载与执行；

e) 在执行 Java、JavScript、ActiveX、PDF、Shockware movies 等移动代码前，应能进行对移动会话的完整性的验证，防止执行被恶意篡改的移动代码。

5.7.2.4 安全会话

本项要求包括但不仅限于：

a) 对于关键控制流程或区域的监控与维护应使用安全远程会话；

b) 应对 DCS 的关键接口设定网络通信的安全策略（如最大带宽、最大连接数、并发会话数量），降低 DoS 攻击的风险；

c) 当会话不活动状态超过设定时间，应能自动终止会话；

d) 会话发起者应能手动终止会话。

5.7.2.5 安全审计

本项要求包括但不仅限于：

a) DCS 应能提供产生包括访问控制、请求错误、操作系统事件、控制系统事件、备份与存储事件、配置更改、潜在侦查活动、审计日志事件等记录的能力；

b) 单个审计记录应包括时间标识、源、分类、事件 ID 与事件结果；

c) 应能从 DCS 的多个组件中记录审计信息，集中管理审计事件；

d) 应能根据日志管理和系统配置来合理分配审计存储容量，当审计记录到达存储容量应能发出告警信息；

e) 当审计处理失败时，应能提供报警功能，防止基本服务和功能的丢失。

5.7.3 网络安全

5.7.3.1 网络分区

本项要求包括但不仅限于：

a) 应具有提供对 DCS 的 MES 层网络与过程监控层网络进行逻辑隔离或物理隔离的能力；

b) 应具有提供对 DCS 的过程监控层网络与现场控制层网络进行数据检测和数据过滤的防护能力；

c) 应具有提供对 DCS 现场控制层的关键控制区网络与非关键控制区网络进行逻辑隔离或物理隔离的能力；

d) 应具有提供对现场控制层实施独立网络服务的能力。

5.7.3.2 区域边界保护

本项要求包括但不仅限于：

a) 应根据不同网络层次、安全要求，以及可能面对的威胁，制定区域边界保护策略；

b) 任何与外界网络或控制系统所进行的连接，其接口处应具有边界保护或旁路监测措施；

c) DCS 各层网络的边界保护应提供相应等级的防护和管理措施，采用代理、网关、路由器、防火墙等合适的边界防护设备对不同网络层次进行隔离；

d) 当边界保护机制出现失败时，DCS 应具备告警能力，及时告知管理人员 DCS 系统异常；

e) DCS 系统应配置能阻断各层网络边界上任何通信的管理人员；在必要时，阻断异常的通信

线路；

f) 安全人员应定期对防护日志和监测记录进行分析，对安全策略进行优化。

5.7.4 数据安全

本项要求包括但不仅限于：

a) 应对涉及 DCS 的信息与数据进行分类，确定数据涉密类型，如 DCS 网关与路由器上的网络配置信息应视为保密信息；

b) 应通过写授权来确保 DCS 的核心和敏感信息在存储或传输过程中的保密性；

c) 应能提供 DCS 存储信息（包括备份信息）与不信任网络下安全远程会话信息的保密能力；

d) 应能保证 DCS 组态信息、控制指令信息、关键工艺参数在区域边界进行传输时的保密性；

e) 应能保证 DCS 组件的移除和更换不会造成组件上具有写授权信息的泄露；

f) 应能阻止未授权的信息通过共享内存资源进行传输；

g) 应能保证存储或包含 DCS 的核心和敏感信息的载体，在其传递或销毁过程中信息不会发生泄露；

h) 加密方法的选择应与需要保护的信息的价值、被泄露的影响后果以及 DCS 控制系统的运行约束等要素相匹配；

i) 销毁储存 DCS 核心和敏感信息的物理载体，可选择物理破坏或化学腐蚀等方法解决数据泄露问题。

5.7.5 无线安全

5.7.5.1 使用审批

本项要求包括但不仅限于：

a) 应制定使用无线连接的申报、审批及备案制度；

b) 应明确与工业控制系统进行无线通信的范围；

c) 应防止用户拥有未经授权而独立配置无线联网能力。

5.7.5.2 访问控制

本项要求包括但不仅限于：

a) 在允许用户通过无线连接访问工业控制系统前，应对用户的身份进行鉴别；必要时还需对用户使用的设备身份进行鉴别，禁止非授权访问；

b) 应能监控并告警未授权的无线连接。

5.7.5.3 数据安全

本项要求包括但不仅限于：

a) 应视具体应用需求，采用控制无线接入点的发射功率、无线信号屏蔽等措施，使得在工业控制系统工作区域物理边界之外的信号强度在可接受的范围内；必要时，应通过测试、验证，确保达到设计要求；

b) 应使用加密机制保护无线连接信道不被窃听；

c) 无线接入点应配置为点对点性质的无线访问；

d) 应能及时禁止未使用的嵌入系统无线联网的功能。

5.7.5.4 未授权设备监测

本项要求包括但不仅限于：

a) 应能扫描、识别和报告在工业控制系统物理环境内，已开启且能够接入工业控制系统在用无线网络的未授权无线设备(如发送 WiFi，蓝牙或其无线信号的设备)，确保没有任何非授权无线访问点与系统连接；
b) 在识别出未授权无线设备后，应能及时查找定位并关闭其发射功能或采用保护措施，尽可能消除未授权无线设备干扰控制系统正常运行或泄漏通信数据的风险；
c) 应制定在控制系统物理环境内使用未授权无线设备的惩罚措施或规章制度；并定期进行安全意识教育。

5.8 通信安全

5.8.1 网络安全管理

本项要求包括但不仅限于：
a) 应建立 DCS 中的网络设备管理职责和规程，确保控制网络中的信息和支持信息处理组件的安全；
b) 应使用具体的控制措施，确保通过公共网络或无线网的数据的保密性和完整性；
c) 应采用防护手段，隔离控制网络和外部管理网络，限制外部网络对控制网络的连接，禁止对控制服务或应用的直接访问。

5.8.2 信息传输

本项要求包括但不仅限于：
a) 建立网络安全传输的策略、规程，以保证企业/组织与外部方之间安全的商业信息传输；
b) 应定义控制和通知信息传输、派遣、接收过程的管理职责；
c) 应具有能检测和防止通过电子通信传输的恶意代码的程序；
d) 应使用密码技术，保护信息的完整性、保密性和真实性；
e) 应明确机密信息，并对其做保密处理，防止未授权的泄露或机密信息遭受破坏。

5.9 系统运营与维护

5.9.1 安全测试

本项要求包括但不仅限于：
a) 应测试 DCS 组件的安全功能与能力；
b) 应要求设备供应商进行 DCS 组件安全测试，并由企业或组织进行核实与确认；
c) 应要求设备集成商进行集成安全测试，并由企业或组织进行核实与确认；
d) 系统交付后，企业或组织应开展系统测试，确定 DCS 系统满足企业或组织的安全目标。

5.9.2 变更管理

本项要求包括但不仅限于：
a) 应建立 DCS 变更管理策略与规程并实施 DCS 变更管理系统，至少包括授权跟踪、备份与存储、补丁管理以及防恶意代码升级等；
b) 应对 DCS 设备或系统的变更进行评审，确定对 HSE 以及网络安全可能造成的风险；
c) 应详细说明变更的内容与位置，并符合变更申请要求；
d) 变更的批准与实施应分别交付不同的职能部门或个人进行；
e) DCS 网络安全变更管理应与现运行的 PSM 程序保持一致；
f) 应定期对变更管理的安全策略与规程进行评审。

5.9.3 补丁管理

本项要求包括但不仅限于：

a) 应建立并实施补丁管理和反病毒管理程序；

b) 应评估并确定补丁安装对系统安全的影响，确保补丁安装后系统能够满足目标安全等级；

c) 系统升级与维护应满足所在网络分区或环境的安全防护要求。

5.9.4 备份

本项要求包括但不仅限于：

a) 应建立备份与储存流程；

b) 应能提供当前控制系统安装的 DCS 组件及其属性的组件清单，清单内容至少应包括元件 ID、功能与维修等级；

c) 应采用配置管理过程来控制清单里组件信息的更改；

d) 应明确 DCS 用户级信息、系统级信息中关键文件的身份和位置；

e) 应确认所备份的介质与数据能成功使用。

5.9.5 恢复与重构

本项要求包括但不仅限于：

a) DCS 各操作站与控制站应能提供在不影响现有安全状态的情况下切换至紧急电源的能力；

b) DCS 各操作域与控制域应能提供从一个失败或破坏中恢复与重建到一个已知安全状态的能力；

c) 安全状态应包括控制系统参数已配置安全、主要补丁已安装、安全相关的配置已启用、系统文件与运行规程可用、系统软件与应用软件重新安装与安全配置、信息已从安全备份中下载、系统经过测试并且功能良好等方面要求。

5.10 供应商关系

5.10.1 供应商关系中的网络安全

本项要求包括但不仅限于：

a) 应建立与供应商关系相关的网络安全管理规程，识别和记录供应商的类型，并定义不同类型的供应商允许访问的信息类型，确保供应商可访问的 DCS 资产的安全；

b) 满足企业或组织对 DCS 网络安全要求和控制目标的条件，应记录在企业/组织与供应商签订的协议中；

c) 应监视和评审系统运行维护过程中，每个对应的供应商类型和访问类型的操作执行过程是否满足已经建立的网络安全管理规程；

d) 企业或组织应能处理与供应商访问相关联的突发事件和意外事故；

e) 更多供应商关系中的网络安全要求可参照 ISO/IEC 27002—2013 中的 15.1。

5.10.2 供应商服务交付管理

本项要求包括但不仅限于：

a) 应监测和评审供应商服务交付水平，是否满足双方签订的协议中的网络安全条款；监控服务执行级别以检查对协议的符合度；

b) 检阅供应商产生的服务报告，并结合独立审计员的审计报告（如有可能）对供应商进行审计，

识别存在的问题；

c) 解决和管理任何已识别的供应商服务问题；

d) 当供应商提供的服务发生变更时，应变更供应商协议，改进现有的网络安全策略，加强供应商提供的现有服务；

e) 更多供应商服务交付管理的网络安全要求可参照 ISO/IEC 27002—2013 中的 15.2。

5.11 信息与文件管理

5.11.1 文件控制

本项要求包括但不仅限于：

a) 应建立 DCS 生命周期的文件管理流程，以维护控制系统配置的安全性、可用性与使用性；

b) 对所访问的信息应定义相应的保密等级及其对应的共享、复制、传输与发布等权限限制；

c) 对涉及 DCS 的敏感信息，如控制系统设计参数、脆弱性评估结果、网络结构信息、工业运行控制项目信息等应进行分类保护，根据信息的敏感程度以及泄漏后可能所造成的后果来决定保护等级；

d) 应对需要特殊保护与处理的信息进行定期评审，以验证特殊保护是否依然需要；

e) 应定期对信息与文件管理流程实施审计。

5.11.2 记录控制

本项要求包括但不仅限于：

a) 应建立策略与规程来确保纸质版、电子版以及其他介质内信息的更新、保留、破坏、清除等的详细记录；

b) 应采取方法与措施确保数据在备份与记录过程中不受到破坏。

5.11.3 介质处置

本项要求包括但不仅限于：

a) 应建立信息的存储、修改、交换等介质管理规程；

b) 应建立安全处置介质的规程；

c) 应避免介质老化或更新换代导致信息丢失或不能读取。

5.12 业务连续性规划

本项要求包括但不仅限于：

a) 应建立 DCS 业务连续性规划小组，制定业务连续性规划；小组成员应包括企业或组织的关键股东；

b) 应对业务连续性规划小组的成员岗位与职责进行分配，可根据职能不同建立分小组，成员应包括 DCS 以及其他工业操作者；

c) 应根据组织或企业的风险容忍度与恢复目标决定关键业务与 DCS 子系统的重建优先级；

d) DCS 各操作域和控制域应确定相应的系统恢复目标与数据恢复目标；

e) 应明确 DCS 关键业务流程或系统恢复所需要的时间与资源，包括备份文件的位置、硬件、备份频率、热备份空间等；

f) 应确保存储备份系统(硬件、软件、文件等)的地方是安全的；

g) 应保证涉及文件管理与备份/恢复流程的多种形式(纸质、电子版)的记录有效；

h) 应考虑业务活动中断对供应链以及利益相关团体可能造成的影响；

i) 应详细规划当失去 email、电话等通讯方式时，团队成员之间的通信联系；
j) 应识别进行连续性规划时所面临的风险以及如何消除这些威胁；
k) 应根据测试计划测试备份系统的运行；
l) 应定期对业务连续性规划进行验证，若发现不足或有缺陷的地方，需及时修订。

5.13 安全事件规划与响应

5.13.1 规划制定

本项要求包括但不仅限于：

a) 应制定并实施 DCS 安全事件规划与响应规程，包括执行规划的责任人、事件响应队伍、协调防卫与响应的责任制、安全事件从始至终的评审、用于对安全事件识别、分类与优先级排序的规程、以及用于应对不同种类安全事件的规程等，识别相关责任人及其岗位要求与行为；
b) 事件响应规划应包含 DCS 应用环境下可能发生的网络安全事件的分类及其对应的响应行为，形成文件；
c) 事件响应规划应包含当出现安全事件时的持续性规划，包括对 DCS 进行隔离或恢复等；
d) 事件响应规划应能确保组织内部相关部门及其人员与外部组织之间保持联系。

5.13.2 安全事件上报

本项要求包括但不仅限于：

a) 应建立识别与报告 DCS 网络、操作域与控制域中不正常事件的规程；
b) 应对 DCS 操作类人员与安全管理类人员进行网络安全事件上报培训；
c) 应定期上报 DCS 网络安全事件，并保证安全事件上报的及时性；
d) 组织或企业应协同内部 IT 安全部门与涉及工业控制、自动控制应用部门就 DCS 安全事件进行交流。

5.13.3 安全事件管理与改进

本项要求包括但不仅限于：

a) 应详细记录 DCS 安全事件、所获得的教训以及所采取的行动；
b) 应建立安全事件处理制度，明确相关人员的责任和奖惩方案，以便事后进行安全事件追责；
c) 应对过去安全事件进行常规评审以改进 ISMS；
d) 应对事件响应规划进行定期演练，根据演练结果对规划进行改进。

5.14 符合性

5.14.1 符合法律要求

本项要求包括但不仅限于：

a) 明确定义所有与 DCS 相关的法令、法规和合同的要求以及满足这些要求企业或组织所采取的方法，并形成文件，保持更新；
b) 应实施适当的规程，以确保在使用具有知识产权的材料和具有所有权的软件产品时，符合法律、法规和合同的要求；
c) 防止重要记录（如数据库记录、安全事件记录、审计日志等）的遗失，毁坏和伪造，以满足法令、法规、合同和业务的要求；
d) 应依照相关的法律、法规和合同条款的要求，确保 DCS 重要工艺参数、数据的保护和隐私。

5.14.2 符合安全策略、标准，技术符合性

本项要求包括但不仅限于：

a) 管理人员应定期评审，确保在其职责范围内的所有关于 DCS 的安全规程被正确地执行，以确保符合安全策略及标准；

b) 应定期检查 DCS 系统与安全实施标准的符合程度。

参 考 文 献

[1] GB/T 18044—2004 信息技术 安全技术 信息安全事件管理指南
[2] GB/T 20282—2006 信息安全技术 信息安全工程管理要求
[3] GB/T 20720.1—2006 企业控制系统集成 第1部分:模型和术语
[4] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则
[5] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[6] GB/Z 24364—2009 信息安全技术 信息安全风险管理指南
[7] NIST SP 800-53 Recommended Security Controls for Federal Information Systems
[8] NIST SP 800-82 Guide to Industrial Control Systems(ICS)Security