ICS 25.040
N 10

中华人民共和国国家标准

GB/T 33009.4—2016

工业自动化和控制系统网络安全 集散控制系统(DCS) 第4部分:风险与脆弱性检测要求

**Industrial automation and control system security—
Distributed control system (DCS)—
Part 4: Risk and vulnerability detection 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4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、刘大龙、陆耿虹、刘文龙、吴彦彪、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4部分:风险与脆弱性检测要求

1 范围

GB/T 33009的本部分规定了集散控制系统(DCS)在投运前、后的风险和脆弱性检测,对DCS软件、以太网网络通信协议与工业控制网络协议的风险与脆弱性检测提出具体的要求。

本部分适用于对DCS中的下列对象进行脆弱性检测:

a) 监控软件、组态软件、数据库软件等DCS中的应用软件;

b) DCS操作员站和控制站等操作系统;

c) DCS中的具有网络协议实现和网络通信能力的功能和组件。

本部分不适用于智能仪表和工业无线的脆弱性检测。

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 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 28449—2012 信息安全技术 信息系统安全等级保护测评过程指南

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

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

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

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

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

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]

3.1.7

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]

3.1.8

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。

3.1.9

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]

3.1.10

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]

3.1.11

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]

3.1.12

嗅探 sniffing

使用嗅探器对数据流的数据截获与分组分析。

3.1.13

溢出漏洞 overflow vulnerability

由于程序中的某个或某些输入函数(使用者输入参数)对所接收数据的边界验证不严密造成的缓冲区溢出。

3.1.14

强度测试 stress testing

评价系统或部件在它规定的需求的限定或超出时情况的测试。

[GB/T 11457—2006,定义 2.1599]

3.1.15

模糊测试 fuzzy testing

通过向应用提供非预期输入并监控输出异常来发现软件中故障的方法。

3.1.16

语法测试 syntex testing

根据输入域和(或)输出域的定义设计测试用例。

3.1.17

数据完整性 data integrity

数据完整性泛指数据库中数据的正确性和一致性,包括实体完整性、参照完整性和用户定义完整性。

[GB/T 20273—2006,定义 3.1.9]

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)

ERP:企业资源计划(Enterprise Resource Planning)

HMI:人机界面(Human Machine Interface)

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

OPC:用于过程控制的对象链接与嵌入[Object Linking and Embedding(OLE)for Process Control]

4 DCS 风险与脆弱性检测概述

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。

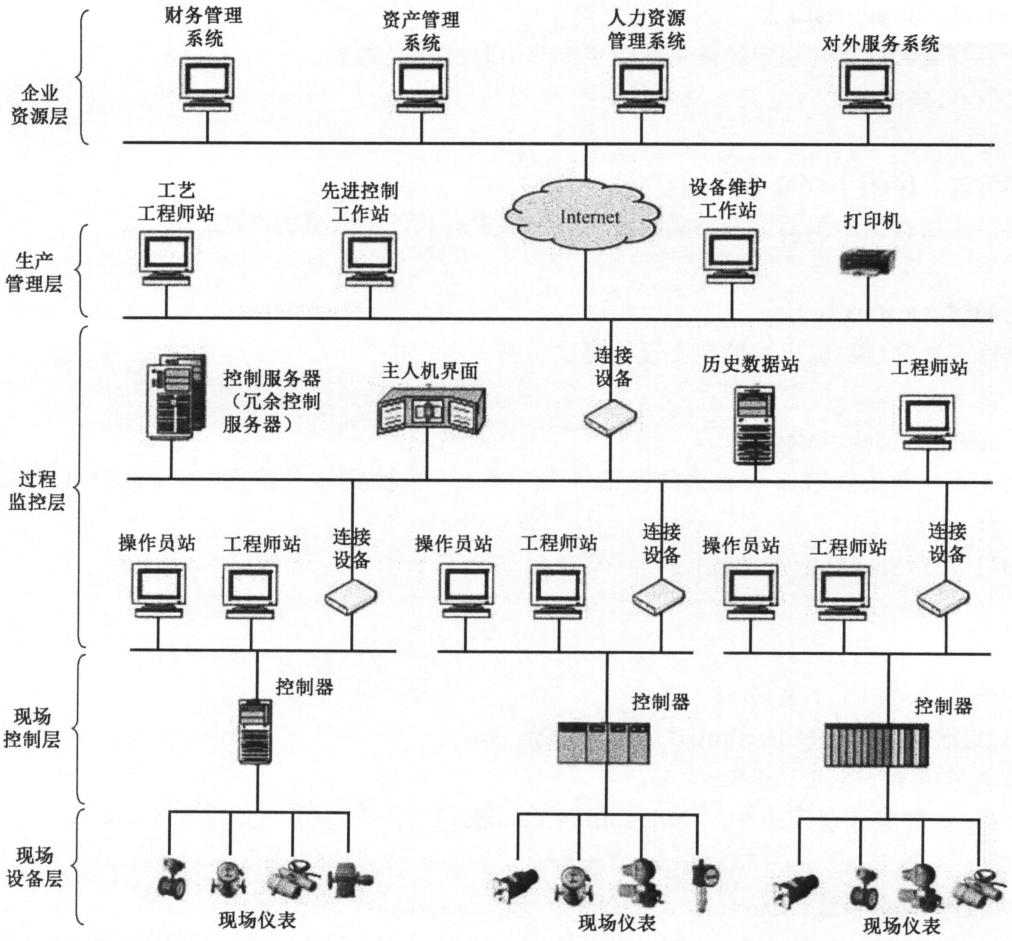

图 1　典型 DCS 系统应用的网络结构示意图

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风险与脆弱性检测的目标

DCS风险与脆弱性检测的目的是在DCS安全风险评估的基础上，通过对DCS系统的软件和系统通信安全的风险和脆弱性检测，发现现有DCS中潜在的安全风险和脆弱性。企业通过对潜在风险的处置，进一步提高DCS系统的安全性。DCS风险与脆弱性检测是对DCS安全风险评估工作的补充和扩展，主要用于对DCS系统安全性要求较高的行业和用户。

4.3 DCS风险与脆弱性检测基本原则

DCS进行风险与脆弱性检测时，应不明显影响原有系统的实时性、可用性、可靠性、安全性(safety)，而且检测应从系统的实时性、可用性、可靠性、安全性(safety)角度出发。对于DCS软件安全风险与脆弱性的各项测试内容建议在离线或模拟环境下执行；DCS网络通信协议安全风险与脆弱性的检测，为确保其有效性，建议在网络结构完整的DCS环境下进行，如在相同网络结构的模拟系统或目标DCS系统检修期间。本部分的建立旨在对DCS软件安全和网络通信的风险与脆弱性进行检测，使DCS满足DCS运行安全总体要求。

4.4 DCS风险与脆弱性检测内容

风险与脆弱性检测是DCS用户发起的，可由发起方实施或委托DCS安全服务组织支持实施。测试内容的选择宜以检测项为单位进行，以免破坏单个测试项的完整性。检测内容包括以下几个方面：

a) DCS软件安全风险与脆弱性
   1) 服务器和控制站的操作系统(见5.1)。
   2) 数据库管理系统(见5.2)。
   3) OPC类软件(见5.3)。
   4) DCS监控软件(见5.4)。
   5) DCS组态软件(见5.5)。
   6) 其他软件(见5.6)。
b) DCS网络通信安全风险与脆弱性
   1) 商用以太网协议通信机制(见6.1)。
   2) 工业网络协议通信机制(见6.2)。

3) DCS 通信数据安全(见 6.3)。

4) DCS 通信服务(见 6.4)。

5) DCS 状态转换(见 6.5)。

4.5 DCS 风险与脆弱性检测基本工作单元

根据 DCS 对稳定性、实时性和安全性的要求,结合 GB/T 28449—2012 关于信息系统安全等级保护测试工作单元的描述,建立 DCS 的安全检测工作单元。安全检测工作单元是 DCS 安全检测的基本工作单位,对应一组相对独立和完整的检测内容。DCS 安全检测工作单元由检测项、检测对象、检测方式、检测实施和结果判定组成,如图 2 所示。

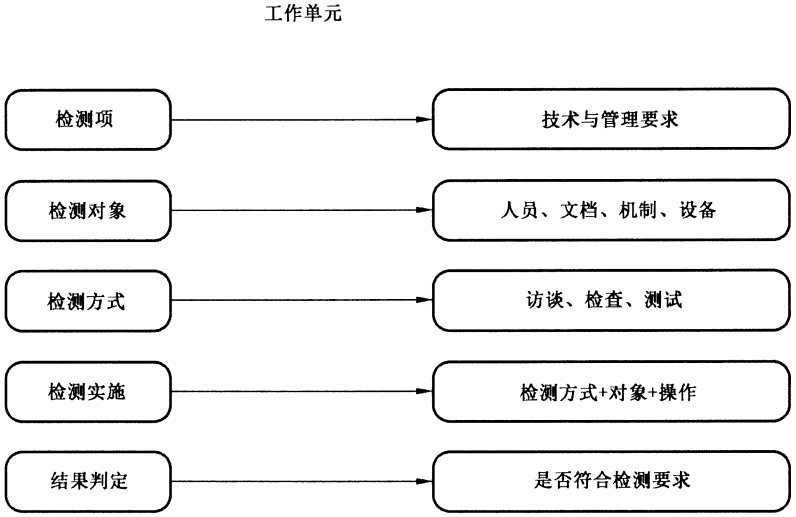

图 2 检测工作单元构成

检测项:描述检测目的和检测内容,提出具体的技术和管理要求。

检测对象:检测实施过程中涉及 DCS 的组成以及相关的操作与管理人员,是客观存在的人员、文档、通信机制或者设备等。检测对象是根据该工作单元中的检测项要求提出的。一般来说,实施检测时面临的具体检测对象可以是单个人员、文档、通信机制或者设备等,也可能是由多个人员、文档、通信机制或者设备等构成的集合,它们分别需要使用某个特定安全控制的功能。

检测方式:检测人员依据检测目的和检测内容选取的、实施特定检测操作的方式方法;一般包括三种基本检测方式:访谈、检查和测试。访谈是指检测人员与被测 DCS 系统有关人员(个人/群体)进行交流、讨论等活动,获取相关证据,了解有关信息。检查可分为文档审查、配置检查和实地查看等几种具体方法。文档审查是指检查操作规程、安全管理策略等文档是否齐备,是否有完整的制度执行情况记录(如机房出入登记表)等。配置检查是指检查与 DCS 相关的系统、设备等是否配置正确。实地查看是指检测人员到 DCS 系统运行现场通过实地观察人员行为、技术设施和物理环境判断人员的安全意识、业务操作、管理程序等方面的安全情况。测试是指利用技术工具进行测试。

检测实施:工作单元的主要组成部分。它是依据检测目的,针对检测内容开发出来的具体的检测执行实施的要求,涉及具体的检测方式、检测对象和操作过程。在描述检测实施过程中使用助动词"应(应该)",表示这些过程是强制性活动,检测人员作出结论必须完成这些过程;使用助动词"可(可以)"表示这些过程是非强制性活动,对检测人员作出结论没有根本性影响,检测人员可根据实际情况选择完成。本部分中的检测措施都是重要且需被考虑的,但是宜根据 DCS 的实际应用场景、企业或组织的 DCS 安全要求确定检测措施是否合适,选择切实可行的检测措施。

结果判定:描述检测人员执行检测操作得到各种检测证据后,如何依据这些检测证据来判定被测系

统是否满足检测项要求。在给出整个工作单元的检测结论前，需要先给出单个检测实施项的结论。一般来说，单个检测实施项的结论判定常常需要检测人员的主观判断，通常认为取得正确的、关键性证据，则该检测实施项就得到满足。

4.6 DCS 风险与脆弱性检测的执行

对于尚未部署和实施的 DCS 系统，DCS 风险与脆弱性检测可以选择在 DCS 投产运行前，安全评估后进行。

对于在现有 DCS 基础上进行升级或新增扩展功能的 DCS，建议在新旧系统联调测试前对新增系统部分进行风险与脆弱性检测。在新旧联调阶段对受影响的 DCS 关键组件和网络通信功能进行风险与脆弱性检测。

对于在役运行的系统，可选择在 DCS 升级改造后或检修、停运时进行风险与脆弱性检测。实际环境所限无法在运行环境中进行的风险与脆弱性检测项，可以在模拟环境中进行检测。

4.7 DCS 风险与脆弱性检测结果的处置

通过 DCS 风险与脆弱性检测结果，应依照以下流程进行处置：

a) 分析各检测项的测试结果，对不符合项合并整理后形成潜在风险描述；
b) 结合系统安全要求，分析潜在风险对 DCS 的安全影响，依照 DCS 安全方针确定潜在风险是否可接受。

对于不可接受的潜在风险，处置方法如下：

a) 采用适当的控制和管理措施(参见 GB/T 33009.2—2016 的 5.7，技术防护措施见 GB/T 33009.1—2016 的第 5 章～第 8 章)；
b) 对风险环节进行调整，避免风险；
c) 相关风险转移，如：保险公司，供应商等；
d) 进行潜在风险处置结果的有效性验证，重新对各不合规项进行验证检测。对于验证无效的风险处置应重新进行设置。

5 DCS 软件安全风险与脆弱性

5.1 服务器和控制站的操作系统

5.1.1 总则

服务器和控制站操作系统的主要功能是进行 DCS 资源管理和提供用户界面。管理的资源包括各种用户资源和 DCS 系统资源。操作系统以文件的形式对 DCS 的硬件资源和软件资源进行管理。文件类型包括数据文件、可执行文件、配置文件等。

根据 DCS 对稳定性、实时性和安全性的要求，结合 GB 17859—1999 所列安全要素和 GB/T 20271—2006 关于信息系统安全功能要素的描述，本条款重点检测 DCS 的主要操作节点(工程师站、操作员站、数据库服务器、OPC 服务器等连接在监控层和控制层上的人机会话接口站点)的操作系统在系统类型版本、补丁更新、账户管理、身份鉴别等方面的脆弱性。

5.1.2 检测项

检测项包括但不仅限于：

a) 操作系统类型和版本；
b) 操作系统补丁更新；

c) 账户管理；
d) 身份鉴别；
e) 访问控制；
f) 隐蔽信道；
g) 日志记录；
h) 审计；
i) 数据完整性。

5.1.3 检测对象

DCS 工程师站、DCS 操作员站、各类服务器的计算机主机，权限控制、升级记录和日志记录。

5.1.4 检测方式与实施

检测方式与实施包括但不仅限于：
a) 应访谈操作系统管理人员，检查操作系统类型和版本是否经过安全认证；
b) 应查看操作系统补丁更新记录，检查操作系统是否进行及时的补丁更新；
c) 应检查普通用户账户的账户权限，确定普通用户是否无法对操作系统的安全设置、系统文件和软件安装与卸载进行人为的更改与干预；
d) 应检查每一个授权账户的密码是否包含有限时间的有效期，确保该账户逾期无法登录；
e) 应检查员工职位变动后，是否删除与该员工相关的原账户；
f) 应检查账户的授权与注销是否由相关的安全管理人员按照安全管理规范进行集中管理；
g) 应检查是否对账户口令设置进行强制规定，如口令应具有一定的长度，并使用数字、大小写字母和特殊字符的组合，以及口令不能与个人信息相关等；
h) 应检测系统是否能阻止非授权用户的访问；
i) 应检测是否存在隐蔽信道，并确认信道危害在系统可容忍范围内；
j) 应检查系统日志是否准确记录系统事件、账户登录次数和时间与账户访问对象；
k) 应检查系统的安全审计记录是否完整；检测系统能否保护审计记录不被未授权的访问、修改和破坏；
l) 应检测储存在系统储存介质上的用户数据是否出现完整性错误。

5.1.5 结果判定

如果 5.1.4 a)～l)均满足要求，则 DCS 系统符合本单元检测指标要求。否则，信息系统不符合或部分符合本单元检测指标要求。

5.2 数据库管理系统

5.2.1 总则

数据库管理系统为 DCS 的数据采集、操作、监视、报表生成、报警、记录等功能提供支持。DCS 数据库管理系统包括实时数据库，报警数据库和历史数据库等。

根据 DCS 对稳定性、实时性和安全性的要求，结合 GB 17859—1999 所列安全要素和 GB/T 20271—2006 关于信息系统安全功能要素的描述，本条款重点检测 DCS 数据库管理系统对过滤恶意输入数据、数据连接安全、数据完整性、抵御 DoS 攻击等方面的脆弱性。

5.2.2 检测项

检测项包括但不仅限于：

a) 软件类型和版本；
b) 软件完整性；
c) 身份鉴别；
d) 访问控制；
e) 系统服务；
f) 数据连接；
g) 用户数据完整性；
h) 用户数据保密性；
i) 恶意输入；
j) 补丁更新；
k) 服务拒绝漏洞；
l) 溢出漏洞。

5.2.3 检测对象

数据库管理系统。

5.2.4 检测方式与实施

检测方式与实施包括但不仅限于：

a) 应访谈数据库管理人员，询问数据库软件的软件版本、软件授权属性，确认其为官方发布的正式版；
b) 应检查数据库管理系统功能实现所需的组件或文件的完整性，检测文件的大小及安装时间；
c) 应访谈数据库管理员，询问数据库软件的身份标识与鉴别机制采取何种措施实现；
d) 应检查数据库管理系统的鉴别信息是否具有不易被冒用的特点，口令的易猜测程度和复杂程度，确认登录用户和数据访问用户的口令是否相同，口令是否同时包括数字、大小写字母和符号三种字符，长度是否满足规定要求；
e) 应检测数据库管理系统能否根据不同的操作和对象，开放不同的访问权限，并限制具有某一权限的用户将该权限传给其他用户；
f) 检测数据库服务器上是否启动 DCS 中未使用的服务；
g) 应访谈数据库管理人员，询问是否采用了远程管理。若采用远程管理，查看是否采用了防止鉴别信息在网络传输过程中被窃听的措施；
h) 应检测数据库管理系统中用户数据的数据完整性；
i) 应检测数据库管理系统中数据库传输、储存的用户数据的保密性；
j) 通过构造格式错误的恶意非法输入，检测数据库管理系统的响应情况；
k) 应查看数据库管理系统补丁更新记录，检查数据库管理系统是否进行及时的补丁更新；
l) 检测数据库管理系统在 DoS 攻击下的可靠性和实时性，是否满足企业或组织的要求；验证数据库管理系统在被攻击环境下的数据操作响应时延；
m) 检测数据库管理系统的堆/栈溢出漏洞。

5.2.5 结果判定

如果 5.2.4 a)-b)，d)～m)均满足要求，则 DCS 系统符合本单元检测指标要求。否则，信息系统不符合或部分符合本单元检测指标要求。

5.3 OPC 类软件

5.3.1 总则

OPC 类软件用于实现不同控制系统之间的数据交换，能够实现 HMI 工作站、企业数据库、ERP 系统和其他面向企业的软件应用之间的数据交换。

根据 DCS 对稳定性、实时性和安全性的要求，结合 GB 17859—1999 所列安全要素和 GB/T 20271—2006 关于信息系统安全功能要素的描述，本条款重点检测 OPC 类软件（服务器与客户端）在访问控制、数据完整性等方面的脆弱性。

5.3.2 检测项

检测项包括但不仅限于：

a) 软件版本和类型；
b) 软件完整性；
c) 身份鉴别；
d) 恶意输入；
e) 补丁更新；
f) 服务拒绝漏洞；
g) 溢出漏洞。

5.3.3 检测对象

DCS 中 OPC 类软件服务器端、客户端。

5.3.4 检测方式与实施

检测方式与实施包括但不仅限于：

a) 应访谈 OPC 类软件管理人员，询问 OPC 类软件的软件版本、软件授权属性，确认其为官方发布的正式版；
b) 检测 OPC 类软件功能实现所需的组件或文件的完整性；
c) 访谈 OPC 类软件管理人员，询问 OPC 类软件的身份标识与鉴别机制采取何种措施实现，检测关键 OPC 类软件是否提供身份鉴别措施；
d) 检测 OPC 类软件口令的易猜测程度和复杂程度是否满足企业或组织的密码管理要求；
e) 通过构造格式错误的恶意非法输入，检测数据库软件的响应情况；
f) 应查看 OPC 类软件补丁更新记录，检查数据库软件是否进行及时的补丁更新；
g) 检测在 DoS 攻击下，OPC 类软件的可靠性和实时性；验证软件在被攻击状态下数据响应的时延是否在可接受范围内，是否出现不响应请求的情况；
h) 检测 OPC 类软件的堆/栈溢出漏洞。

5.3.5 结果判定

如果 5.3.4 a)～h)均满足要求，则 DCS 系统符合本单元检测指标要求。否则，信息系统不符合或部分符合本单元检测指标要求。

5.4 DCS 监控软件

5.4.1 总则

监控软件用于实现对整个生产过程的监控。监控软件反映的生产过程信息直接影响操作员对整个

生产过程状态的认识和判断。监控软件反应信息的真实性对操作员的决策行为至关重要。

根据 DCS 对稳定性、实时性和安全性的要求，结合 GB 17859—1999 所列安全要素和 GB/T 20271—2006 关于信息系统安全功能要素的描述，本条款重点检测监控软件在身份鉴别、数据完整性、真实反映现场信息等方面的脆弱性。

5.4.2 检测项

检测项包括但不仅限于：

a) 软件版本和类型；
b) 软件完整性；
c) 身份鉴别；
d) 恶意输入；
e) 信息真实性；
f) 服务拒绝漏洞；
g) 异常告警；
h) 监控数据保密性；
i) 溢出漏洞。

5.4.3 检测对象

DCS 工程师站、操作员站。

5.4.4 检测方式与实施

检测方式与实施包括但不仅限于：

a) 应访谈 DCS 监控软件管理人员，询问监控软件的软件版本、软件授权属性，确认其为官方发布的正式版；
b) 检测监控软件功能实现所需的组件或文件的完整性；
c) 访谈监控软件管理人员，询问监控软件的身份标识与鉴别机制采取何种措施实现，检测关键软件是否提供身份鉴别措施；
d) 检测监控软件口令的易猜测程度和复杂程度，确认口令复杂程度是否满足要求；
e) 通过构造格式错误的恶意非法输入，检测监控软件的响应情况；
f) 检测现场生产过程和设备状态信息与监控软件显示的信息的相符性；
g) 检测在 DoS 攻击下，监控软件的可靠性和实时性；验证软件在被攻击状态下数据响应的时延是否在可接受范围内，是否出现不响应请求的情况；
h) 在出现实时数据异常等情况时，检测监控软件是否能正常告警，并将异常数据记录到日志中；
i) 应检查是否对数据进行分类处理，并针对不同数据类型进行不同程度的保密性，检测除具有访问权限的合法用户外的其他用户是否能访问保密性数据；
j) 检测监控软件的堆/栈溢出漏洞。

5.4.5 结果判定

如果 5.4.4 a)～j)均满足要求，则 DCS 系统符合本单元检测指标要求。否则，信息系统不符合或部分符合本单元检测指标要求。

5.5 DCS组态软件

5.5.1 总则

组态软件一般安装于工程师站，用于实现对DCS的应用组态。通用的DCS经过组态成为针对特定具体控制应用的可运行系统。

根据DCS对稳定性、实时性和安全性的要求，结合GB 17859—1999所列安全要素和GB/T 20271—2006关于信息系统安全功能要素的描述，本条款重点检测组态软件在身份鉴别、数据完整性等方面的脆弱性。

5.5.2 检测项

检测项包括但不仅限于：

a) 软件版本和类型；
b) 软件完整性；
c) 身份鉴别；
d) 恶意输入；
e) 组态下载验证；
f) 服务拒绝漏洞；
g) 溢出漏洞。

5.5.3 检测对象

DCS工程师站、DCS操作员站。

5.5.4 检测方式与实施

检测方式与实施包括但不仅限于：

a) 应访谈DCS组态软件管理人员，询问组态软件的软件版本、软件授权属性，确认其为官方发布的正式版；
b) 检测组态软件功能实现所需的组件或文件的完整性；
c) 访谈组态软件管理人员，询问组态软件的身份标识与鉴别机制采取何种措施实现，查看关键软件是否提供身份鉴别措施；
d) 检测组态软件口令的易猜测程度和复杂程度，用信息嗅探手段，对组态软件的口令进行检测，验证软件口令是否存在易被获取和破解的风险；
e) 通过构造格式错误的恶意非法输入数据，检测组态软件的响应；
f) 检测组态下载前，是否具备安全验证机制防止非法组态的发生；
g) 检测在DoS攻击下，组态软件的可靠性和实时性；验证软件在被攻击状态下数据响应的时延是否在可接受范围内，是否出现不响应请求的情况；
h) 检测组态软件堆/栈溢出漏洞。

5.5.5 结果判定

如果5.5.4 a)～h)均满足要求，则DCS系统符合本单元检测指标要求。否则，信息系统不符合或部分符合本单元检测指标要求。

5.6 其他软件

涉及DCS的其他软件的检测，可参照上述软件的检测方法实施检测。

6 DCS网络通信安全风险与脆弱性

6.1 商用以太网协议通信机制

6.1.1 总则

商用以太网通信协议的实现都具有不同程度的脆弱性，应该对DCS中广泛存在的商用以太网通信协议进行脆弱性检测。商用以太网协议通信机制检测针对DCS过程监控层网络与上层网络结构，以及协议服务的事件机制进行脆弱性检测。

6.1.2 检测项

检测项包括但不仅限于：

a) 商用以太网协议的实现；

b) 商用以太网协议和TCP/IP协议的健壮性。

6.1.3 检测对象

DCS过程监控层网络所应用的商用以太网协议和TCP/IP协议。

6.1.4 检测方式与实施

检测方式与实施包括但不仅限于：

a) 应访谈DCS系统安全管理员，询问是否存在相应措施防止过程监控层用户私自连接到外部网络的行为；

b) 应询问DCS系统安全管理员，在过程监控层和企业管理层之间的通信边界是否具有相应的安全防护措施，检测这些措施对网络“非法连接”“非法访问”是否有效；

c) 应检测所应用的以太网协议和TCP/IP协议抵抗强度测试的能力，是否满足企业或组织的安全要求；

d) 应检测所应用的以太网协议和TCP/IP协议抵抗模糊测试的能力，是否满足企业或组织的安全要求；

e) 应检测所应用的以太网协议和TCP/IP协议抵抗语法测试的能力，是否满足企业或组织的安全要求。

6.1.5 结果判定

如果6.1.4 b)～e)均满足要求，则DCS系统符合本单元测评指标要求。否则，信息系统不符合或部分符合本单元测评指标要求。

6.2 工业网络协议通信机制

6.2.1 总则

常用的DCS工业网络通信协议在制定的时候未考虑安全因素，并且在控制设备上进行远程操控命令并不需要传统意义上的任何鉴别。对工业网络协议的检测主要从协议的实现是否满足通信协议本身规定的要求，以及协议会对网络实时性、可靠性、稳定性的影响出发。针对不同工业网络协议，其具体的检测方法可由检测机构与产品供应商、系统集成商、生产商以及协议制定者共同商讨确认。

6.2.2 检测项

检测项包括但不仅限于：

a) 工业网络协议的实现；

b) 工业网络协议的健壮性。

6.2.3 检测对象

检测对象为工业网络协议。

6.2.4 检测方式与实施

检测方式与实施包括但不仅限于：

a) 在工业网络协议的硬件实现检测方面，宜检测物理层信号实现和数据链路层实现的相关功能，是否满足协议规定的通信目标；

b) 在工业网络协议的软件实现检测方面，宜检测协议中的时钟同步机制在软件实现上是否满足协议规定的要求，其时钟同步精度是否满足企业或组织的业务需求；

c) 宜检测协议软件实现的仲裁机制是否能在企业或组织规定的时间内解决总线竞争冲突，实现畅通的数据通信；

d) 宜检测协议软件实现的错误校验机制，能否及时发现并处理通信数据异常，及错误校验机制对DCS系统性能的影响是否在企业或组织生产要求的可接受范围；

e) 宜检测协议软件实现的状态转换机制，在协议运行过程中是否会进行相应的状态转换，使协议按照预定的目标运行；

f) 宜检测所应用的工业网络协议抵抗强度测试的能力，是否满足企业或组织的安全要求；

g) 宜检测所应用的工业网络协议抵抗模糊测试的能力，是否满足企业或组织的安全要求；

h) 宜检测所应用的工业网络协议抵抗语法测试的能力，是否满足企业或组织的安全要求。

6.2.5 结果判定

由于不同的工业网络协议具有不同的通信机制，上述所给的检测实施项可作为检测工业网络协议脆弱性的一种参考。检测第三方或检测机构可根据DCS所使用的工业网络协议，选择其中的检测项执行，若这些检测项均满足要求，则DCS系统符合本单元检测指标要求。否则，信息系统不符合或部分符合本单元检测指标要求。

6.3 DCS通信数据安全

6.3.1 总则

DCS协议通信数据应该满足数据的完整性、保密性与可用性的要求。

6.3.2 检测项

检测项包括但不仅限于：

a) DCS通信协议数据的完整性；

b) DCS通信协议数据的保密性；

c) DCS通信协议数据的可用性。

6.3.3 检测对象

DCS通信协议数据。

6.3.4 检测方式与实施

检测方式与实施包括但不仅限于：

a) 询问现场工作人员，确认是否对 DCS 中过程监控层网络和现场设备层网络中传输的协议报文数据具有完整性校验措施；

b) 应检测对传输过程的通信协议数据进行篡改、删除、插入等操作时，DCS 系统能否及时正确的识别异常数据；

c) 询问现场安全管理人员，是否具有相应的加密措施保证 DCS 系统重要生产信息数据的安全性，防止其泄露；

d) 应检测 DCS 系统加密机制的安全性以及加密对系统实时性、可靠性、可用性等的影响；

e) 应检测记录 DCS 中重要的生产信息数据的存储资源的保密性和安全性。

6.3.5 结果判定

如果 6.3.4 b)、d)～e)均满足要求，则 DCS 系统符合本单元检测指标要求。否则，信息系统不符合或部分符合本单元检测指标要求。

6.4 DCS 通信服务

6.4.1 总则

为了实现应用软件与现场设备的数据通信，DCS 通信协议规定了多种服务，比如读/写设备信息、设置设备属性等。DCS 通信服务检测主要检测这些服务数据区中的有关设备自身的信息（如设备地址、设备属性等）的安全性，保证请求服务的正确性。

6.4.2 检测项

检测项包括但不仅限于：

a) DCS 设备地址的唯一存在性；

b) DCS 设备配置信息的完整性与修改合法性；

c) DCS 设备可用性；

d) DCS 设备活跃端口和服务的合理性。

6.4.3 检测对象

检测对象为 DCS 通信设备。

6.4.4 检测方式与实施

检测方式与实施包括但不仅限于：

a) 访问 DCS 工程师站技术人员，在系统组态完毕后是否对 DCS 系统中设备的物理或者逻辑地址的存在性和唯一性进行核实与确认；

b) 应检测 DCS 设备，验证是否可以对设备的地址信息进行非授权访问、修改或删除；

c) 询问 DCS 工程师站技术人员是否具有对 DCS 设备配置信息的完整性和修改合法性的保护措施以及合法性校验；检测破坏 DCS 配置信息时，DCS 系统能否及时发现并告警，以及检测 DCS 系统是否允许非法的配置信息修改；

d) 检测当 DCS 设备不能正常工作时，DCS 系统是否具备失效保护和冗余机制，保证 DCS 系统正常运作；

e) 确认 DCS 设备中活跃的通信端口以及正在执行的服务的必要性，检测是否及时将不必要的端口和服务关闭。

6.4.5 结果判定

如果 6.4.4 b)～d)均满足要求，则 DCS 系统符合本单元检测指标要求。否则，信息系统不符合或部分符合本单元检测指标要求。

6.5 DCS 状态转换

6.5.1 总则

在技术条件允许的情况下，根据 DCS 的组态配置、实时测量数据采集、控制指令输出等执行过程，对 DCS 状态转换进行检测，以确认 DCS 按照正常的流程安全运行。

6.5.2 检测项

检测项包括但不仅限于：

a) DCS 运行操作过程的状态转换功能；

b) DCS 网络通信过程的状态转换功能。

6.5.3 检测对象

操作员站、工程师站、DCS 控制器、工控网络(现场总线通信模块)。

6.5.4 检测方式与实施

检测方式与实施包括但不仅限于：

a) 在给定测量信号的情况下，检测 DCS 是否按照系统设计的要求，进行控制运算，控制指令发出等操作；

b) 在 DCS 输入输出点数超过系统设计上限的情况下，检测 DCS 是否按照设定的目标采集输入信号，运算并发出控制指令；

c) 对于具有通信能力的 DCS 组件(如操作员站、工程师站、OPC 服务器、OPC 客户端、DCS 控制器、输入输出模块、通信控制器等)，分别在网络流量为正常负荷、过载负荷、满负荷的情况下，检测 DCS 组件是否正常工作，以及 DCS 组件的工作状态是否按设定的流程进行转换；

d) 对于具有通信能力的 DCS 组件(如操作员站、工程师站、OPC 服务器、OPC 客户端、DCS 控制器、输入输出模块、通信控制器等)，在异常报文、异常流量的情况下，检测 DCS 组件是否正常工作，以及 DCS 组件的工作状态是否按设定的流程进行转换。

6.5.5 结果判定

如果 6.5.4 a)～d)均满足要求，则 DCS 系统符合本单元检测指标要求；否则，信息系统不符合或部分符合本单元检测指标要求。

参 考 文 献

[1] GB/T 11457—2006 信息技术 软件工程术语

[2] GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求

[3] GB/T 20278—2006 信息安全技术 网络脆弱性扫描产品技术要求

[4] IEC 62443-1-1 Security for industrial automation and control systems—Part 1-1: Terminology, concepts and models

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