ICS

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

集散控制系统(DCS)风险与脆弱性检测标准

The standards used for distributed control system risk and vulnerability detection

（征求意见稿）

（本稿完成日期：2014-5-7）

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

集散控制系统(DCS)风险与脆弱性检测标准

1 范围

本标准规定了集散控制系统（DCS）的风险和脆弱性检测，重点对DCS软件、DCS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。

本标准适用于对以下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 工业站的操作系统；

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。

本系列集散控制系统（DCS）安全类标准共包括集散控制系统（DCS）安全防护标准、集散控制系统（DCS）安全管理标准、集散控制系统（DCS）安全评估标准、集散控制系统（DCS）风险与脆弱性检测标准四个标准。四个标准相辅相承，系统的定义了集散控制系统在实施、运行和维护过程中，系统安全性的持续和改进的安全要点和执行方法。其中：

——集散控制系统（DCS）安全防护标准中定义了集散控制系统在运行和维护过程中应具备的安全能力和防护技术要求，是其它三个标准的基础和实施依据；

——集散控制系统（DCS）安全管理标准定义了集散控制系统在运行和维护过程中应具备的安全管理要点和防护管理要求；

——集散控制系统（DCS）安全评估标准定义了集散控制系统在运行和维护过程中对系统技术防护能力和安全管理有效性的评估过程和方法；

——集散控制系统（DCS）风险与脆弱性检测标准定义了集散控制系统在运行和维护过程中潜在系统脆弱性和安全风险的检测内容和测试方法。

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 20272—2006《信息安全技术 操作系统安全技术要求》

集散控制系统（DCS）安全防护标准(2014)

集散控制系统（DCS）安全管理标准（2014）

3 术语、定义、缩略语和约定

3.1 术语和定义

3.1.1 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。

3.1.2 可用性 availability

数据或资源的特性，被授权实体按要求能访问和使用数据或资源。

3.1.3 鉴别 Authentication

用于验证用户所声称的身份。验证用户身份的过程或装置，通常是允许进行信息系统资源访问的先决条件。

3.1.4 授权用户 Authorized User

依据安全策略可以执行某项操作的用户。

3.1.5 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。

3.1.6 机密性 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。

3.1.7 控制系统信息安全 control system cyber 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。

3.1.8 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。

3.1.9 识别 identify

对某一评估要素进行标识与辨别的过程。

3.1.10 安全风险 information 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。

3.1.11 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。

3.1.12 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：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：更多的信息参见IEC 62264-1。

3.1.13 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。

3.1.14 远程终端装置（RTU） Remote Terminal Unit

集远方数据采集、传输、存储功能于一体的终端设备。

3.1.15 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。

3.1.16 安全事件 security incident

指系统、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。

3.1.17 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。

3.1.18 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。

3.1.19 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。

3.1.20 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

3.2 缩略语和缩略词

CSMS	网络信息安全管理系统 Cyber security management system
DCS	集散控制系统 Distributed control system
DMZ	隔离区 Demilitarized zone
Dos, DDos	服务拒绝，分布式服务拒绝 Denial of service, Distributed denial of service
FDN	现场设备网络 Field device network
HMI	人机界面 Human machine interafce
IACS	工业自动化和控制系统 Industrial automation and control system(s)
MES	制造执行系统 Manufacturing execution system
PCN	过程控制网络 Process control network
PLC	可编程逻辑控制器 Programmable logic controller
VLAN	虚拟本地网 Virtual local area network
VPN	虚拟专用网 Virtual private network

4 DCS 风险与脆弱性检测概述

4.1 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，自上到下依次为企业管理层、制造执行系统（manufacturing execution system，简称MES）层、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。本标准主要对DCS应用中与DCS系统密切相关的MES层、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定义。

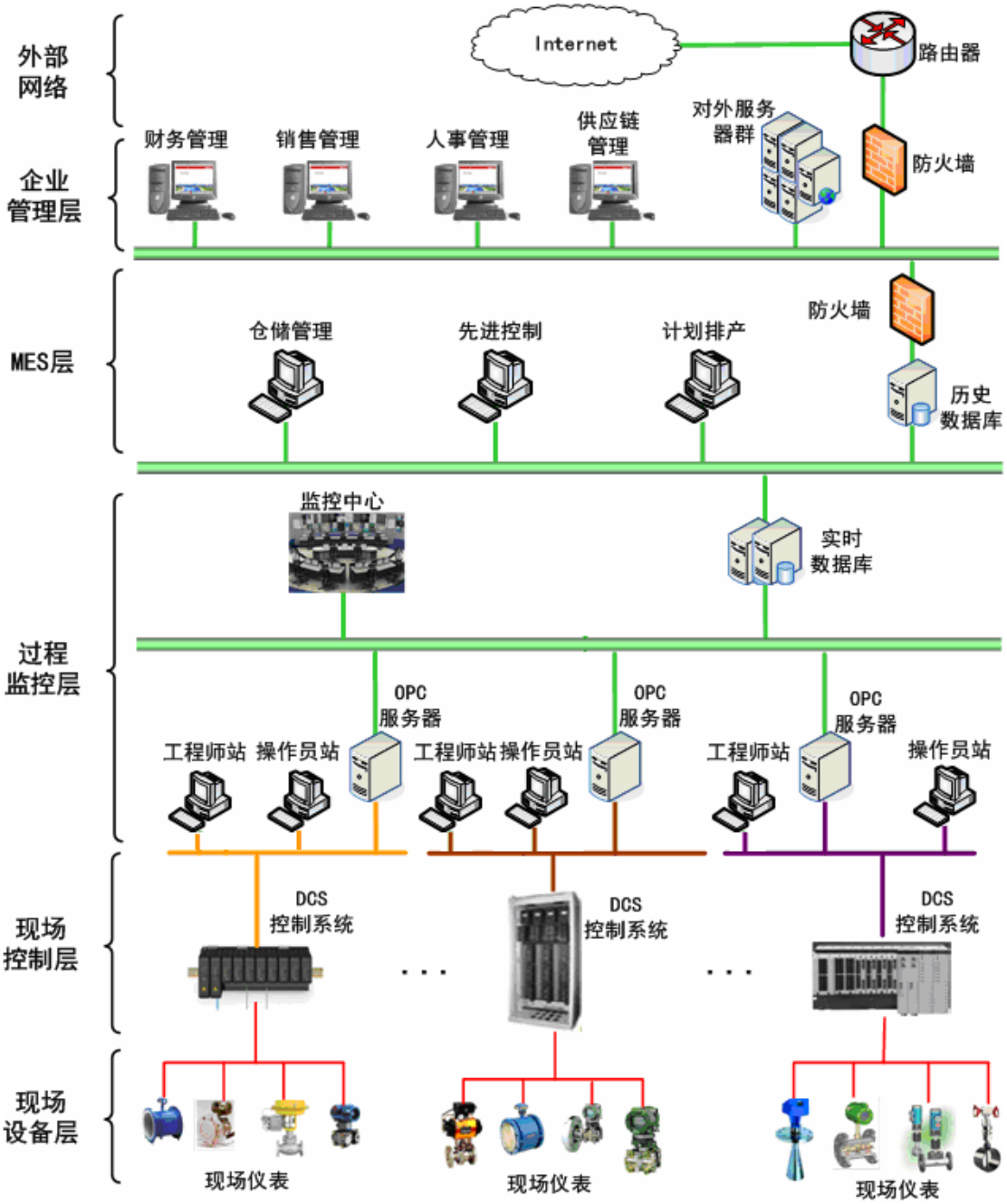

图1　典型 DCS 系统应用的网络结构示意图

企业管理层：企业管理层所面向的使用者是厂长、经理、总工程师等行政管理或运行管理人员，因此只有大规模的DCS系统才具备这一层。该层网络主要包括ERP系统，该系统主要包含供应链管理、销售与市场管理、财务管理和人力资源管理等功能。

MES层：MES将生产过程控制、生产过程管理和经营管理活动中产生的诸多信息进行转换、加工、传递，是生产过程控制与管理信息集成的重要桥梁和纽带。MES要完成生产计划的调度与统计、生产过程成本控制、产品质量控制与管理、设备控制与管理、生产数据采集与处理等功能，负责生产管理和调度执行。

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，实现反馈控制、逻辑控制、顺序控制和批量控制功能；对现场设备及I/O卡件进行自诊断；与过程监控层进行数据通信。

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

与DCS的层次结构相对应，DCS系统网络主要包括现场控制网络、监控网络和管理网络。

现场监控网络主要由现场总线以及远程I/O总线构成，包括控制器与现场仪表、I/O模块之间的所有总线。

监控网络位于监控层，用于连接监控层工程师站、操作员站、实时数据库、监控计算机等人机接口站，传递实时监控数据。

管理网络位于企业管理层，用于连接各类管理计算机。

4.2 DCS 运行安全总体要求

——实时性要求

DCS在性能上主要以实时性和可靠性作为最主要的评判依据，系统不允许存在延迟和抖动，需具备实时响应能力。

——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。

——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，否则会引起重大的人员伤害，设备损失以及环境污染等。

——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。

——高可靠性要求

DCS具有可靠性要求，DCS一部分设备出现故障不应该影响整个系统的正常工作，为此系统采用了多微处理机分散控制结构，某一单元失效时，不会影响其他单元的工作。即使在全局性通信或管理站失效的情况下，局部站仍能维持工作。

4.3 DCS 风险与脆弱性检测的目标

DCS风险与脆弱性检的目的是在DCS安全评估的基础上，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漏洞，企业通对对潜在风险的处置，进一步提高DCS系统的安全性。DCS风险与脆弱性检对DCS安全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。

4.4 DCS 风险与脆弱性检测的执行阶段

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，DCS安全评估之后进行。

对于在现有DCS进行升级或扩展功能新增的DCS，建议在新旧系统调联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DCS系统受影响的关键组件和网络通信功能进行风险与脆弱性检测。

对于已投产在运行的系统，可选择在DCS系统检修或升级改造阶段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。

4.5 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，对潜在风险对 DCS 的安全的影响进行分析，依照 DCS 的安全方针确定，潜在风险是否可被接受；
c) 对于不可接受的潜在风险，进行处置方法如下：
d) 采用适当的控制措施，管理控制措施见《集散控制系统（DCS）安全管理标准》条目 5.6，技术防护措施见《集散控制系统（DCS）安全防护标准》条目 5~8。
e) 对风险环节进行调整，避免风险；
f) 将相关业务风险转移到其他方，如：保险，供应商等。
g) 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处置。

4.6 DCS 风险与脆弱性检测内容

风险与脆弱性检测是DCS拥有方、运营方或使用方发起的对DCS进行的检测，可由发起方实施或委托DCS安全服务组织支持实施。检测的内容主要包括：

1）DCS 软件安全风险与脆弱性

a) 工作站操作系统（见 5.1）
b) 数据库软件（见 5.2）
c) OPC 软件（见 5.3）
d) 人机交互软件（见 5.4）
e) 监控软件（见 5.5）

2）DCS网络通信协议安全风险与脆弱性检测

a) 以太网协议通信机制检测（见 6.1）
b) 工业网络协议通信机制检测（见 6.2）
c) DCS 通信数据安全检测（见 6.3）
d) DCS 通信服务检测（见 6.4）
e) DCS 状态机转换检测（见 6.5）

实施检测的组织可根据组织自身的实际用户需求进行检测目标的设立，可选用标准中完整或剪裁的检测内容进行测试，测试内容的选择应以检测项为单位进行，以免破坏单个测试项的完整性。

4.7 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，应不影响原有系统的实时性、可靠性、安全性，而且检测应从系统的实时性、可靠性、安全性角度出发，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。

本标准的建立旨在对DCS操作软件、与监控软件、网络通信协议、网络数据安全的风险与脆弱性进行检测，使DCS满足以下要求：

1）可用性

确保合法用户可以随时访问DCS资源，包括控制系统、安全系统、操作站、工程师站以及通信系统等，可用性是生产过程连续稳定运行的基础。

2）完整性

防止未授权用户或者恶意程序对DCS信息和数据的修改，所要保护的信息包括检测值、控制命令、配置信息以及系统内部审计信息等。

防止对非授权用户或者恶意程序的信息泄露，所要保护的信息包括两类：一类是特定工业生产领域的专有信息，如生产方法、设定性能数据等；另一类是系统安全机制类的信息，如口令、密钥等。

4.8 DCS 风险与脆弱性检测基本工作单元

根据DCS对安全性、稳定性和实时性的要求，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。

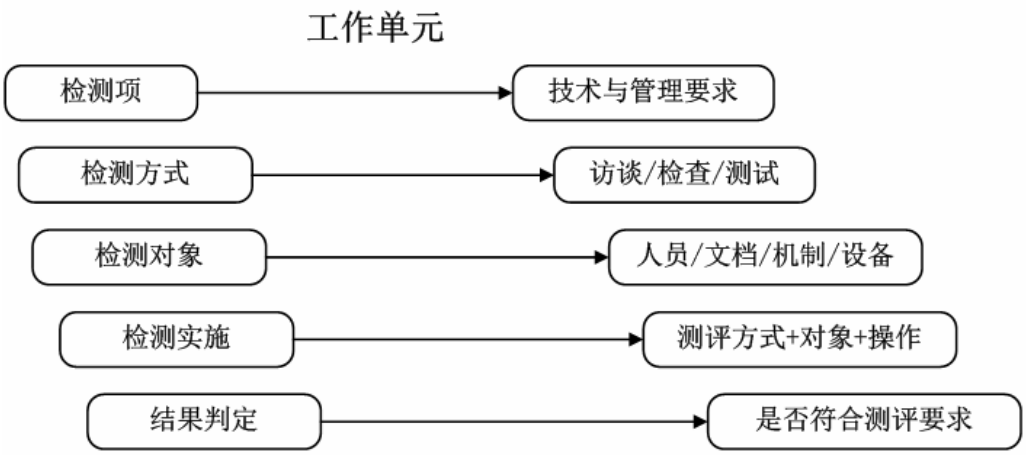

图2　检测工作单元构成

检测项：描述测评目的和测评内容。

检测方式：测评人员依据测评目的和测评内容应选取的、实施特定测评操作的方式方法，一般包括三种基本测评方式：访谈、检查和测试。

检测对象：测评实施过程中涉及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、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，面临的具体测评对象可以是单个人员、文档、机制或者设备等，也可能是由多个人员、文档、机制或者设备等构成的集合，它们分别需要使用到某个特定安全控制的功能。

检测实施：工作单元的主要组成部分，它是依据测评目的，针对具体测评内容开发出来的具体测评执行实施过程要求。测评实施描述测评过程中涉及到的具体测评方式、内容以及需要实现的和/或应该取得的测评结果。在测评实施过程描述中使用助动词“应（应该）”，表示这些过程是强制性活动，测

评人员为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，对测评人员作出结论没有根本性影响，因此测评人员可根据实际情况选择完成这些过程。

结果判定：描述测评人员执行完测评实施过程，产生各种测评证据后，如何依据这些测评证据来判定被测系统是否满足测评项要求的方法和原则。在给出整个工作单元的测评结论前，需要先给出单项测评实施过程的结论。一般来说，单项测评实施过程的结论判定不是直接的，常常需要测评人员的主观判断，通常认为取得正确的、关键性证据，该单项测评实施过程就得到满足。

5 DCS 软件安全风险与脆弱性检测

5.1 工作站操作系统检测

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管理DCS的硬件资源和软件资源，文件形式有数据文件、可执行文件、配置文件等。

根据DCS对安全性、稳定性和实时性的要求，结合GB17859-1999 所列安全要素和GA/T 20271-2006 关于信息系统安全功能要素的描述，本条款的目的在于检测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、时钟同步服务器等连接在过程信息网和过程控制网上的人机会话接口站点的操作系统在安全级别、补丁更新、安全设置、口令安全等方面的脆弱性。

5.1.1 检测项

a) 操作系统类型和版本；
b) 操作系统补丁更新；
c) 账户安全；
d) 登录口令；
e) 日志记录。

5.1.2 检测方式

访谈，检查。

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及其计算机管理员，密码管理制度，升级记录，日志纪录，恶意代码检测记录，分析报告。

5.1.4 检测实施

a) 应检查操作系统类型和版本是否经过安全认证；
b) 应检查操作系统的安全级别是否达到 GB/T20272—2006 标准规定的第三级要求；
c) 应检查操作系统是否进行及时的补丁更新；
d) 普通用户账户应不具有管理员权限，应检查普通用户是否无法对操作系统的安全设置、系统系统文件和软件安装与卸载进行人为的更改与干预；
e) 应保证每一个授权账户包含有限时间的有效期，逾期后账户无法登录；
f) 员工职位变动时，应删除原有账户，且保证每次授权账户的用户名不具有相关性，攻击者难以根据之前的账户名猜测或推断出现有用户名；
g) 账户的授权与注销应由安全人员按照安全管理规范进行集中管理；

h) 系统已有授权帐户的口令应具有一定的复杂度/健壮性，应满足由账户名无法经过简单的变换而得到与之对应的口令；
i) 系统已有授权帐户的口令应具有一定的复杂度/健壮性，应满足未使用易于猜测的口令；
j) 系统已有授权帐户的口令应具有一定的复杂度/健壮性，应满足口令与个人信息无关；
k) 系统已有授权帐户的口令应具有一定的复杂度/健壮性，口令具有一定的长度，并使用数字、字母和特殊字符的组合
l) 应确保事件与日志准确记录系统事件、账户登录次数和时间与账户访问对象。

5.1.5 结果判定

5.1.4 a）- l）均为肯定，则信息系统符合本单元测评项要求。

5.2 DCS 数据库软件检测

数据库系统为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数据库系统包括实时数据库，报警数据库和历史数据库等组成。

根据DCS对安全性、稳定性和实时性的要求，结合GB17859-1999 所列安全要素和GA/T 20271-2006关于信息系统安全功能要素的描述，本条款的目的在于重点检测DCS数据库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。

5.2.1 检测项

a) 软件合法性；
b) 软件完整性；
c) 身份鉴别；
d) 登录口令；
e) 系统服务；
f) 数据连接；
g) 恶意输入；
h) 补丁更新；
i) 拒绝服务；
j) 信息嗅探；
k) 内存漏洞。

5.2.2 检测方式

检查，测试。

5.2.3 检测对象

数据库服务器。

5.2.4 检测实施

a) 检测的数据库软件的软件授权属性，对软件版本进行检测，是否为官发布的正式版；
b) 检测数据库软件数字证书的合法性；
c) 检测数据库软件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；
d) 检测数据库软件对接收的外部数据的完整性验证；

e) 检测数据库软件对用户的身份鉴别机制，确认用户身份认证机制是否设为默认方式,是否安全有效；
f) 检测数据库软件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据、字母和符号三种字符，长度是否大于 8 位；
g) 对数据库服务器上运行的各项服务进行检测，是否启动 DCS 中未使用的服务；
h) 进行远程数据库查询检测，检测操作结果，验证是否可以远程对用户口令等等敏感数据进行访问；
i) 通过构造不具有正确格式的恶意非法输入数据，以达到执行非授权命令或功能的目的，检测数据库软件的响应；
j) 对软件进行补丁更新检测；
k) 检测拒绝服务攻击下软件的可靠性和实时性,验证数据库软件是被攻击环境下的数据操作响应时延；
l) 对网络进行信息嗅探检测；
m) 检测数据库软件栈溢出漏洞；
n) 检测数据库软件堆溢出漏洞。

5.2.5 结果判定

5.2.4 a）- o）均为肯定，则信息系统符合本单元测评项要求。

5.3 OPC 软件检测

OPC用于实现不同的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系统和其它面向企业的软件应用之间的数据交换。

根据DCS对安全性、稳定性和实时性的要求，结合GB17859-1999 所列安全要素和GA/T 20271-2006关于信息系统安全功能要素的描述，本条款的目的在于重点检测OPC软件（服务器与客户端）在防问控制、数据完整性、抵御中间人攻击等方面的脆弱性。

5.3.1 检测项

a) 软件合法性；
b) 软件完整性；
c) 身份鉴别；
d) 登录口令；
e) 恶意输入；
f) 补丁更新；
g) 拒绝服务；
h) 信息嗅探；
i) 内存漏洞。

5.3.2 检测方式

检查，测试。

5.3.3 检测对象

DCS各应用服务器端、客户端。

5.3.4 检测实施

a) 检测 OPC 软件授权属性；
b) 检测 OPC 软件数字证书合法性；
c) 检测 OPC 软件功能实现所需的组件或文件的完整性；
d) 检测 OPC 软件对中间人攻击的抵御能力；
e) 检测 OPC 软件对用户的身份鉴别机制；
f) 检测 OPC 软件口令的易猜测程度和复杂程度；
g) 对 OPC 服务器上运行的各项服务进行检测；
h) 通过构造不具有正确格式的恶意非法输入数据，以达到执行非授权命令或功能的目的，检测 OPC 软件的响应；
i) 对软件进行补丁更新检测；
j) 检测拒绝服务攻击下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，是否出现响应不响应请求的情况；
k) 检测 OPC 软件内部功能模块间的数据流以及软件对输入数据的响应;
l) 对网络进行信息嗅探检测；
m) 检测 OPC 软件栈溢出漏洞；
n) 检测 OPC 软件堆溢出漏洞。

5.3.5 结果判定

5.3.4 a）- o）均为肯定，则信息系统符合本单元测评项要求。

5.4 DCS 人机交互软件检测

人机交互软件一般位于操作员站，提供了操作员与生产过程交互的接口，主要完成控制过程中控制算法、参数设定功能，操作员指令实时、安全的传送到控制器对控制过程的稳定、安全运行至关重要。

根据DCS对安全性、稳定性和实时性的要求，结合GB17859-1999 所列安全要素和GA/T 20271-2006关于信息系统安全功能要素的描述，本条款的目的在于重点检测人机交互软件在身份鉴别、数据完整性、抵御中间人攻击和重放攻击等方面的脆弱性。

5.4.1 检测项

a) 软件合法性；
b) 通信完整性；
c) 身份鉴别；
d) 登录口令；
e) 输入验证；
f) 输出确定性；
g) 拒绝服务；
h) 中间人攻击；
i) 重放攻击；
j) 内存漏洞。

5.4.2 检测方式

检查，测试。

5.4.3 检测对象

具有人机交互界面的各操作站。

5.4.4 检测实施

a) 检测人机交互软件授权属性；
b) 检测人机交互软件数字证书合法性；
c) 检测人机交互软件功能实现所需的组件或文件的完整性；
d) 检测人机交互软件对接收的外部数据的完整性验证；
e) 检测人机交互软件对用户的身份鉴别机制；
f) 检测人机交互软件口令的易猜测程度和复杂程度，确认口令中是否同时包括数字、字母和符号三种字符，口令长度是否大于 8 位；
g) 授权用户输入错误数据或进行不适当操作时，检测人机交互软件的运行状态，检测是否具备输入合法性验证机制；
h) 通过构造不具有正确格式的恶意非法输入数据，以达到执行非授权命令或功能的目的，检测人机交互软件的响应，检测是否具备输入合法性验证机制；
i) 检测当人机交互软件受到攻击不能正常运行时，是否具备输出确定性保护机制或措施；
j) 检测拒绝服务攻击下软件的可靠性和实时性；
k) 对人机交互软件和控制器进行中间人攻击检测；
l) 对人机交互软件和控制器进行重放攻击检测；
m) 检测人机交互软件内部功能模块间的数据流以及软件对输入数据的响应。
n) 检测人机交互软件栈溢出漏洞；
o) 检测人机交互软件堆溢出漏洞。

5.4.5 结果判定

5.4.4 a）- o）均为肯定，则信息系统符合本单元测评项要求。

5.5 DCS 监控软件检测

监控软件用于实现对整个生产过程的监控，包括实时数据曲线、历史数据曲线、报警的生成等。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对安全性、稳定性和实时性的要求，结合GB 17859-1999 所列安全要素和GA/T 20271-2006关于信息系统安全功能要素的描述，本条款的目的在于重点检测监控软件在数据完整性、抵御中间人和重放攻击、真实反映现场信息等方面的脆弱性

5.5.1 检测项

a) 软件合法性；
b) 通信完整性；
c) 身份鉴别；
d) 登录口令；
e) 输入验证；
f) 信息真实性；
g) 拒绝服务；

h) 中间人攻击；
i) 重放攻击；
j) 信息嗅探；
k) 内存漏洞。

5.5.2 检测方式

检查，测试。

5.5.3 检测对象

DCS工程师站、操作员站。

5.5.4 检测实施

a) 检测监控软件授权属性；
b) 检测监控软件数字证书合法性；
c) 检测监控软件功能实现所需的组件或文件的完整性；
d) 检测监控软件对接收的外部数据的完整性验证；
e) 检测监控软件对用户的身份鉴别机制；
f) 检测监控软件口令的易猜测程度和复杂程度；
g) 通过构造不具有正确格式的恶意非法输入数据，以达到执行非授权命令或功能的目的，检测监控软件的响应；
h) 检测拒绝服务攻击下软件的可靠性和实时性；
i) 检测现场生产过程和设备状态信息与监控软件的显示信息的相符性；
j) 对监控软件和现场设备进行中间人攻击；
k) 检测监控软件内部功能模块间的数据流以及软件对输入数据的响应；
l) 检测监控软件栈溢出漏洞；
m) 检测监控软件堆溢出漏洞。

5.5.5 结果判定

5.5.4 a）- n）均为肯定，则信息系统符合本单元测评项要求。

5.6 DCS 组态软件检测

组态软件一般安装于工程师站，用于实现对DCS的应用组态，一个通用的DCS经过组态成为一个针对特定具体控制应用的可运行系统。组态软件采集和控制设备之间的数据交换，将来自设备的数据与计算机图形画面上的元素相联系，同时为使用者提供灵活多变的组态工具以适应不同领域的需求。

根据DCS对安全性、稳定性和实时性的要求，结合GB17859-1999 所列安全要素和GA/T 20271-2006关于信息系统安全功能要素的描述，本条款的目的在于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。

5.6.1 检测项

a) 软件合法性；
b) 通信完整性；
c) 身份鉴别；
d) 登录口令；

e） 输入验证；
f） 组态下载验证；
g） 拒绝服务；
h） 信息嗅探；
i） 内存漏洞。

5.6.2 检测方式

检查、测试。

5.6.3 检测对象

DCS工程师站。

5.6.4 检测实施

a） 检测组态软件授权属性；
b） 检测组态软件数字证书合法性；
c） 检测组态软件功能实现所需的组件或文件的完整性；
d） 检测组态软件对接收的外部数据的完整性验证；
e） 检测组态软件对用户的身份鉴别机制；
f） 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；
g） 通过构造不具有正确格式的恶意非法输入数据，以达到执行非授权命令或功能的目的，检测组态软件的响应；
h） 组态下载前是否具备安全验证的机制以防止非法组态的发生；
i） 检测拒绝服务攻击下软件的可靠性和实时性；
j） 检测组态软件内部功能模块间的数据流以及软件对输入数据的响应；
k） 检测组态软件栈溢出漏洞；
l） 检测组态软件堆溢出漏洞。

5.6.5 结果判定

5.6.4 a）- l）均为肯定，则信息系统符合本单元测评项要求。

6 DCS 网络通信协议安全风险与脆弱性检测

6.1 以太网协议通信机制检测

基于以太网实现的协议(HTTP、FTP/TFTP、Telnet、SMTP和SNMP)都具有不同程度的漏洞，它们是DCS中广泛的存在通信协议，应该对每种协议进行脆弱性检测。DCS以太网协议通信机制检测针对DCS过程监控层网络与企业管理层网络结构，以及协议服务的事件机制进行脆弱性检测。

6.1.1 检测项

a） 以太网协议的硬件实现；
b） 以太网协议的茁壮性。

6.1.2 检测方式

访谈、检查、测试。

6.1.3 检测对象

企业管理层网络、DCS过程监控层网络所应用的以太网协议。

6.1.4 检测实施

a) 许可的访问对象与 IP 地址、TCP/UDP 端口和状态的指定情况及其潜在的脆弱性；
b) 企业管理网络和过程监控层网络的连接方式及其潜在的脆弱性；
c) 过程监控层网络允许的协议在企业管理网络有使用情况及其潜在的脆弱性；
d) 所有由过程监控层发起的对企业管理网络的访问的源服务、目的服务和端口的控制情况及其潜在的脆弱性。
e) 企业管理网络允许的协议在过程监控层网络的使用情况及其潜在的脆弱性；
f) 历史数据库的访问通信对系统的影响程度；
g) 对所应用的以太网协议进行风暴/压力测试；
h) 对所应用的以太网协议进行模糊测试；
i) 对所应用的以太网协议进行语法测试。

6.1.5 结果判定

6.1.4 a）- i）均为肯定，则信息系统符合本单元测评项要求。

6.2 工业网络协议通信机制检测

现场设备层主要包括控制器与现场设备，控制器与现场设备之间通常采用现场总线相连，交互的数据主要是实时的现场数据及控制站的控制指令。常用的DCS工业网络通信协议有FF-H1，Profibus-DP，Profibus-PA，CAN，CANopen，DeviceNet，Modbus/TCP，EtherNet/IP，Interbus，工业无线协议（如HARTWireless）等。这些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会对网络实时性、可靠性、稳定性的影响出发。

6.2.1 检测项

a) 工业网络协议的硬件实现；
b) 工业网络协议的软件实现；
c) 工业网络协议的茁壮性。

6.2.2 检测方式

检查、测试。

6.2.3 检测对象

DCS控制站的主控器、工业交换机等嵌入式设备所应用的工业控制通信协议的软件。

6.2.4 检测实施

工业网络协议的硬件实现检测，至少应包括：

a) 物理层信号实现的相关功能；
b) 数据链路层实现的相关功能。

工业网络协议的软件实现检测，至少应包括：

a) 协议栈中的时钟同步机制安全检测；
b) 协议栈中的仲裁机制安全检测；
c) 协议栈中的错误校验机制安全检测；
d) 协议栈中的状态转换机制安全检测；
e) 协议栈中的调度算法安全检测；

工业网络协议的茁壮性检测，至少应包括：

a) 风暴/压力测试；
b) 模糊测试；
c) 语法测试。

6.2.5 结果判定

6.2.4 a）- j）均为肯定，则信息系统符合本单元测评项要求。

6.3 DCS 通信数据安全检测

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。

6.3.1 检测项

a) DCS 协议通信数据的存储完整性；
b) DCS 协议通信数据的传输完整性；
c) DCS 协议数据的传输保密性；
d) DCS 协议数据的可用性。

6.3.2 检测方式

测试。

6.3.3 检测对象

DCS协议数据。

6.3.4 检测实施

a) 是否对 DCS 中过程监控层网络和现场设备层网络中存储的协议数据具有完整性保证措施；
b) 是否对 DCS 中过程监控层网络和现场设备层网络中存储的协议数据具有完整性保证措施，当检测到完整性错误时，是否采取必要恢复、审计或报警措施，具体有哪些；
c) 应对被传输的 DCS 协议数据进行检测，检测传送或接收的 DCS 协议数据被篡改、删除、插入等的威胁；
d) 应对系统恢复被破坏的数据为原始的 DCS 协议数据的能力进行检测。
e) 应对记录 DCS 中重要的生产信息数据的存储资源进行保密性检测；
f) 应对 DCS 中的存储加密机制的安全性进行检测；
g) 应对 DCS 协议数据传输媒介和监控设备的安全机制进行检测；
h) 应对加密机制的安全性以及加密对系统的影响进行检测；
i) 当存储或传输数据受到破坏时，采取的保护或恢复机制具体有哪些。

6.3.5 结果判定

6.3.3中 a）- i）为肯定，则信息系统符合本单元测评项要求。

6.4 DCS 通信服务检测

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。

6.4.1 检测项

a) DCS 设备地址的唯一存在性；
b) DCS 设备属性的完整性与合法性；
c) DCS 设备可用性。

6.4.2 检测方式

访谈、检查与测试。

6.4.3 检测对象

DCS通信设备。

6.4.4 检测实施

a) 访问 DCS 工程师站技术人员，在系统组态完毕后是否对 DCS 系统中设备的物理地址或逻辑地址的存在性进行核实；
b) 访问 DCS 工程师站技术人员，是否对 DCS 中设备的物理或者逻辑地址的唯一性进行核实与确认；
c) 应测试 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，以测试其影响；
d) 应测试 DCS 设备，采取两个相同的设备地址以测试其冲突影响；
e) 是否有技术措施或安全策略对 DCS 设备地址信息进行管理；
f) 是否具有 DCS 设备的配置信息完整性保护措施；
g) 是否具有 DCS 设备的配置信息的访问和修改合法性保护措施；
h) 当 DCS 设备不能正常工作时，是否具备失效保护机制，机制如何运作。

6.4.5 结果判定

6.4.4 a）- h）为肯定，则信息系统符合本单元测评项要求。

6.5 DCS 状态机转换检测

DCS状态机转换检测根据状态机的历史执行数据和实时执行流程是否符合预先设定的执行逻辑，是否有异常情况改变协议状态执行流程来检测是否有异常数据和异常情况发生。

6.5.1 检测项

a) DCS 历史执行数据的可用性；
b) DCS 状态机转换功能。

6.5.2 检测方式

测试。

6.5.3 检测对象

工业网络通信协议栈。

6.5.4 检测实施

a) 对 DCS 历史执行数据的可用性是否有保证措施，具体有哪些；
b) 是否有采取措施对 DCS 状态机预先设定的执行逻辑的正确性进行保证，具体有哪些；
c) 是否有采取措施对协议状态执行流程进行监测，具体有哪些；
d) 是否有采取措施对协议状态转换过程中的数据的异常情况进行监测，具体有哪些。

6.5.5 结果判定

6.5.4 a）- d）为肯定，则信息系统符合本单元测评项要求。

参 考 文 献

[1] NIST SP 800-82 工业控制系统安全指南
[2] IEC 62443-1-1 工业通信网络-网络和系统信息安全 第1-1部分：术语、概念和模型
[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] GB/T 20984—2007 信息安全技术 信息安全风险评估规范