ICS 75.200
E 70
备案号：53453—2016

SY

中华人民共和国石油天然气行业标准

SY/T 7037—2016

油气输送管道监控与数据采集（SCADA）系统安全防护规范

Pipeline SCADA system security

2016－01－07 发布　　2016－06－01 实施

国家能源局　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009《标准化工作导则　第 1 部分：标准的结构和编写》给出的规则起草。

本标准使用翻译法等同采用 API Std 1164：2009《Pipeline SCADA system security》（英文版）。为了便于使用，本标准按照 GB/T 1.1—2009 和 GB/T 20000.2—2009 的要求做了下列一些编辑性修改：

——删除了 API Std 1164：2009（英文版）的特别声明、前言和参考文献；

——删除了“API 石油工业安全指南”；

——删除了附录 B 部分“根据美国能源部 21 个步骤提高 SCADA 网络安全防护水平”；

——删除了附录 B 部分“美国能源部文件中的 21 个步骤列表如下，以供参考”；

——删除了“NIST”的定义和缩写。

本标准由石油工程建设专业标准化委员会提出并归口。

本标准起草单位：中国石油天然气管道工程有限公司、北京油气调控中心、中国石油管道公司、中石化石油工程设计有限公司。

本标准主要起草人：聂中文、徐志强、汪涛、董旭、王怀义、田京山、高原、卜志军、邓东花、程德发、刘亮、王勇、莫巨华、张书勇、吴兆鹏、闫峰、颜辉、马永祥、尹明路。

油气输送管道监控与数据采集（SCADA）系统安全防护规范

1 范围

本标准为油气输送管道监控与数据采集（SCADA）系统提供了高水准的整体安全防护推荐作法。附录中提供了更详尽的细节描述和技术指导。按照本标准正文和附录的要求，可制定一套规范的安全防护操作方法。由于SCADA系统的复杂性，管道SCADA系统网络安全防护性能的提高，不是一个简单的过程或一次性事件，而是一个持续的过程，按照本标准正确实施整个过程可能需要数年时间。此外，SCADA系统升级可参照本标准，将本标准推荐的安全防护措施可作为新系统的内置应用，提升整个系统的安全性。

1.1 目的和目标

运营商的目标是对管道进行有效的控制，避免因运营商或其他方的行为对员工、环境、公众及客户等造成不良影响。SCADA安全防护程序宜通过以下方法，提高管道SCADA运行安全：

——分析可被未授权系统利用的SCADA系统漏洞；

——列出用于识别和分析未授权系统攻击SCADA系统漏洞的过程；

——提供用于强化核心架构的综合实践列表；

——提供行业内最佳实践案例。

1.2 角色和职责

运营商的高级管理人员应严格执行SCADA安全防护管理程序，保证能在各组织层面识别SCADA安全防护的各项责任。SCADA系统安全防护程序的涵盖范围包括运营商、业务合作伙伴、供应商、SCADA系统软硬件产品供货商和技术服务商。SCADA安全防护程序应形成SCADA安全防护计划文件，用于识别执行策略和规程的安全防护专家及从业者的任务和责任，并对SCADA领域中整个组织的计算机安全活动提供协调一致的安全防护。应规划和宣贯SCADA安全防护管理程序，以便所有实际影响或潜在影响SCADA系统安全防护的操作人员能够充分了解他们的安全任务和职责，并接受足够的培训以便安全地完成任务。SCADA安全防护程序的设计应确保正在执行的是网络安全的行业最优方案，并符合所有相关规范。

2 定义和缩略语

2.1 定义

下列定义适用于本文件。

2.1.1

访问控制列表 access control list（ACL）

每个对象配有一个权限列表。该列表明确了允许访问该对象的人员，以及允许在该对象上执行的操作。

2.1.2

后门 backdoor，trap door

由程序员编写，以正式或非正式的方式获得权限，来访问程序、在线服务或整个计算机系统的程序代码。

2.1.3

生物识别技术　biometrics

根据一个或多个固有的生理或行为特征，唯一地识别人员的方法。

2.1.4

保密信息　confidential

对企业的敏感信息进行分级，通过严格的安全防护避免未经授权的泄露、修改或破坏。

注：未经授权的泄露，修改或破坏，可能产生重大影响。本类信息需要更高等级的保证，以确保其准确性和完整性（见第6章）。

2.1.5

访问控制　controlled access

某区域或系统中的资源仅限于经授权的人员、用户、程序、流程或其他系统访问，未经授权拒绝访问。

2.1.6

数据中心　data center

用于安置计算机系统及相关部件的设施，如通信和储存系统。一般它包含冗余电源系统、冗余数据通信连接、环境控制和安全防护设备。

2.1.7

数据库管理系统　database management system（DBMS）

对基于多种数据模型的数据库进行管理的计算机软件。

2.1.8

深层防御　defense in depth

通过SCADA系统执行多层次和多类型防御策略的最优实践方案，在整个系统生命周期可处理人员、技术和操作的问题。

2.1.9

隔离区　demilitarized zone（DMZ）

隔离区是介于可信和不可信网络之间的缓冲区，它能监视并控制访问和数据传输（如图4所示）。

2.1.10

脱氧核糖核酸　deoxyribonucleic acid（DNA）

包含了所有已知生物体在生长和机能实现中起作用的遗传指令的一种核酸。

2.1.11

域名系统　domain name system

通过将易读的计算机主机名转换成IP地址，将域名与各种信息联系起来。

2.1.12

双宿计算机　dual-homed computer

具有连接多重网络或安全域网络接口的计算机。

注：这种计算机区别于冗余设置两个网络接口卡的计算机。

2.1.13

动态主机配置协议　dynamic host configuration protocol（DHCP）

为在IP网络中进行操作获得所需的参数，而在联网设备中所使用的一种协议。

2.1.14

消除　eliminated

去除或移除威胁。

2.1.15

增强型安全防护　enhanced security

高于正常级别的安全防护，包括但不限于：严密的或多重的身份验证、加密、包括物理和生物识别技术的多级访问控制。

2.1.16

外联网　extranet

企业内部网的一部分，它可延展到企业以外的用户。它也被描述为一个“理念”，企业内部网经常被人们看作与其他企业进行业务活动的一种途径，或是向客户售卖产品的一种途径。

2.1.17

设施　facility

坐落在同一地点，由单一的地理周界（通常用栅栏或其他屏障包围并且限制不受控制的访问）所确定的工厂、建筑物、结构，或者它们连续的结合体，用于运营商或承包商从事其管辖下的工作。

注：术语“设施”包括其地域周界内的土地（土壤）、地表水和地下水。

2.1.18

文件传输协议　file transfer protocol（FTP）

在互联网上进行文件传输的互联标准。

注：FTP 程序和实用工具用来从外部硬盘驱动器到允许 FTP 访问的远程服务器上传和下载网页、图形和其他文件。

2.1.19

防火墙　firewall

一套内置在网关服务器上对内部网络进行保护的计算机程序。

注：防火墙检查每一个网络数据包，以确定是否将其转发到目的地。防火墙通常安装在一个专门的与其他网络分开的设备上，从而任何进入请求都不能直接到达专有网络资源中。建议的最佳实践方案是至少具有状态检测或深度的数据包检测。

2.1.20

人机界面　human machine interface（HMI）

通常配有图形画面的计算机终端，实现人和终端设备之间的交互功能。

2.1.21

事故响应计划　incident response plan（IRP）

识别和记载规程的计划，该规程可检测、响应网络安全事故并将影响减至最小。

2.1.22

信息所有者　information owner

负责特定数据的归类、维护和安全防护的人。

2.1.23

即时通信　Instant Messaging（IM）

通过互联网或企业内部网，用于两人或多人之间数据和信息交换的实时通信系统。

2.1.24

内部　internal

那些可允许所有员工，以及可向运营商提供服务的承包商进入或使用的信息。只对运营商使用（见第 6 章）。

2.1.25

互联网控制消息协议　internet control message protocol（ICMP）

ICMP 包含错误、控制和信息的数据包，是 RFC 792 定义的 IP 协议的扩展。

2.1.26

互联网协议　internet protocol（IP）

一种封装在数据链路层的网络协议簇，例如以太网。

2.1.27

互联网服务提供商　internet service provider（ISP）

主要向客户提供互联网接入的企业。

2.1.28

企业内部网　intranet

在一个企业已建立的规则框架内的所有内部计算机网络。

注：企业内部网通常使用标准的网络技术，如以太网技术、TCP/IP 技术、网络浏览和网络服务技术。

2.1.29

入侵检测和防御系统　intrusion detection and prevention systems（IDPS）

广义上指基于 IDS（入侵检测系统）和 IPS（入侵防御系统）功能的网络安全系统，它展示了各项正在发展的技术并融合成为一系列的产品。

2.1.30

入侵检测系统　intrusion detection system（IDS）

一种针对计算机和网络的安全防护管理系统。IDS 可对来自不同地区和网络的信息进行收集并加以分析，识别可能存在的安全漏洞，它包括入侵和误用两种情形。

2.1.31

入侵防御系统　intrusion prevention system（IPS）

可接收 IDS（入侵检测系统）嗅探数据或扫描数据，使用分析程序和信息处理给出入侵结论，并做出适当的响应。与入侵保护系统相关的产品也都具有自我保护能力，能够保护与之有关的数据，防止对系统进行未经授权的访问或修改，确保授权行为的执行。

2.1.32

网际协议安全　IP security（IPsec）

由互联网工程任务组（IEFT）开发的协议，该协议能够对 IP 层面上的数据包交换提供安全支持。VPN 广泛使用 IPsec 技术。

注：IPsec 支持两种加密模式：传输和隧道。

——传输模式只对每个数据包中的数据部分加密，而对报文头则不加密。

——隧道模式则更加安全，隧道模式对报文头和数据部分都进行加密。在接收方，符合网际协议安全规则的设备对每个数据包都做加密处理。

2.1.33

专业监督　knowledgeable escort

经验丰富的专业人员，可指导非专业人员的工作。该人员应对所执行工作中可能存在的风险具有全面和深入的理解，并执行监督工作。

2.1.34

第二层隧道协议　layer two（2）tunneling protocol（L2TP）

PPP 的扩展，该协议使 ISP 能更可靠地操作 VPN。

注：第二层隧道协议融合了另外两种隧道协议（微软公司®[1]的 PPTP 协议和 Cisco 系统®[1]的 L2F 协议）的最好的功能。与 PPTP 类似，L2TP（第二层隧道协议）要求 ISP 的路由器必须支持该协议。

1）本术语仅用于举例。

2.1.35

局域网　local area network（LAN）

分布在限定区域内的一组计算机和关联设备，可通过通信连接实现互连和信息交换。

2.1.36

逻辑网络　logical network

SCADA 网络和企业网使用相同的基础设施，二者之间可自由传输数据的网络结构。

2.1.37

监视　monitoring

为实现维护和改进程序性标准及防护措施而进行的观察、监督及记录，包括监测异常情况。

2.1.38

网络文件系统　network file system（NFS）

允许用户在一个客户端计算机上通过网络访问文件的一种协议。

2.1.39

网络新闻传输协议　network news transfer protocol（NNTP）

一种互联网应用协议，主要用于阅读和发布文章，以及在新闻服务器间传递信息。

2.1.40

运营商　operator

拥有或经营管道设施的人员。

注：本标准中如无特殊说明，术语“管道运营商”和“运营商”含义相同。

2.1.41

点对点协议　point-to point-protocol（PPP）

在两个节点之间建立直接链接的数据链路层协议。

2.1.42

策略　policy

概述了特定需求或应遵循准则的文档。

注：在信息/网络安全防护领域，策略通常是覆盖单独某个区域的特定点。比如，一个“可接受使用的”策略应包含适当的使用计算机设备的规则和准则。

2.1.43

规程　procedure

将活动、步骤、决策或流程顺序文档化，按照编制的文档执行，可产生期望的结果。

2.1.44

过程控制网络　process control network（PCN）

在 SCADA 系统和测控单元之间传输指令和数据的网络。

2.1.45

可编程逻辑控制器　programmable logic controller（PLC）

一种用于工业过程自动化的计算机控制装置。

2.1.46

公共信息　public

适用于一般性质的信息，能与所有人共享，不需额外的任务或作业验证（见第 6 章）。

2.1.47

远程访问服务　remote access services（RAS）

通过任意硬件和软件组合，远程访问驻留在 SCADA 的网络设备上的工具或信息。

2.1.48

远程终端单元　remote terminal unit (RTU)

一种远程设备，可用来采集状态、报警和模拟信号数据，传输到 SCADA 系统，并将 SCADA 系统的控制信息传送到现场设备。

2.1.49

受限信息　restricted

适用于非敏感企业信息，仅限于可访问的合法业务。

注：未经授权而泄露、修改或破坏信息都可能产生不利影响。信息只在企业内部使用，或者在某些情况下与相关组织例如企业的业务合作伙伴使用（见第 6 章）。

2.1.50

风险评估　risk assessment

一种对安全和可靠操作的连续性造成风险的安全防护和安全问题的过程评估。

2.1.51

基于角色的应用　role-based applications

包含多层的功能应用。根据工作职能授权用户对不同层所必要的最小访问权限。

2.1.52

SCADA 供应商　SCADA vendor

开发和维护 SCADA 系统软件或/和硬件的商业实体或运营商。

2.1.53

安全外壳协议　secure shell (SSH)

一套命令和协议。用数字证书对“主机”和“客户端”进行认证，并对通信进行加密，确保安全防护。

2.1.54

安全套接层　secure sockets layer (SSL)

在网络计算环境中提供安全通信的加密协议，用于网页浏览、电子邮件、互联网传真、IM 和其他数据传输。

2.1.55

安全防护域/安全防护区　security domains/security zones

一个或多个通过防火墙与其他网络相隔离的区域。

2.1.56

安全防护计划　security plan

由管理层制定一系列的策略、规程或者操作要求，为安全防护问题及相关事件提供多层次的解决方法。

注：这种方法会包括评估、决策树、保护机制、响应和恢复时间，操作安全防护级别和重要资产识别等。一个安全防护计划通常应考虑人员、流程和技术。

2.1.57

串行通信　serial communication

一种通过计算机总线或其他通信信道每次按顺序发送 1bit 数据的通信方式。

注：通常的串行通信电气接口规范包括 EIA/TIA 232，422 和 485。

2.1.58

简单网络管理协议　simple network management protocol (SNMP)

一个网络管理的标准 TCP/IP 协议。网络管理员使用简单网络管理协议可对网络的可用性、性能参数和差错率进行监视。

注：SNMP 和网络设备工作需使用分布式的数据库，称作 MIB。所有的 SNMP 兼容设备都包含一个 MIB，用来提供设备的相关属性。在 MIB 中有些属性是固定的或者称作“硬编码”，其他属性值是动态的，根据设备上代理软件的运行进行计算。

2.1.59

强密码　strong passwords

按不可预知顺序排列并结合大、小写字母、数字和特殊符号组合的密码方式。

2.1.60

超级用户执行　superuser do（SUDO）

基于 UNIX®[2] 系统的功能，它提供了有效的方式，允许特殊用户使用系统根用户（最高）级别的特殊命令。

注：SUDO 同样也记录所有的命令和参数。

2.1.61

监控和数据采集　supervisory control and data acquisition（SCADA）

一系列计算机硬件及软件的组合，可用于发布命令及采集数据从而实现监视与控制（如图 1 所示）。

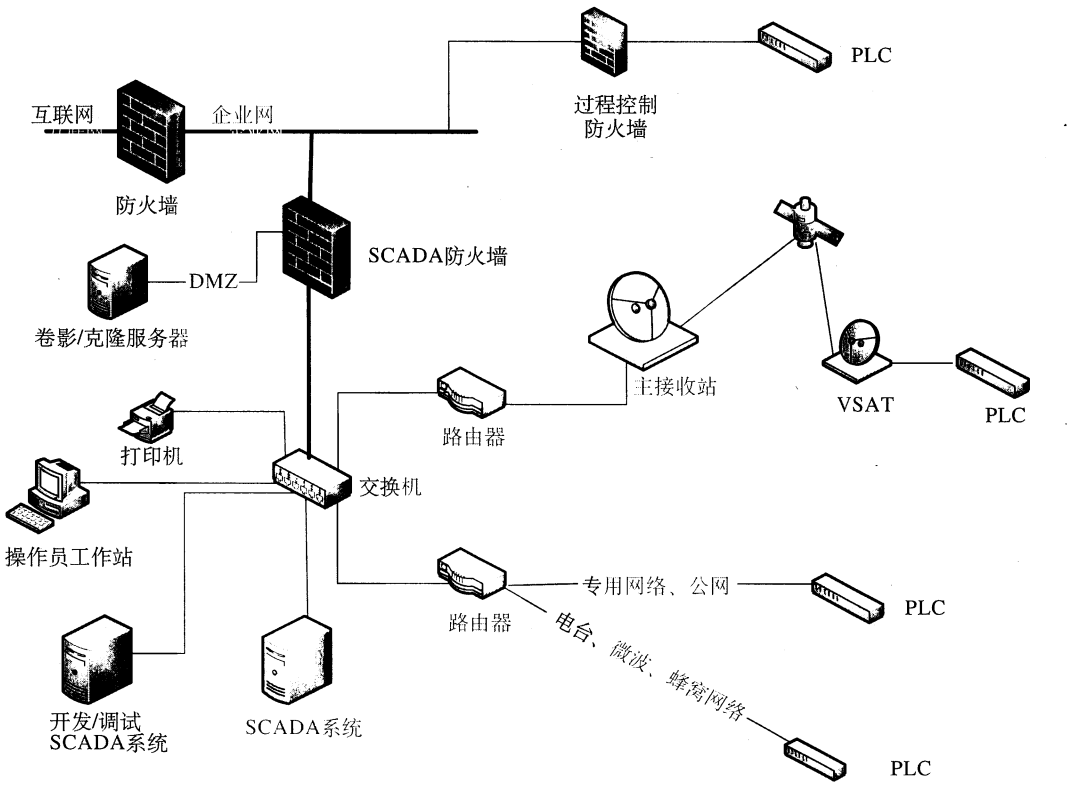

图 1　典型 SCADA 系统结构

2.1.62

通信中心　telecommunication center

一种安装有通信及网络设备，可连接独立终端设备、用户及其他设备的设施。

2.1.63

第三方　third party

2）本术语仅用于举例。

供应商、支持服务人员及其他公司。

2.1.64

传输控制协议/互联网协议　transmission control protocol/internet protocol (TCP/IP)

TCP 是 TCP/IP（传输控制协议/互联网协议）网络中的主协议。TCP 能使两台主机建立联系并进行数据交换，而 IP 仅处理数据包。

注：TCP 能保证数据的传输，也能保证数据包的发送方式与接受方式相同。

2.1.65

简单文件传输协议　trivial FTP (TFTP)

一种简单形式的 FTP，TFTP 协议使用“用户数据报文协议（UDP）”，而不具备任何安全防护特性，常用于引导无磁盘工作站、X 终端和路由器等。

2.1.66

公用设施　utilities

为控制系统提供的电、水、天然气及通信等服务。

2.1.67

虚拟专用网络　virtual private network (VPN)

在非可信任网络中使用逻辑、经验证和加密的链接，通过加密和其他安全防护方法确保仅允许授权用户进入网络，未经授权用户不能读取和下载数据。

2.1.68

语音 IP/IP 电话　voice over IP/IP telephony (VoIP/IPT)

使用 IP 网络管理和传输语音通话的技术。

2.1.69

漏洞评估　vulnerability assessment

对易暴露区域评估的技术和系统组件。

2.1.70

广域网　wide area network (WAN)

提供比局域网（LAN）更多独立用户的数据通信，并传输更大区域范围的物理或逻辑网络。

2.2　缩略语

下列缩略语适用于本文件。

ACL：access control list 访问控制列表

BCP：business continuity plan 业务连续性计划

DBMS：database management system 数据库管理系统

DHCP：dynamic host configuration protocol 动态主机配置协议

DMZ：demilitarized zone 隔离区

DNA：deoxyribonucleic acid 脱氧核糖核酸

DRP：disaster recovery plan 灾难恢复计划

FTP：file transfer protocol 文件传输协议

HID：host intrusion detection 主机入侵检测

HMI：human machine interface 人机界面

ICMP：internet control message protocol 互联网控制消息协议

IDPS：intrusion detection and prevention system 入侵检测和防御系统

IDS：intrusion detection systems 入侵检测系统

IEFT：internet engineering task force 互联网工程任务组

IIS：internet information services 互联网信息服务

IM：instant messaging 即时通信

IP：internet protocol 互联网协议

IPS：intrusion prevention system 入侵防范系统

IPsec：IP security 互联网协议安全

IRP：incident response plan 事故响应计划

ISDN：integrated service digital network 综合业务数字网

ISP：internet service provider 互联网服务提供商

LAN：local area network 局域网

L2F：layer two (2) forwarding 第二层转发协议

L2TP：layer two (2) tunneling protocol 第二层隧道协议

MIB：management information base 管理信息库

NID：network file system 网络入侵检测

NFS：network intrusion detection 网络文件系统所

NNTP：network news transfer protocol 网络新闻传输协议

PBX：private brand exchange 专用分组交换机

PC：personal computer 个人计算机

PCN：process control network 过程控制网络

PLC：programmable logic controller 可编程逻辑控制器

PPP：point - to - point protocol 点对点协议

RAS：remote access services 远程访问服务

RSA：an algorithm for public - key cryptography，developed by Rivest，Shamir and Adleman (surnames) 由 Rivest，Shamir 和 Adleman 开发的公钥加密算法

RTU：remote terminal unit 远程终端单元

SCADA：supervisory control and data acquisition 监控与数据采集

SMTP：simple mail transfer protocol 简单邮件传输协议

SNMP：simple network management protocol 简单网络管理协议

SSH：secure shell 安全外壳协议

SSL：secure sockets layer 安全套接层

SUDO：super user do 超级用户执行

TCP/IP：transmission control protocol/internet protocol 传输控制协议/互联

TFTP：trivial FTP 简单文件传输协议

TIA：Telecommunications Industry Association 电信工业协会

UDP：user datagram protocol 用户数据报协议网协议

VoIP/IPT：voice over IP/IP telephony 语音 IP/IP 电话

VPN：virtual private network 虚拟专用网络

VSAT：very small aperture terminal satellite 甚小口径卫星通信终端

WAN：wide area network 广域网

WINS：windows internet name service Windows 互联网命名服务

3 系统管理

运营商应制定一套 SCADA 安全防护管理程序，该程序是在本标准的指导下，为完善和完成管道

安全防护计划所定义的策略和规程。

3.1 人员

运营商应制定具有人员安全防护措施的联系和培训策略，该策略规定角色、职责及培训计划，从而保证访问 SCADA 系统的人员对潜在风险和个人安全防护责任保持较高的意识。

人员应：

——熟知正在处理信息的性质；

——熟知信息的安全防护；

——熟知信息的正确分类；

——熟知如何报告和应对潜在威胁。

运营商应制定包括系统管理员、安全协调员、SCADA 系统技术支持人员和操作人员等关键人员的岗位职责。员工应遵循各自岗位职责要求。

运营商应制定一套流程，确保管理 SCADA 系统的员工具有资质，并能达到企业规定的安全防护要求。

3.2 安全防护策略

运营商应制定安全防护策略，通过执行安全防护计划来保证安全和可靠的操作。

3.3 风险和漏洞评估

运营商应定期进行风险和漏洞评估。这些评估可确保系统在整个生命周期中的安全性和可操作性。有许多外部参考和指南可用于指导这类评估。

3.4 业务连续性计划（BCP）

BCP 是为系统的中断做准备，是指渡过异常事件或异常事件后恢复的能力。BCP 是安全防护计划的一部分，包括人员、流程和技术。“人员”包括关键员工在危机期间（响应）和在危险期后（恢复）需要采取的行动。“流程”是恢复的重要操作，用来保证安全和业务连续性。“技术”是指支持这些重要流程并促进响应的技术，恢复阶段的技术也应予以考虑。业务连续性和恢复计划应是衡量系统可用性的一部分。

运营商应建立 BCP，以解决可预见的对 SCADA 系统的干扰，特别是那些涉及管道控制设施的干扰。BCP 应包含运营商管理层所识别的管道资产安全运行、有记录并可恢复的目标。BCP 应包含实现恢复目标所需的所有要素，应包含重要系统备份和恢复程序。

运营商的 BCP 应记录 BCP 恢复团队的角色和职责。该团队应包含成功执行 BCP 所必须的所有人员。该团队应在指定时间间隔内测试、运行并不断完善恢复程序。

BCP 应能保证管道连续安全的运行。由于许多潜在风险存在于个别的控制设施，运营商的 BCP 应包括备份控制设施，在主控制设施不能工作或不可用的条件下保证安全和可靠地运行管道资产。在准备阶段、中断期间和之后应考虑访问控制。

BCP 的要素包括灾难恢复计划（DRP）。DRP 的基本特征和功能如下（不限于此）：

——备份数据的存储与恢复；

——应急人员、供应商、服务提供商和紧急救援等联系人员名单；

——设施维护和餐饮服务；

——人员；

——软件许可；

——特定的硬件，例如计算机平台、网络设备、打印机、传真机和电信设备；

——操作系统和基础应用软件的安装介质和安装说明；
——通信系统、语音和数据链路服务商；
——第三方供应商。

3.5 事故响应计划（IRP）

运营商应建立 IRP，该计划定义和记录用于检测、响应网络安全防护事故和使其影响最小化的程序。该计划应包含运营商管理人员的输入和许可，还应包括所有可能受网络安全防护事故影响或有责任响应网络安全防护事故的功能组。该计划应包括对筹划、响应和恢复等阶段各方面问题的识别。该计划应包括所有相关的人员和职责清单，以列表方式提供事故响应小组成员的姓名和联系信息。

应为 IRP 所有相关责任人员建立培训计划。IRP 应定期测试和评估，确保对网络安全防护事故有准备、有预案和有记录。

3.6 变更管理

变更管理流程规定具体的策略和规程，用于管理 SCADA 系统的所有组件的安装、配置和维护的变更。SCADA 系统包括但不局限于系统主机、历史服务器、可编程逻辑控制器/远程终端单元（PLC/RTU）和其他现场设备、人机界面（HMI）工作站、认证和网络管理/监视服务器、网络基础设备（路由器、交换机、防火墙）及其相关的操作系统和软件。运营商应制定并发布变更管理计划，实现 SCADA 系统的变更管理。该计划应明确说明运营商变更管理的目标，保证 SCADA 系统的可用性、完整性和保密性。应定期审查和更新变更管理计划，并且当组织、人员或技术变化时需更新该计划。

变更管理计划应为 SCADA 系统的所有组件制定一个基线配置。基线配置文件应记录 SCADA 系统组件的所有信息，用于运营商在 BCP 规定时间内重建组件。SCADA 系统发生变更时，应记录以及更新基线配置文件。

基线配置文件的任何计划性变更应包括详细的“撤销”或“回退”程序，如变更执行过程中遇到意外影响或故障，可用于恢复基线配置文件。所有 SCADA 系统的变更在投运前，应先在开发或测试环境中执行和评估。

变更管理计划应规定策略和规程，用于计划、传达、记录、批准、执行和审查 SCADA 系统基线配置文件的所有变更。应明确规定所有相关人员的角色和职责，以及变更管理中使用的记录和通信方式。应切实解决操作人员的健康、安全防护和安全要求，以及人力资源和业务需求。应仔细调整该程序，反映基线配置文件变更对 SCADA 系统带来的相对风险。应包括有效的对变更是否有损于 SCADA 系统的操作或安全性能的验证程序。

3.7 操作系统和应用程序更新

由于系统的复杂性，操作系统和应用软件不具备固有的安全性。此外，计算和网络环境的不断变化会持续地暴露新的漏洞，供应商通过发布补丁程序、服务包和应用程序升级解决这些问题。通常有必要安装补丁程序和更新，保持系统的稳定性和安全性，安装前应权衡在实时系统中使用补丁程序和更新的风险与目前漏洞所带来的风险的大小。在应用软件修改时，为防止产生操作安全防护问题和 SCADA 系统安全问题，应采取以下预防措施：

——仅安装 SCADA 系统供应商核准的软件；
——安装前，任何更新应由 SCADA 系统供应商进行认证；
——更新时，应分析运行环境的适用性；
——宜从 SCADA 系统供应商处获得更新文件的安装程序；
——不应直接从互联网上更新；

——在安装到生产环境之前，应在离线测试环境中测试更新程序；

——系统修改安装到生产环境前，应进行功能测试；

——系统修改完成后，应进行安全防护合规性审查，保证 SCADA 系统仍然符合运营商的安全防护策略。

对于本标准，开发和维护 SCADA 系统的内部数据的运营商被认为是 SCADA 供应商。这些措施应与运营商的变更管理计划一致。

3.8 应用与软件限制

SCADA 系统网络主要用于支持采用低宽带要求的高效协议和有限传输延迟容错能力的专用控制系统。由于这些网络分布范围广，加之历史上广域网（WAN）的接入比较昂贵，所以通常都是按照最小的带宽进行设计。由于此类原因，除 SCADA 系统网络外，其他协议、应用程序或通信软件包应注意保持 SCADA 系统的可用性。SCADA 系统不应添加对于管道操作及 SCADA 网络基础维护不必要的其他协议、应用程序或软件。SCADA 系统网络应拒绝商业业务软件及信息服务，例如接入互联网。使用电子邮件的系统事件或报警通知应采取适当的安全防护。SCADA 系统中不可添加盗版或者非法软件。因为现代服务器和软件包能大量消耗 WAN 容量，这是以牺牲 SCADA 网络通畅为代价的，所以 SCADA 系统网络中添加的任何新协议和应用程序应在测试或开发环境中运行，评估对 SCADA 系统性能的潜在损害，特别是对带宽的潜在损害。

4 物理安全防护

重要管道输送基础设施的运营商应采取措施和控制方法，用来拒绝未经授权的人员访问。以下概述了一些控制室物理安全防护的有效措施：

运营商应制定并维护一种安全防护策略和相关规程，要求对具有 SCADA 系统设施访问权限的所有人员进行定期安全防护审查。

运营商应为其控制中心的操作控制公用设施制定并维护安全防护计划。这些公用设施包括但不限于配电系统、不间断电源（UPS）以及发电设备。

运营商应为其控制的 SCADA 系统网络基础设施制定并维护安全防护计划。应保证所有网络和计算端口访问权限的安全性，并停用任何未使用的端口。

运营商应为其所有控制 SCADA 系统所属的设施进行风险评估，同时应制定这些设备访问控制的流程。宜考虑在无人站场，例如阀组区、泵站、计量设施等处安装入侵检测设备。未经授权的人员应由授权人员陪护访问 SCADA 系统设施。

5 系统访问控制

系统访问控制涉及用户账户、身份验证和授权。以下各节将确定和说明 SCADA 系统的特定要求。

5.1 限制访问

多层访问和多因素身份验证能够比单层系统更好地保护系统免受危害。在多层系统中，因为每一层功能是独立的，所以某层失效不会危及整个系统。使用深层防御，多层安全防护系统能够大大减少系统受损的概率。

5.2 用户账户

SCADA 系统通常拥有两层用户账户：分别为操作系统层（UNIX®[3] 或 Windows®[3]）和应用层，应用层可设置多种操作权限。每层均应具有一份访问控制列表（ACL）。允许访问 SCADA 系统或资源的用户应具有有效的业务需求，确保用户只能访问其所需要的数据。

5.3 操作系统账户

操作系统的“系统管理员”账户的权限允许其完全控制一个工作站，能修改或删除工作站上的任何文件或设备。应严格控制访问“系统管理员”账户。只有当个人需要这个账户提供的功能时，才应获取访问权限。在如 UNIX®[3] 操作系统中，使用“超级用户执行（SUDO）”命令能提供一些系统管理员（root）账户功能而非全部功能。其他操作系统也有类似的工具。

SCADA 系统操作控制台应一直保持登录状态，监视管线的相关操作。每天 24h/每周 7d 一直工作的操作控制台可使用共享的操作系统账户，控制台通常通过物理安全防护来保护，并且每天24h/每周 7d 一直有人值守。应定期审查这些共享的用户账户的使用，并将其限定于特定的控制台操作。

SCADA 供应商有时会使用或创建操作系统账户，使其能监视和维护 SCADA 系统。这些账户可能为入侵者提供方便。所有操作系统账户应保证安全，并使用强密码或生物识别技术。

有些操作系统和/或应用程序使用内部账户。这些账户通常有操作系统的强大访问权限。应审查这些内部账户，保证适当的安全防护级别设置，防止非授权用户使用该账户。

5.4 SCADA 系统账户

SCADA 系统应用程序的所有用户应拥有各自唯一的账户，且需要密码或生物识别技术访问系统。唯一的账户有助于追踪系统上的异常活动。

由于存在潜在的操作风险，一些运营商不使用各自的账户。考虑使用交互方式登录时，运营商应寻求使用最小潜在操作风险的流程，从而提高系统安全防护。所有非控制台式的 SCADA 系统账户应使用增强型安全防护措施。

不以操作为目的工作站/个人计算机（PC）应考虑使用非活动计时器，离开终端超过规定时间的用户将自动注销。

5.5 密码管理

强密码方案是一个良好的安全防护系统的基础。强密码方案应包括以下一些属性：

——定期更改；

——密码的最小长度要求；

——禁止使用重复密码、常用词、纯数字或纯字母模式；

——密码应区分大小写；

——数次尝试密码失败后应锁定；

——首次登录更换初始或默认账户密码。

所有系统/设备宜具备上述这些特征。计算机系统为简化日常活动提供了许多工具和技术，包括脚本文件、别名和快捷键。考虑到入侵者能读取这些文件，并使用密码操纵该系统，应保证密码不会被嵌入到这些工具中。同时，由于 SCADA 系统的源代码也可能拥有硬编码密码。SCADA 系统安全防护策略应阻止/禁止将敏感密码嵌入源代码、脚本、别名、快捷键中。如必须嵌入，则应使用加密

3）本术语仅用于举例。

技术。尽量减少其他用户访问嵌入的密码以保证所有源代码的安全。密码应由用户在每次登录时输入，而不是保存密码进行自动登录。

5.6 生物识别技术

生物识别技术是一种基于一个或多个内在生理或行为特征来识别人员唯一属性，用于访问安全网站、信息或应用程序的应用。生物识别技术包括：

——生理学：脸、指纹、手部特征、虹膜、脱氧核糖核酸（DNA）；

——行为：按键输入、签名、声音。

在 SCADA 系统和过程控制网络（PCN）系统内使用生物识别技术有以下几个原因：

——主动识别一个特定的个体（推测的）；

——方便性：不需随身携带徽章、密码或安全防护令牌设备。

利用多种身份识别的优势和支持深层防御的生物识别技术成为有价值的第二种输入方式。生物识别技术例如拇指指纹识别能够应用在使用账户/密码进行访问控制的地方。

正确使用生物识别技术有助于增强网络安全防护，但生物识别技术控制并非绝对可靠，它们能受到损害。研究表明指纹、虹膜、视网膜扫描都具有很高的欺骗可能性。生物识别技术是一项新兴技术，使用前应考虑实施策略、交叉错误率以及平台可用性。

5.7 禁止非必要的服务

应删除或禁用 SCADA 系统不使用的操作系统服务，减少被攻击机制利用的风险。当操作系统安装在服务器上时，有些服务可能是默认运行但 SCADA 系统并不使用，这些服务应被禁用，防止被不恰当的使用。其他服务应进行风险评估，评估其运行收益与被潜在利用的风险。禁用的操作系统服务一般包括：

——自动更新；

——动态主机配置协议（DHCP）服务；

——分布式文件系统；

——DNS 客户端；

——文件传输协议（FTP）服务；

——IIS 管理服务；

——索引服务；

——即时通信（IM）；

——网络文件系统（NFS）；

——网络新闻传输协议（NNTP）服务；

——远程运行本地查看服务（remsh）；

——远程执行命令服务（Rexec）；

——简单邮件传输协议（SMTP）；

——远程登录；

——Windows 互联网命名服务（WINS）；

——Web 发布服务。

5.8 操作系统工具

如 UNIX®[4] 操作系统的远程 Shell、远程登录、远程复制功能在工作站之间允许建立“信任”连

4）本术语仅用于举例。

接。如该功能可用，已成功登录到一台工作站上的用户能访问网络上其他工作站。操作系统提供的远程功能应仅在必要时使用。对于大多数用户来说，宜禁用此功能。当需要远程功能时，使用安全外壳协议（SSH）等工具能提高远程功能的安全防护。

FTP 允许文件在工作站/PC 上发送或接收。如没有适当的安全措施，入侵者可使用这个工具来安装程序以控制工作站/PC。应严格控制在 SCADA 系统上使用 FTP。系统管理员账户不应被授予 FTP 功能。需要 FTP 功能时，使用安全工具能提高 FTP 功能的安全性。

在操作系统环境下，一般通过外壳（shell）或窗口（windows）可访问 SCADA 系统的任何功能。除了预定的功能，能使用外壳或窗口作为接入点，访问 SCADA 系统的其余功能。使用安全外壳、窗口工具以及良好的账户设计将限制访问系统的其他部分。

5.9 设备访问

除了工作站和个人计算机外，在网络上还有许多设备，例如网络交换机、路由器、防火墙、终端服务器，以及设置在现场的变送器、PLC、流量计算机等。这些设备多数设有出厂默认密码或空密码，入侵者能通过这些密码操纵这些设备，获得 SCADA 系统访问权限。为保证安全，这些设备宜设置强密码，不应使用由供应商提供的默认密码。也应考虑为这些设备更改与供应商预设密码不一样的 ID 或账户。

5.10 人员管理

尽管本项属于管理系统部分，但重申这些还是很重要的：作为安全防护计划的一部分，应具有定期审查和审计 SCADA 系统和/或设备账户的规定；且应具有及时处理离职员工或承包商信息的规定。

6 信息发布

某些类型信息的共享会增加对 SCADA 系统的不恰当访问和误用的潜在可能。因此，建议对所有类型的 SCADA 系统中的信息，在共享之前都要根据运营商安全防护计划和程序进行分析和分类，并确定具体岗位或角色能共享的信息类型。当保密/受限信息必须同第三方人员共享时，应考虑采用保密协议、背景筛选、安全程序意识培训等措施。

运营商应遵照企业既定策略来处理信息。

推荐至少把 SCADA 系统的信息分类为三个级别。运营商应基于以下参考确定信息级别：

——保密信息；

——受限信息；

——公共信息。

6.1 保密信息

保密信息只应由那些“须知”的人员共享。只应在为了达到某个工作或任务的要求而需要知道这些信息的情况下，才能访问并使用保密信息。保密信息不是被广泛共享的信息，应高度保护。SCADA 系统的特定细节应被分类为保密信息，列为保密信息应得到最可靠措施的保护。

保密信息示例如下（不限于此）：

——访问规则设置；

——地址表；

——PLC 寄存器分配；

——系统图；

——系统配置；

——用户账户信息。

6.2 受限信息

受限信息共享范围可能比保密信息更广泛，仍需受到保护。受限信息虽然在工作或任务需要时能访问或使用，但这类信息仍然不是所有人能够全部获得的信息。

受限信息示例如下（不限于此）：

——通信媒介；

——使用的通信协议；

——设备清单；

——安全防护计划。

6.3 公共信息

公共信息是一般性的，能与所有人共享。公共信息共享仅用于了解，并不是满足工作或任务的需要。

鉴于 SCADA 系统的重要特性，极少量属于 SCADA 系统的信息可被分类为公共信息。归类为公共信息的 SCADA 系统信息应通过管理层的审查，并应进行信息发布风险评估。

7 网络设计和数据交换

以往 SCADA 系统被隔离并独立于其他商业业务功能和应用，但是随着技术的进步，系统互连成为普遍现象。允许业务系统访问 SCADA 系统具有很多优点，以下各节阐述如何实现系统的安全互联。

7.1 网络设计

很多方法能实现 SCADA 系统和相关业务系统的连接，这些连接应被限制在特定的服务或设备上，且应是安全的。值得注意的是任何设备接入 PCN 时，应做网络风险和设备连接风险评估。

7.1.1 企业网络与 SCADA 网络的互联

在 SCADA 系统和业务系统共享相同的逻辑网络或在两个网络之间的链路是开放的路由时（如图 2 所示），这种连接会使 SCADA 系统容易受到主动或无意识的攻击。运营商应考虑将 SCADA 系统网络进行隔离。

7.1.2 通信分界点

通信分界点应设置在物理上安全的地点，减少未经授权人员的访问。

7.1.3 防火墙

被监视和维护的防火墙为网络层和应用层提供了外围防护。SCADA 网络和企业网连接时应使用防火墙。防火墙应阻止所有非必需的访问，而只允许安全防护策略准许的重要访问（如图 3 所示）。

7.1.4 隔离区（DMZ）

DMZ 是一种位于 SCADA 系统网络防火墙和企业网络防火墙之间的独立网络（如图 4 所示）。与 SCADA 系统网络和企业网都通信的计算机或其他设备应放置在 DMZ 网络中，这样能确保 SCADA 网络和企业网络之间不存在直接的通信。

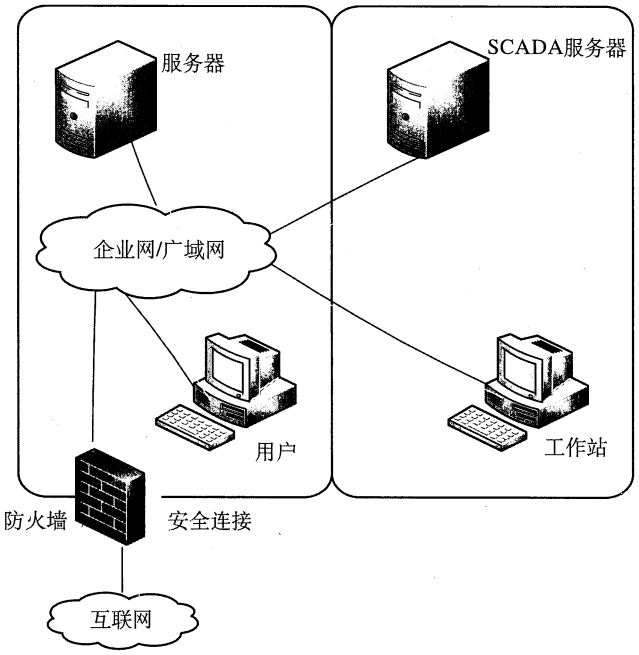

图 2　典型非隔离应用——不推荐

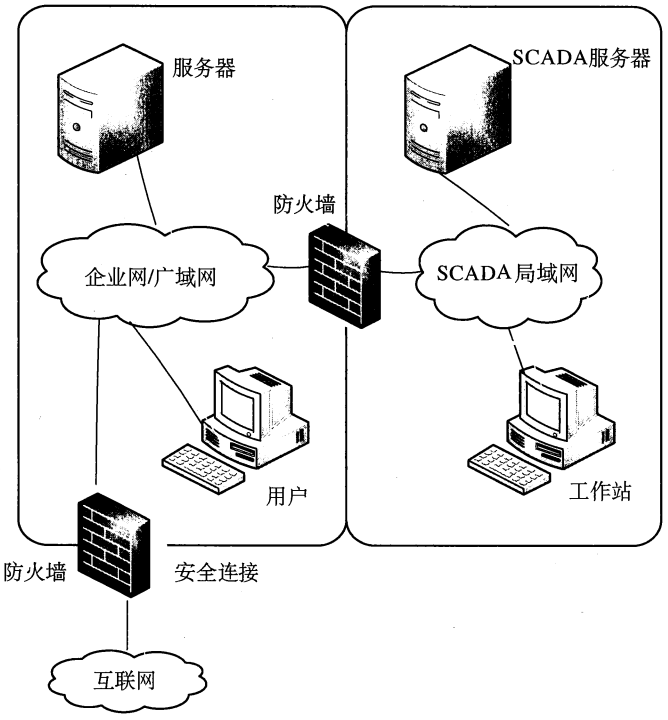

图 3　典型防火墙隔离应用——最小隔离

7.1.5　双宿计算机

连接到两个不同安全域的双宿计算机（专业的防火墙除外）不应在 SCADA 系统网络内使用。除非具有专业防火墙功能，否则有可能通过双宿计算机绕过网络安全防护隔离（如图 5 所示）。

7.2　网络管理

网络管理要求记录有关网络设计和操作的最新文档和图表。网络管理流程应与整体变更管理计划

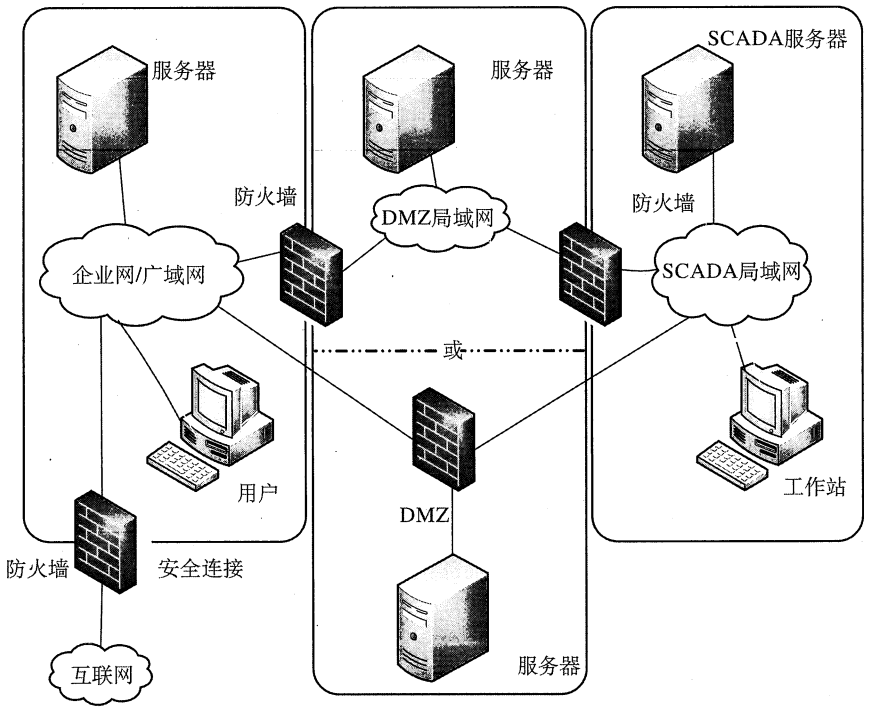

图 4　典型隔离区（DMZ）应用——推荐

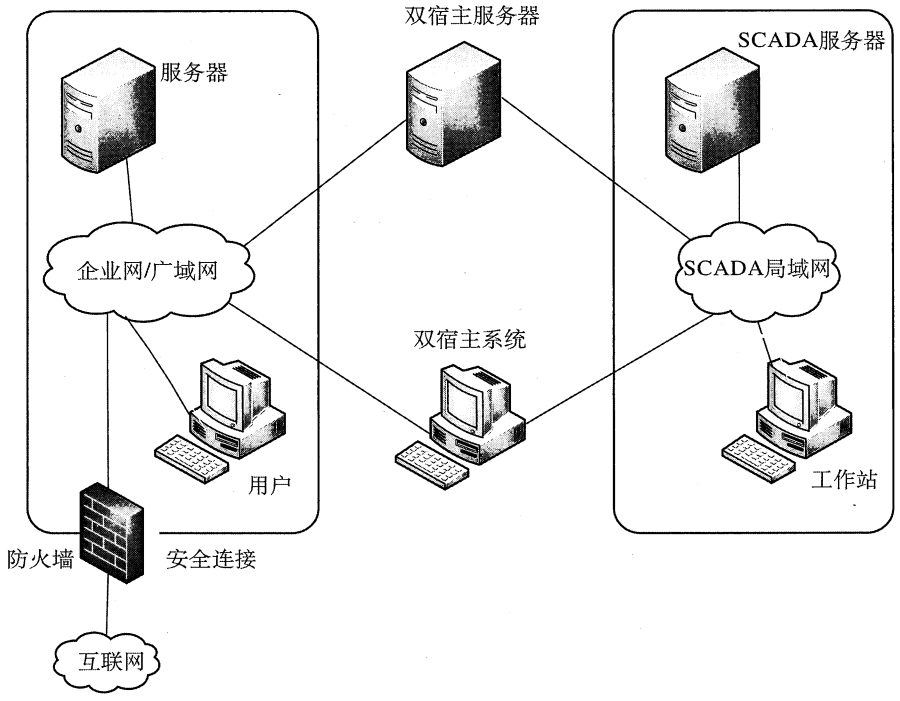

图 5　典型双宿计算机桥接应用——不推荐

相一致。

运营商应保证将网络设备（例如路由器、交换机、防火墙）的配置文件正确地存档，保证存档文件与运行设备的配置相符。运营商应定期审查这些网络设备中运行的软件版本，审查和评估任何已知的漏洞并且按照需求进行修复。

运营商应通过监视网络流量和活动来管理网络，避免对非托管设备的使用，同时监视网络的使用和流量。运营商应定期地审查网络日志文件、错误信息和其他事件，来跟踪潜在的安全防护漏洞或其

他的异常行为。

能通过适当的工具加强网络设备管理。

7.2.1 网络监视

在SCADA或控制系统中，对于网络的监视不存在普遍接受的最好方式，应使用包含防火墙之内的组合技术来加强网络安全防护和管理。基于传输控制协议/互联网协议（TCP/IP）的网络已经成为基于工业标准互联的推进者。这种相对的易用性在网络管理和安全防护方面面临许多挑战。

当超出技术的使用范围，应按照安全防护计划中的基本规则对所产生的数据进行审查。若不能实现，将无法在管理或安全防护上有任何提高。多源信息的聚合和关联，以及将这些信息以有意义的方式呈现出来是一个必要及繁重的任务，并能够通过合适的工具协助完成。

7.2.2 网络安全防护

除了使用防火墙、流量监视和事件日志外，那些专注于特定安全防护的技术也应考虑使用，如：

——入侵检测和防御；

——文件审计和控制。

7.2.2.1 入侵检测和防御系统（IDPS）

运营商应评估IDPS的使用，监视网络的各种行为，可识别异常或不受欢迎的事件。IDPS所使用的方法包括：

——网络监视：在网段或设备处检测，发现网络和应用协议中的可疑行为（也称为NID——网络入侵检测）；

——无线检测：通过检测无线网络的流量信息，发现在协议中的可疑行为；

——行为或启发式检测：通过网络检测不正常的流量；

——主机监视：通过对作为主机的计算机进行检测，查找可疑行为（也称为HID——主机入侵检测）。

由于SCADA网络（通常认为与大多数传统的业务系统不同）的本质和所使用独特的协议，使用IDPS时应仔细检查，确保系统的安全和可靠操作，不会被IDPS的自动行为所危害。在使用入侵防御系统（IPS）之前，应首先进行测试和审查。

7.2.2.2 文件审计和控制

运营商应监视文档和日志的变更，保证SCADA系统和数据的完整性。应监视异常修改的文件（包含操作系统、应用程序和配置文件），能检测和记录该修改。能通过合适的工具加强文件的审计和控制管理。

7.3 数据交换

众多业务需求推动了SCADA网络和其他网络的互联，如SCADA安全防护程序允许这类连接，则存在重大的网络安全防护风险。应分析该风险，按照安全防护程序导则，提前采取适当的预防措施。作为这项要求的一部分，还包括确认SCADA系统安全防护风险时，应完善策略和程序，并使企业和外部组织的响应达成一致。

7.3.1 SCADA控制中心的运行设备、数据中心和通信中心的连接

通常推荐将控制中心的操作设备放在离SCADA数据和通信系统尽可能近的地方。系统设计应确保SCADA操作员具有连接SCADA系统的能力，同时SCADA系统服务器与远程管道站场通信连接

不会中断。

7.3.2 SCADA 系统和企业网的连接

除操作需求外，相关企业对于 SCADA 和 PCN 数据的使用越来越规范。应考虑确保 SCADA 系统业务所用数据和网络保持可靠并且不受相关数据采集的影响。除非操作需要，被其他相关企业所访问的系统应是一个隔离的系统，而不是运行操作的系统。隔离的安全防护区域或子网，例如 DMZ，用来复制系统数据并安全地提供数据给相关用户使用。在 SCADA 系统和复制系统及 DMZ 和其他网络设备之间，应采用防火墙等适当的网络安全防护措施。

7.3.3 SCADA 系统和业务合作伙伴的 SCADA 系统间的连接

在多数情况下，需要将一个企业 SCADA 系统的控制数据和另一个企业的 SCADA 系统进行通信。这些数据包括但不局限于：关断请求、测量信息、阀门状态等。这些信息能通过不同的方式发送，例如主机到主机、PLC 到 PLC 等。当需要此类通信时，运营商应相互开发安全的通信方式。

7.3.4 与所支持的第三方连接

第三方能够对所售的系统进行支持是很重要的，在某些情况下，他们会因此要求访问 SCADA 系统。第三方访问 SCADA 系统的方法包括通过外联网、互联网、调制解调器等。第三方连接应严格控制并通过授权的方法确保安全。

应按照运营商的安全防护策略对第三方连接进行监视，供应商有时需要通过网络访问对 SCADA 系统进行支持，这些访问应通过防火墙和其他安全防护设备来进行控制。访问首先应被分配到安全的相关网络，然后授权通过这个网络来访问 SCADA 系统。在供货商完成其工作后，系统管理员通过监管及时取消所给予的访问权限。应使用防火墙将 SCADA 系统网络与互联网分隔开。

7.3.5 互联网和企业网访问

SCADA 系统不应直接访问企业网资源或互联网。若要访问非信任资源，推荐提供一个独立的专门用于业务用途的工作站，工作站连接到一个不与 SCADA 网络或 PCN 连接的网段，例如收发邮件或网络浏览。

7.3.6 语音 IP/IP 电话（VoIP/IPT）

商业上已经采用 VoIP 来降低通信费用。当一个物理通信链路与非 SCADA 用户共享时，不推荐在 SCADA 系统中使用 VoIP。同时，VoIP 可能使用在 SCADA 网络内部来提供重要任务服务，如 VoIP 的使用要求和上面所述一致，则应通过额外的控制方法来保护和隔离语音流量。VoIP 流量不应影响 SCADA 流量传输。

7.3.7 即时通信（IM）

商业上通常使用 IM 作为重要的业务交流工具。与 IM 系统相关联的风险包括间谍软件、木马程序、病毒、蠕虫攻击、垃圾邮件和重要或相关信息的丢失等。基于互联网的 IM 系统不宜在 SCADA 系统中使用。如企业策略需要使用 IM，则应采取控制手段来保证 IM 系统不会妨碍 SCADA 系统。应使用监视系统避免此类风险。如使用 IM，应仅用于通信，宜禁用文件共享。

7.3.8 无线网络

在使用无线网络前，应对其用途进行仔细评估，同时也应对其所带来的风险进行评估。对 PCN 和/或 SCADA 系统来说，无线网络应具有更高等级的安全防护。因此，应评估执行风险以比较使用

无线联网的收益和带来的潜在风险。这些技术可能使 SCADA 系统的数据在不确定的地理距离内传输，而且超出了本地的任何物理安全防护措施。在无线网络中应使用规范的网络管理措施，例如加密和防火墙隔离等。另外，应考虑无线网络控制技术。这些技术包括但不局限于：安全协议、增强型认证、隧道技术和控制访问点等。

应对无线设备进行物理访问控制。同时，应保护好网络基础设施，防止无线技术中的未授权入侵。无线连接应包含在网络文档、策略和程序中。无线网络技术更新频繁，安全性取决于所用设备的现状及其保护措施。

7.3.9 音频/视频会议

音频和视频会议是一种能与远方人员联系及促进双方业务交流的通信方式。考虑到安全防护，以及音频和视频会议带宽的要求，这些技术不宜在 SCADA 通信网络中使用。

当需要在 SCADA 通信网络中使用音频和/或视频会议系统时，应制定相关措施减少其对 SCADA 操作数据传输的影响。这些措施包括 SCADA 操作数据传输的优先权，会议数据的带宽限制，或其他服务质量措施来减少音频和/或视频会议系统在网络基础设施中对 SCADA 操作的影响。由于增加了安全漏洞，任何音频或视频会议的流量应通过过程控制防火墙。

7.3.10 视频监视

视频监视可以认为是一种特殊类型的 SCADA 数据，用来监视并加强远方现场的安全。当 SCADA 网络需要具有视频监视功能时，应制定相关措施减少其对 SCADA 操作数据传输的影响。这些措施包括对非视频 SCADA 信息给予优先权，对视频监视数据的带宽限制，或其他用于减少在 SCADA 运行时对网络设备影响的限制其服务质量的措施。视频监视数据应按照本标准第 6 章所述的内容进行保护。当在两个安全防护区间传输视频监视数据时应采取适当的措施。

8 现场通信

通信对于 SCADA 系统的成功运行起到重要作用。通信系统除了能够提供基本的通信方法，还能对数据流提供保密性、完整性和可用性功能。SCADA 通信正在逐步淘汰租用专用的串行线路或基于 IP 拨号上网的方式。通常，从控制中心到远程设备之间的 SCADA 通信连接具有较长的通信路由。利用外部的电信系统通信会使 SCADA 遭到未经授权的监视或干预。以下各节将重点描述 SCADA 通信系统的特征。

8.1 现场设备技术

现场设备为 SCADA 系统提供一个工业设备接口，用来传送来自传感器和变送器的模拟量和状态量信息。这些信号被转换为数字量，并根据要求使用各种遥测的方法进行传输。SCADA 系统以同样的方式将命令传送给现场设备。某些现场设备，如 PLC、流量计算机、发动机/电机安全设备以及电气设备等，将完成特定的功能。如这些设备发生故障，可能带来运行风险。

现场设备可通过本地或远程访问进行配置、校准和编程。通常现场设备不具有安全的网络连接能力。因此，本标准中所有安全防护控制措施应适用于这些设备。

部分安全防护控制方式如下：

——每台设备的密码宜唯一，根据运营商的密码管理策略进行更改。由设备制造商提供具有串行端口的设备无密码保护或使用默认密码时，就会存在漏洞。

——使用时，现场设备宜采用多级用户授权等增强型身份认证功能。如该功能不可用，宜采用外置的通信接口保护措施。

——操作面板应具有密码保护功能，防止未经授权的个人访问。
——运营商宜要求现场设备具有内部逻辑保护功能，如收到未经授权的命令，现场设备以故障安全方式响应，从而保护设备。
——现场设备配置的软件和开发工具提供有限的安全防护，设备访问应需要增强型身份认证。应对现场设备外壳提供物理安全防护并保持现场设备外壳的完整性。
——设备软件开发、升级和变更的管理应遵照 3.6 概述的安全防护要求。

8.2 系统访问

SCADA 系统经常与各种系统连接，包括 SCADA 系统的内部和外部网络连接。本节讨论各种互联和关联的最佳方式。

8.2.1 网络协议

TCP/IP 协议正在成为主机和现场设备互联的优先协议。应禁用不必要的服务，例如简单网络管理协议（SNMP）、简单文件传输协议（TFTP）等。如需要使用这些服务，应将默认用户名和密码更改为复杂的读/写字符串和强密码。宜使用安全协议代替 Telnet 和 FTP 等非安全协议。

8.2.2 访问路径的数据加密

宜加密现场和 SCADA 系统之间的连接。采用安全加密技术能降低数据保密性、完整性和可用性的风险。不推荐使用互联网作为现场数据通信连接方式。如互联网是唯一可行的连接方式，在现场和 SCADA 系统之间应采用加密型安全连接方式。采用任何加密方法前应进行分析，以确保增强型安全防护不会干扰 SCADA 系统的正常操作。

8.2.3 临时用户访问网络

应禁止未经授权的工作站连接到网络。应禁用未使用的网络端口。

8.2.4 远程访问 SCADA 系统组件

只有必要且在严格身份验证获得批准后，才能远程访问例如 HMI，PLC，RTU 等 SCADA 系统组件。这些措施应采用增强型网络安全措施弥补物理安全的不足。如可行，应参考其他行业关于安全远程连接的最佳作法。

8.2.5 维护用拨号调制解调器的访问

任何用于维护用途的拨号调制解调器应具有增强型安全防护措施。由于调制解调器本身难以保证安全，所以回拨和验证服务是理想的增强措施。当不使用拨号调制解调器时，应从网络上断开。最低限度的使用拨号调制解调器。

附 录 A
（资料性附录）
SCADA 安全防护示例

下表根据本标准和业内最佳作法进行编制，可指导运营商审查具有相应保护级别的 SCADA 系统进行审查。该附录不是一个完整的统计列表，也未覆盖 SCADA 系统所有可能的安全漏洞。

安全防护计划和规程	已制定/需要/不需要	审核
针对人员、流程和技术的安全防护计划、策略及规程是否已制定？		
重要资产和操作功能是否已被定义并形成组织机构共识？		
各级组织是否明确了优先权？包括安全性、合规性、物理和信息的安全防护等。安全防护计划是否考虑上述内容？		
是否清楚描述了管理层的角色与职责、审查计划，以及是否需要更新安全防护计划？		

信息保存/存档/备份标准	已制定/需要/不需要	审核
应用软件的数据按企业信息保存策略进行保存。运营商在制定每一项应用软件的异地备份周期和保存计划时，应考虑保存要求。这些保存要求是基于运营商提出的有关要求和记录保存计划。该异地备份周期和保存计划应反映出储存信息的风险评估		
系统管理员应确保所有数据按照运营商的有关要求与记录保存计划进行备份。文件/数据库服务器应至少每天进行增量备份，每周进行一次完整备份。备份文件应拷贝到异地。系统管理员应确保系统能够恢复并满足信息所有者的业务需求		
运营商应根据信息所有者的要求编制备份与恢复规程		
根据信息保存策略，受限或保密信息系统数据宜每日进行备份并保存在一个适当的异地位置		
公共信息系统数据应定期备份，并定期转移至安全位置；备份周期由运营商和信息保管人共同决定		
应用软件的信息保管人负责编制并修订软件和硬件的恢复规程		
软件应包括但不限于重建生产环境所必需的程序、应用软件和系统		
与重要业务相关的、受限或保密数据的机构应编制和修订现行的 BCP		
运营商应确定信息系统的可用性要求。此需求的确定是在分析对组织的影响及系统必须在多长时间内恢复的基础上进行的		
运营商负责对 DRP 进行维护、测试、记录和执行。DRP 是业务连续的一部分，须包含数据备份与恢复规程及软硬件恢复规程		

业务连续性计划	已制定/需要/不需要	审核
为保证时效性，BCP 应至少每年审查并更新一次		
BCP/DRP 中的系统过程恢复使用的时间应与业务需求及业务恢复策略保持一致		
成功实施备份和恢复过程后，或备份过程中的组件（数据源、介质、设备、逻辑路由等）发生变化时，运营商应至少每年对恢复过程进行一次测试。只有经过运营商授权的人员（信息保管人、系统管理员）可调用备份和执行恢复		
此计划应包括重建生产环境所必须的所有系统软件和关键支持应用软件的详细目录		
每个单位每年都应测试 BCP/DRP。测试应有记录，并将结果报告给运营商和企业管理层指定的其他委员会		
恢复测试应在测试环境下，用现场产生的备份数据在测试系统上进行		
BCP/DRP 的副本和备份软件（数据和系统）应保存在一个异地存储设施中		
环境恢复时，应在连续操作计划中明确替代或人工恢复方法		
该计划应包括但不仅限于对应急设施和硬件设备的规定。应急设施应按照报告单位的技术规格书要求的全部操作功能进行配置		
BCP/DRP 应包括备用系统硬件的可用性和安装位置		
应明确与第三方供应商［例如互联网服务提供商（ISP）、公共设备或电话企业］相关的依赖关系和恢复流程，并纳入 BCP/DRP		
硬件包括但不仅限于所有中央处理单元（CPU）、存储单元、外围设备、远程终端、控制器、通信设备、线路、打印机，以及重建生产环境所需的其他相关硬件设备		
系统与应用软件的备份应在系统升级/维护前进行		
所有受限或保密信息的磁带备份都应按照 BCP/DRP 中规定的时间间隔发送到异地		
BCP/DRP 应包括系统环境的过程变更，如软硬件升级		
计划中应包括基于不同灾难类型的相关方案		
网络与其他应用软件间如有依赖关系，计划中应明确		
计划应包括对恢复系统和数据的人员的规定、时间表、职责、培训与技能发展跟踪记录。恢复团队应包括业主和系统的使用者，还应包括经过培训的重建系统的替代人员		
计划应包括申请异地备份媒介的规程		
应明确记录灾难发生后、系统恢复过程中及系统恢复后恢复团队人员所使用的通信规程		
系统使用者应参与 BCP/DRP 测试，确保系统正常工作		

变更、配置与问题管理标准	已制定/需要/不需要	审核
运营商应负责编制变更控制规程		
报告单位的变更申请表用于记录包含受限或保密信息的应用软件和/或系统的变更申请，变更申请表应至少包括以下信息： ——变更发起人； ——变更执行人； ——变更批准人； ——变更理由； ——变更性质（如适用）； ——变更所需的资源预计； ——变更所需的测试、测试负责人； ——变更终止程序； ——受影响的系统； ——系统使用者的联系信息		
变更请求必须由运营商批准		
少量因素可能会中止变更（如员工数量太少）。在此情况下，应相应减少控制步骤或按例外处理		
变更管理标准应包括控制规程，以应对 SCADA 系统及其网络发生的紧急情况，这些情况会对健康、安全或环境构成威胁		
所有紧急变更请求执行后应建档记录。文档材料应包括变更执行人、时间、日期、执行的命令、受影响的程序和数据文件等。紧急变更执行人应向相应的运营商提交一份书面材料，说明变更执行的内容		
运营商负责监视紧急修复的安装，极少情况下，程序员需要升级到访问生产环境的权限，应创建专用的临时账户或访问途径。紧急事件处理后，必须禁用或删除这些临时账户		
变更控制过程中涉及的人员角色和职责应明确界定并记录。不相关的职责必须剔除（例如负责代码变更的程序员不可将这些同样的变更转移到生产系统中）		
应用软件开发人员不应对生产环境和可执行代码进行写访问		
应用软件应具有单独的控制环境，用于： ——开发/暂存； ——集成测试和用户验收测试； ——生产源代码（在适用情况下）； ——生产可执行代码		
运营商应确保对符合详细的变更控制规程（例如高危版本升级与低风险的维护）的条件（变更的类型）进行识别和记录		
运营商应对变更控制规程的文档进行更新		
在小单位中进行职责分离和测试可能是不实际的，宜进行例外处理，可通过减少控制实现		
所有 SCADA 系统源代码和配置文件应仅向授权的支持人员开放		
生产源代码库应是唯一的。开发人员修改程序时，应从这个库中获取源代码。所有生产源代码的修改应记录并进行版本控制		
开发人员进入生产源代码库的访问权限应受到限制，只允许将生产区的源代码复制到开发区，并将修改后的代码写入或转移到一个暂存库中		

变更、配置与问题管理标准	已制定/需要/不需要	审核
应制定变更控制流程确保程序员对生产和测试环境的访问权限受到充分限制		
所有信息都要遵循运营商的信息保存计划		
在企业的生产计算机环境中运行应用软件之前，应对所有的应用软件进行综合测试（例如测试相互依赖关系以确保它们不会破坏相关功能）		
用于测试的所有数据都应符合信息保护标准		
用户应用软件验收计划应对所有的主要功能、程序和接口系统进行测试，应记录测试步骤		
用户验收测试期间，逻辑访问限制应确保开发人员不能升级访问权限，在未通知信息所有者之前，不能修改被测试的代码		
所有对企业计算机网络进行的非紧急变更，都应遵循企业的变更和问题管理标准。对企业内部网络的变更包括但不仅限于： ——安装新网络软件； ——改变网络地址； ——重新配置路由器； ——增加拨号线路； ——创建可信主机关系		

操作系统与应用软件标准	已制定/需要/不需要	审核
在开发阶段，新的操作系统和应用软件的实施应采用安全防护措施。将新的操作系统和应用软件放到生产环境之前应对安全防护措施进行测试		
制定操作系统和应用软件更新规程		

应用软件与数据库标准	已制定/需要/不需要	审核
应用软件和数据库不应有未经授权的访问途径（“后门”）		
运营商应对应用软件和数据库进行分析，以确定重要性、数据的敏感性和应用类型。分析可识别基线要求是否足够，或者是否应提出额外的重要性/敏感性要求。 数据敏感性分为： ——保密； ——受限； ——公共		
按照安全防护策略和规程规定，在开发阶段前期，无论是内部制定或商业成品组件，新的应用软件和数据库都要与安全防护措施相结合。在这些应用软件和数据库投入生产环境前应进行安全防护措施的测试		
无论是内部开发的，或者供应商购买/开发的，所有应用软件和数据库都要相互兼容		
所有基于角色的应用软件都需要唯一的用户账户名和强密码，提供用户身份验证来执行角色分离		
应用软件用户账户应进行保护，除非绝对必要，否则不要将用户账户和密码存储在数据库表中。如需要将密码存储在数据库表中，则要对密码进行加密		

应用软件与数据库标准	已制定/需要/不需要	审核
数据库管理权限（删除、插入、选择和更新）应仅限于运营商授权的数据库管理员		
对于缺乏访问控制的分析或公用应用软件的受限或保密数据，应通过操作系统和/或数据库的访问控制功能来实现管理		
针对受限或保密数据，基于角色的应用软件需要有访问授权规程和/或访问控制流程。访问权限应与用户的工作职责相符		
终端用户不应在应用软件的控制之外对应用软件的代码或数据库进行访问。这种访问应只限制于被授权人员（例如系统或应用软件的支持人员）		
在用户被授权访问应用软件或数据库的数据之前应对所有用户进行识别和验证		
基于角色的应用软件、受限的应用软件访问，以及保密数据都应将管理权限制在能够完成管理任务的最小权限范围		
“超级用户/所有”访问账户应只限于管理员，为满足业务需求，他们需要获得不受限制的访问权限		
可执行文件应限制非授权执行或替换		
作为指导性原则，应用软件应强制非运营商用户在闲置15min后自动关闭。访问恢复之前，用户应重新进行身份验证		
每个运营商都应确保对重要应用软件的使用和管理进行记录		
每个运营商应确保对系统和程序进行记录。该记录包括但并不限于： ——硬件和软件配置； ——数据库设计和结构，包括逻辑和物理数据库架构； ——维护和修改规程		
运营商应确保对备份和恢复计划的记录与业务需求保持一致		
所有数据都能由授权用户访问。应保留职责分工		
数据的有效性和完整性（例如业务准则）应符合业务要求		
应用软件应是数据录入、删除或更新的唯一方法。如录入、删除或更新的数据在应用软件的控制之外进行，则需符合变更和问题管理标准		
不应允许对导入文件进行更新。应设置控制防止对文件进行未经授权的更新，致使一个生产环境与另一个生产环境相互影响		
应用软件应设置内部控制，确保数据的准确		
根据计算机、电话和网络使用标准的加密部分的规定，应使用必要的加密手段对保密数据进行安全传输		
仅系统账户（操作系统上或应用软件所定义和使用的账户）能进行后台作业		
应建立接口/传输控制及程序，以确保发现和纠正数据丢失或损坏		

物理安全防护标准	已制定/需要/不需要	审核
所有员工和承包商都应对企业信息（硬拷贝、磁盘、磁带等）进行保护，保护级别应与信息的价值级别相称		
所有运行的服务器或内部保密数据应存放在安全的数据中心或安全的数据机房		
包括计算机硬盘在内的包含保密级别信息的介质，应存储在访问受限的环境中（例如保险库、数据中心、酒店保险箱）		

物理安全防护标准	已制定/需要/不需要	审核
介质上存储的所有信息如被划分为公共信息，则不需要标记。其他分类信息（受限信息和保密信息）应在媒介上适当标记		
永久或临时搬迁之后，应立即安排工作小组对空出来的工作领域和设备进行最终的清理和检查，确保没有信息遗留。应对所有的公共区域进行责任划分检查（例如大厅的文件柜、档案室、衣柜、储藏室等）		
所有网络端口和电话线永久或临时重定向后，应先立即停用，在支付网络端口和电话线的当前客户通过授权后才可继续使用		
工作区域位置发生变化时，应对所有的库存控制文档进行更新，以反映所做的更改		
应对所有 SCADA 计算中心、通信中心和网络中心进行连续监视（每天 24h/一周 7d）。这种监视能通过摄像机、报警门窗、中心配备人员，或以上的组合来进行		
SCADA 控制中心应有一套操作规程，以保护控制中心的设备。这些规程应包括但不局限于以下考虑： ——防火； ——火灾检测； ——灭火； ——关闭流程； ——自然灾害； ——恐怖行为； ——公用设施（电和水）； ——故意毁坏； ——水检测		
SCADA 控制中心应配有自动门，在门被打开后能够立即自动关闭，打开时间超过 30s 时，会发出报警		
SCADA 控制中心应配有监控摄像机，能够对控制中心的入口进行监视		
SCADA 控制中心的消防围墙应为不易燃墙体，且阻火时间至少 1h。所有这些墙壁上的开口（门、通风管道等）应在火灾时自行关闭，阻火时间同样至少 1h		
对磁带、磁盘和文档库的物理访问权限应仅限于岗位职责要求的可访问人员		
所有包含保密数据的信息存储介质（例如硬盘驱动器、软盘、磁带、只读光盘驱动器）在不使用时，未经授权不应访问。如该信息由符合加密标准的加密系统进行保护，则可例外对待		
所有计算机和网络设备未使用的物理端口应被禁止访问，包括以太网交换机、路由器、防火墙以及服务器上的通用串行总线（USB）端口		
对存放企业计算机或通信系统的建筑物，应采取物理安全防护措施予以保护，防止未经授权的人员获取准入权限		
包含企业计算机系统、布线或通信设备［配线室、专用分组交换（PBX）机房等］的所有房间的物理访问都应时刻保持关闭，只有被授权的人员才有访问权限。设备拥有者应持有一份授权访问人员名单，并每年对该名单进行两次审查		
所有员工、承包商和参观者都应一直佩戴标识牌。如丢失了卡片钥匙或等效的访问授权装置，应在 24h 内向当地安保人员报告		

物理安全防护标准	已制定/需要/不需要	审核
一旦访问完毕，24h 内应立即撤销访问权限。直接主管有责任查看离职或调离的员工和承包商的卡片钥匙是否归还和取消		
授权人员不应允许未知人员或未经授权的人员在无人陪同的情况下进入限制区域。无正当理由进入电脑室的人员应立即被护送离开电脑室，授权人员应与合适的保安人员联络		

验证标准	已制定/需要/不需要	审核
用户账户只能通过确定以下内容的文档来建立： ——用户的身份； ——增加用户账户的授权人		
雇佣期满后，应禁用其用户账户		
应对用户账户进行审查，并且适当的情况下，应禁用超过九十天未激活的账户		
每个计算机和通信系统用户账户（强制性管理账户除外）应只能代表唯一用户。尽量不建立联合用户账户或组账户，但允许该类账户操作控制台。不允许用户与其他人分享密码		
每个计算机和通信系统用户账户应是唯一的，且永远与所分配的用户单独对应。员工或承包商离开企业后，不应再使用与该员工或承包商关联的任何用户账户，除非该账户重新分配给同一个人		
用户对使用他们的个人用户账户进行的所有活动负有责任。除账户所有人外，用户账户不可由其他任何人使用。用户不应允许他人使用自己的用户账户进行任何活动		
应给具有访问特权的用户（系统管理员）分配一个单独的、唯一的账户，与非特权账户不同。企业信息系统使用的特权用户账户命名规范应与域名所有者的用户标识标准保持一致		
获得超级用户（操作系统相关）或者特权账户（系统管理员）的用户宜使用其个人账户登录到系统。然后，管理员应根据要求，将当前账户切换到特权账户		
只有作为管理员时，具有访问特权的用户（系统管理员）才使用特殊的权限；正常工作时，他们会使用自己具有有限特权的非特权用户账户。管理员宜使用非特权用户账户登录，然后按照要求升级到特权账户		
超级用户/管理账户的个人使用权限应仅限于那些绝对必要的情况，以保障管道运行		
应在操作系统功能范围内使用复杂性规则。如系统具有无密码的复杂功能（或不足），应使用密码过滤器或其他补偿性控制		
一般用户和管理员： ——密码有效期：九十天； ——最小长度为 8 个字符； ——密码应是字母和数字的组合，能包括符号； ——应启用密码的历史记录功能时，每个用户存储最后 12 个加密密码		

验证标准	已制定/需要/不需要	审核
服务账户（主机到主机的数据传输账户）： ——密码过期：当知道密码的人角色转换时； ——长度至少为 14 个字符； ——密码应由字母、数字和符号的组合而成； ——当系统具有密码历史记录功能时，每个用户存储最后 12 个加密密码		
如操作系统平台或应用软件支持加密，那么应对密码文件进行保护和加密		
传输过程中应在数据包内对密码进行加密，或通过加密通道［如安全套接层（SSL）］进行传输		
安装后，应立即更改应用程序、操作系统、数据库管理系统（DBMS）和其他程序的默认密码		
不应使用企业账户和密码在外部互联网网站上进行验证		
初始、重置的登录密码应遵循密码复杂性规则，并要求用户立即更改密码		
创建强密码时，应避免使用以下内容作为密码： ——容易与企业、账户所有者身份、地址或用户名相关联的词语； ——字典单词或专有名词； ——日历组合，如 jan2001，feb2001 等； ——含单词的顺序号码，如 word002，word0001，word003 等，或 001word，002word，003word 等； ——太相似的密码：与以前的密码至少有三个完全不同的字符； ——重复模式或回文，如：aaa1aaa		
用户是自己密码的所有者。他们： ——不应与他人分享自己的密码； ——不应在任何可访问的地方记下密码； ——应防止在何种环境和情况下，密码可通过观察等活动被获取； ——不应将密码嵌入到文件和脚本中		
每天，每个用户对一个系统或一个应用程序的密码可更改一次		
计算机系统管理员应建立的初始用户密码长度最低为 8 个字符，由字母、数字和特殊字符组成（技术上可行的情况下）		
初始密码不应很容易的与企业或用户相关联（例如身份证号码、员工数量、地址、姓名对应的数值表示等）		
技术上可行的情况下，系统应强制进入该系统的新用户更改初始密码，并使新密码符合密码标准		
硬件和软件在安装后，应更改所有默认密码，新密码要符合企业的密码标准		
使用密码短语代码是一个很好的做法，方法是在密码中使用短语中每个单词的一个字母、数字或符号		
对于非操作控制台，用户连续 5 次验证失败后，用户将被锁定，无法访问资源		
为了获得信息所有者关于访问 SCADA 数据的许可，用户应提供一个合理的业务案例		
如运营商授权用户访问 SCADA 数据，此种授权应确认以下内容并记录下来： ——谁在请求访问； ——正在请求访问的内容； ——由谁批准访问		

验证标准	已制定/需要/不需要	审核
运营商授予预定信息接收人访问权之前，应先了解信息接收人的信息需求。这些需求应是业务目的，如需求信息是真实的业务需求，应允许其进入访问		
仅允许授权员工和/或承包商访问所分配的工作和职责范围内须知、须看或须用数据和信息，其他信息不允许使用、访问和处理		
运营商有责任每半年对系统权限进行一次审查，并应及时撤销用户不再需要的所有特权，包括系统管理员的特权。审计应每半年进行一次，因为业务环境和数据重要性在不断变化。系统管理员有责任向运营商提供恰当的报告，以便审查所有用户的访问		
员工调离或工作重新分配时，应对访问权限进行审查		
对不再需要访问的信息，运营商应尽快移除该信息的访问权限。用户和运营商有责任共同负责保证访问权限与业务需求相一致，且访问权限的分配是建立在须知的基础上		

人员安全防护标准	已制定/需要/不需要	审核
招聘新员工时，人力资源部应协助安全和保密信息处理策略的实施。所有新员工将收到一份与职位和角色相符的信息安全防护策略和/或安全防护宣传材料，并承诺他们了解策略和标准中规定的责任		
要制定一个人员安全防护联系和培训策略，该策略确定员工的角色、职责、雇用条件、招聘筛选过程，并对培训方案进行概述		
各报告单位应建立并维护一个流程，记录所有员工及承包商对信息系统和数据，以及限定的企业财产的访问，这些访问包括但不仅限于： ——胸卡； ——信用卡/名片； ——钥匙； ——笔记本电脑/台式电脑； ——个人数字终端（PDAs）； ——电话； ——远程访问		
主管或经理应通知所有对信息系统或数据进行访问授权的运营商，在员工合同终止时及时撤销此类访问，或员工调离的情况下撤销/修改此类访问		
主管或经理应收回为员工、承包商或第三方配备的设备，例如笔记本电脑、软件、数据、文档、手册、智能卡、手持设备等		
当拥有保密或受限信息访问权限的员工被调离或合同终止时，该员工的主管或承包商的责任人应直接与运营商进行协调，商定撤销用户访问权限的日期。如用户被解雇，那么在用户收到解除合同的通知之前，就应撤销该用户的访问权限		
拥有数据中心访问权限的用户被调离或合同终止的情况下，该员工的主管或承包商的责任人应通知当地的安保人员，以确保受保护区域的访问权限被撤销		
当员工离开任何职位后，经理应审查其电脑文件和纸质文件，以确定谁将保管该类文件		
对存储信息资产的企业设备应实施物理访问控制。这些控制应符合企业的人员和资产安全防护策略		

信息分类与应用重要性标准	已制定/需要/不需要	审核
企业内的所有生产信息都将有一个指定的信息所有者。信息所有者的职责在信息保护角色和责任标准中有详细的阐述		
运营商应编制并维护一份数据库目录或高级别保密和受限信息说明。应每年进行一次审查及更新		
信息所有者进行风险评估工作之前，任何信息不能降到较低的级别		
运营商应设置应用软件重要性和数据敏感性等级		

网络连接标准	已制定/需要/不需要	审核
在企业信任网络、专用网络和互联网之间应设置一个 DMZ		
DMZ 内应设置基于主机和网络的 IDS		
应连续使用两个通信过滤设备（例如路由器和防火墙）过滤流入和流出的通信量，只能对所需的资源进行访问		
应监视从非受信任区域到信任区域的通信		
第三方的访问权限应仅限于满足业务需求的必要资源		
不应通过一台交换机同时连接内部、DMZ 和外部网络		
网络架构的设计应尽量减少因单点故障影响重要系统实现其功能的可能性		
所有用户在访问任何网络资源之前都应进行验证，自助服务终端除外		
应定期审计和更新 SCADA 计算机，安装安全防护补丁和修补程序		
应对所有网络设备的访问控制列表进行记录。记录应包括每个规则的目的、相互依存关系和安全防护的解决		
如未对安全防护要求进行规定，没有明确、记录的审查和批准，就不能进行任何连接		
应对所有无线网络进行适当的保护		
所有对 SCADA 系统的远程访问应在获得批准后方可进行		
所有对 SCADA 系统的远程访问都应使用强验证		
运营商应持有一份拥有远程访问权限的用户列表		
授权的用户未输入验证之前，远程系统不应自动连接到 SCADA 系统		
应进行定期审查，识别出对 SCADA 系统未经授权的访问		
应进行定期审查，确保网络记录为当前记录		

系统安全防护审计与审查标准	已制定/需要/不需要	审核
根据信息保存策略，包含计算机或通信系统安全防护相关事件的日志应保留一段时间。应对日志进行保护，防止发生修改。只有获授权人员才能审查这些日志。这些日志对错误校正、安全防护漏洞修复、调查和相关工作都非常重要		
企业全体员工应留意并及时报告任何潜在的安全防护事故，包括病毒、入侵和不兼容情况，并立即执行企业的事故报告、升级和解决流程		

系统安全防护审计与审查标准	已制定/需要/不需要	审核
按照企业的信息保存策略要求，应对拥有受限或保密信息访问权限的用户访问活动记录进行保存。运营商每个月对这些记录进行审查，并应保留这些记录		
运营商负责监视和记录系统活动，以发现安全防护事件。只有获得授权的个人经管理层事先批准后，才能评估和/或使用网络测试/监视软件或硬件		

承包商、供应商、顾问和第三方标准	已制定/需要/不需要	审核
与信息安全防护服务和产品相关的所有合同均应符合运营商所有适用的安全防护策略		
如承包商所提供的服务可能或将会影响保密信息，应取得运营商的批准		
负责执行与承包商签订合同的经理应确保合同内容符合所有策略，并详细规定违约处理措施		
协议中应规定由承包商开发的软件的所有权		
承包商对企业信息的访问应受合约约束，并符合运营商的信息安全防护策略。合约内容应得到运营商法律部门的批准		
运营商应定期审查承包商是否符合运营商的信息安全防护策略		
承包商应遵守履行合同的条件所需的访问限制		
根据运营商的安全防护策略，为运营商提供服务的每个承包商及其员工都应与运营商签订一份保密协议		

计算机和网络使用标准	已制定/需要/不需要	审核
SCADA 系统的计算和通信资源不应用于个人用途		
禁止使用运营商的 SCADA 系统的计算和通信资源进行以下活动： ——不道德的活动或非法活动； ——试图访问未经授权查看的信息； ——未经授权披露保密或受限信息； ——运营商的安全防护策略禁止的任何其他活动		
不对 SCADA 系统操作造成干扰或负面影响的前提下，安装病毒扫描程序和/或检测程序。如不允许安装，应采取其他措施来隔离和保护系统不受病毒侵害		
安装或执行任何 SCADA 系统外文件之前，应先对其扫描，并对病毒和真实性进行验证。外部存储介质也应先被扫描和验证后，方可使用		

计算机、电话和网络使用标准	已制定/需要/不需要	审核
在被授权登录到任何运营商的 SCADA 计算机之前，运营商应按照其安全防护策略的要求对用户出示登录公告，或者含有以下内容的公告： ——SCADA 系统只能由授权用户使用； ——如继续使用 SCADA 系统，表明该用户他/她是一个授权用户； ——使用 SCADA 系统，表明同意被监视。 下面是一个可被接受的登录公告形式：		

计算机、电话和网络使用标准	已制定/需要/不需要	审核
“SCADA 系统仅由授权用户使用。使用这个系统的任何个人，承认并同意本企业有权监视、访问、使用和披露系统产生、接收或存储的任何信息，并放弃与他/她使用该系统相关方面的所有个人隐私权或隐私。企业策略规定，未经授权和/或使用本系统不当是不能容忍的，企业对违反规定的人将采取正当措施。” 国家可能有特定的法律，规范系统的使用和监视。国家的法律部门应对登录公告的措辞进行审查和修改，使其符合法律规定，并对所有修改进行记录。应引用针对公告修改的法律参考资料。 系统管理员负责发布和修改登录公告		
成功登录之前，不应出现运营商、系统的具体信息、网络、位置或主机的确认信息		
对不成功的登录不提供任何信息，这包括识别哪些登录序列（用户账户或密码）是不正确的		
使用加密时，应使用与 SCADA 系统兼容的最安全的行业标准的方法		
受限或保密信息在 SCADA 系统外部存储或传输时，应对其进行加密		
运营商应遵守运营商的信息保存策略和企业的记录管理程序，该程序为企业的业务记录制定了保存和销毁的方案和要求		
对电子信息存储介质的处理，应与存储于介质中的最高等级信息的处理方式相称		
在对介质进行处理时，介质中存储的信息仍被认为是保密信息，那么所有存储过保密信息的电子介质应被彻底销毁		
在对介质进行处理时，介质中存储的信息仍被认为是受限信息，那么所有存储过受限信息的电子介质应至少被消磁或擦除。如介质不能被消磁或擦除，则应被彻底销毁		
SCADA 安全防护控制区外的个人电脑/笔记本电脑不应无人值守，除非使用终端锁或密码保护屏保。允许锁定工作站的操作系统应提供与操作系统启动之前需要身份验证的操作系统相同的保护级别		
SCADA 安全防护控制区外的个人电脑/笔记本电脑和服务器宜配置带有密码保护的屏保程序。在个人电脑/笔记本电脑或服务器控制台待机 10min 后，屏保程序应输入密码才能进入		

附 录 B
（资料性附录）
SCADA/控制系统安全防护计划

本附录是作为开发运营商开发特定 SCADA 安全防护计划的示例，利用本标准和行业最佳案例汇编而成。该附录并不是一个完全详尽的列表，并不覆盖 SCADA 系统所有可能的安全防护漏洞。

修订记录			
日期	描述	修订编号	批准人
10/01/03	发布的待批准文件	1.1	负责人

B.1 简介

每个业务单位应使用 SCADA/控制系统安全防护计划来制定具体的安全防护计划。

该文件分为五大部分，这五大部分分别是：

——识别和记录。

——风险分析。

——预防措施。

——监督。

——安全防护管理。

前三部分介绍了进行识别、风险分析、采取必要预防措施的必要步骤，以确保 SCADA/控制系

统的安全。监督和安全防护管理这两部分描述了应被用来确保 SCADA/控制系统长期安全防护，以及如何对 SCADA/控制系统的安全防护进行管理的方法。

用来提高 SCADA 网络安全防护的 21 个步骤为：

1） 识别所有与 SCADA 网络的连接。
2） 断开与 SCADA 网络不必要的连接。
3） 评估和加强剩余与 SCADA 网络连接的安全防护。
4） 通过删除或禁用不必要的服务，强化 SCADA 网络。
5） 不要依赖专有协议保护系统。
6） 部署设备和系统供应商所提供的安全防护功能。
7） 对被用作后门进入 SCADA 网络的任何媒介都要严格控制。
8） 使用内部和外部的 IDS，并建立全天 24h 事故监视。
9） 对 SCADA 设备和网络，以及其他任何连接网络进行技术审计，识别安全防护关注点。
10） 对所有连接到 SCADA 网络的远程站场进行物理安全防护调查和评估，以评价其安全防护。
11） 建立 SCADA“红队”识别和评估可能的攻击情景。
12） 明确经理、系统管理员和用户的网络安全防护角色、职责和权限。
13） 对服务于重要功能或包含需要更高级别保护的敏感信息的网络架构和识别系统文档化。
14） 建立一个严格、持续的风险管理流程。
15） 以深度防御原则为基础，建立网络保护策略。
16） 清楚地识别网络安全防护要求。
17） 建立有效的配置管理流程。
18） 执行例行的自我评估。
19） 建立系统备份和 DRP。
20） 高层组织领导应设定网络安全防护性能的预期目标，并就网络安全防护性能承担个人责任。
21） 制定策略并开展培训，将组织人员因疏忽而透露关于 SCADA 系统的设计、操作、安全防护控制等敏感信息的可能性最小化。

B.2 识别和记录

B.2.1 每个［企业］单位对 SCADA/控制系统的网络连接和架构进行识别和记录。每个单位识别出服务于重要功能或包含需要更高级别保护的敏感信息的系统。

本附录和后面部分的所有文件应考虑为敏感文件，不向公众发布。每个文件都要按照 6.2 的规定，作为敏感文件来处理。

本附录收集的信息应作为参考附录，但不应与计划一起发布。

注：开发并记录强大的信息安全防护架构是建立有效保护策略的一部分。重要的是，组织在对网络进行设计时，要考虑安全防护，并在网络架构的整个生命周期内，对网络架构应有充分的了解。尤其重要的是，需要对该系统功能和系统存储信息的敏感性进行深入的了解。如没有这样的了解，就不能正确评估风险，保护策略的制定也不够充分。记录信息安全防护体系结构及其组件是理解整个保护策略、识别单点故障的重要部分。

B.2.1.1 识别、记录并全面了解所有连接到 SCADA/控制系统的连接。

B.2.1.1.1 识别连接到 SCADA/控制系统的连接。

——识别与另一处通信的具体位置。

——识别每个位置与外部发生的通信连接或者可能用于与外部通信的连接。

——外部通信连接包括电话调制解调器、租赁线路调制解调器、综合业务数字网（ISDN）、帧中

继、甚小口径卫星通信终端（VSAT）、无线电、光纤发射器、硬线直接连接、无线以太网发射器、与互联网的连接和/或任何其他能用于与另一个位置通信的通信方法。

——识别通信是否发生在［企业］的 SCADA/控制系统设备之间，或者发生在外部系统之间。

——承运商、供应商/系统集成商、［企业］业务设备等。

——识别在该位置与 SCADA/控制系统以外任何设备通信的连接。

——［企业］业务设备等。

——识别与外部系统进行通信的连接。

——业务合作伙伴、PLC 等。

——识别这些连接通常激活还是未激活。

——识别用于上述连接的通信类型。

——主服务器/从服务器、从服务器/主服务器、点对点、异步或 IP 协议、协议内容等。

——识别与 SCADA/控制系统外部进行连接所使用的方法。

——DMZ PLC、防火墙、双宿计算机、直接连接等。

B. 2. 1. 1. 2 确定连接的目的和必要性。

——识别控制系统运行所必需的连接。

——识别监管所需的连接。

——识别业务合作伙伴用于控制的数据交换连接。

——识别业务合作伙伴不用于控制的数据交换连接。

——识别为业务应用提供控制系统数据所使用的连接。

——识别维护控制系统所需的连接。

——识别不再需要或不再使用的连接。

B. 2. 1. 1. 3 识别连接到 SCADA/控制系统的物理接入点的位置。

——一般是以太网连接，例如能用于访问 SCADA/控制系统的以太网的集线器、交换机或任何墙壁插孔。

——应对其他不使用以太网的接入点进行识别和分析，查看从该点是否可以进入 SCADA/控制系统。

B. 2. 1. 1. 4 识别对连接和接入点的保护程度。

——识别连接的软件安全防护措施。

——识别接入点的物理安全防护措施。

——对连接进行识别，并找出未经授权连接的漏洞。

B. 2. 1. 2 识别和记录连接到 SCADA/控制系统网络的设备。

B. 2. 1. 2. 1 识别连接到 SCADA/控制系统网络的所有设备的位置。

B. 2. 1. 2. 2 识别是否是 SCADA/控制系统设备、业务系统设备或第三方设备。

B. 2. 1. 2. 3 识别设备类型：

——局域网通信设备（LAN）（集线器、交换机、路由器、防火墙）。

——WAN 通信设备（路由器、调制解调器、无线通信设备）。

——域控制器。

——SCADA 服务器。

——HMI。

——文件服务器。

——PLC 或其他控制器。

——历史服务器。

——维护/监视终端。

——其他服务器。

——其他的设备。

B. 2. 1. 2. 4 识别设备的连接类型和协议：

——以太网。

——TCP/IP。

——串行口。

——Modbus。

——其他。

B. 2. 1. 2. 5 识别设备对 SCADA/控制系统的重要性。

B. 2. 1. 2. 6 识别设备中是否包含重要数据。

B. 2. 1. 3 对连接到 SCADA/控制系统网络的所有远程站场和接入点进行物理安全防护调查和评估，以评价其安全防护性能。

注：连接到 SCADA 网络的任何位置都是评估目标，尤其是无人操作或无人看管的远程站场。应对每个连接到 SCADA 系统的设施进行物理安全防护调查并彻查接入点。对信息来源进行识别和评估，包括可能被监控的远程电话/电脑网络/光纤电缆、可能被利用的无线通信和微波链路、可能被访问的计算机终端，以及无线局域网接入点。识别并消除单点故障。必须充分检测站场的安全防护，防止未经授权的访问进入。不允许为了方便，通过在线网络接入点进入远程、无人看管的站场。

B. 2. 1. 3. 1 对 SCADA/控制系统的接入点进行物理安全评估。

——无人远程设施接入点需要有某种形式的物理安全防护，应把这些接入点锁在建筑物内，或者放在周围有防护措施的带锁的箱子里。

——在有人的设施内，只能对有限的访问位置进行访问，并对未经授权的访问实施监视。

——在主办公楼，每个接入点需要放在带锁的或安全的房间内。

B. 3 风险分析

B. 3. 1 每个［企业］单位都要进行安全防护风险分析并建立风险管理流程。

注：透彻地了解网络计算资源的风险，对于制定有效的网络安全防护计划是非常重要的。风险包括：DOS 攻击、可导致敏感信息受损的漏洞。风险评估是理解这些风险的技术依据，对制定有效策略、减少隐患、保持计算资源的完整性也非常重要。首先，应以当前的威胁评估为基础，进行基线风险分析，以用于开发网络保护策略。由于技术快速发展、新威胁每天都在出现，有必要建立一个不间断的风险评估流程，对保护策略进行常规性改变，能确保策略的有效性。风险管理的基础是网络保护策略已实施的情况下对残余风险的识别，并让管理层接受残余风险。

B. 3. 1. 1 对 SCADA/控制系统的每个连接进行风险收益分析。

B. 3. 1. 1. 1 分析过程中不要依赖专有协议作为保护手段。

注：有些 SCADA 系统在现场设备和服务器之间使用独特的专有通信协议。通常情况下，SCADA 系统的安全防护是完全基于这些协议的保密性。但是，独特的协议难以提供“真正的”安全防护。不要依赖专有协议或出厂默认配置设置来保护系统。此外，应要求供应商说明所有后门和供应商进入 SCADA 系统的接口，并要求他们提供能确保安全的系统。

B. 3. 1. 1. 2 检查连接，确定其整体风险，并进行风险分级（1—低风险，5—高风险）。

每个业务单位都将制定和记录风险等级划分的标准。

风险是指某连接存在的危害隐患（例如连接到互联网是一个高风险，本地设备之间的串行连接是一种低风险）。

B. 3. 1. 1. 3 检查连接，确定其整体收益，并进行收益分级（1—低收益，5—高收益）。

每个业务单位都应制定和记录收益等级划分标准。

——检查连接，确定对控制系统的整体收益。

——检查连接，确定对业务操作的整体收益。

——检查连接，确定对维护的整体收益。

——检查连接，确定对客户服务的整体收益。

——检查连接，确定对［企业］的整体收益。

B. 3. 1. 1. 4 对比每个连接的收益与风险，并进行整体等级划分（1—高风险/低收益，5—低风险/高收益）。

每个业务单位都将制定和记录整体等级划分标准。

B. 3. 1. 2 对 SCADA/控制系统使用的设备进行风险分析。

B. 3. 1. 2. 1 对设备进行检查，确定其在整个 SCADA /控制系统的价值（1—低价值，5—重要价值）。

每个业务单位都应制定和记录设备价值等级划分标准。以下几条作为设定标准的参考准则。

——对设备进行评估，确定该设备如不可用，会对 SCADA/控制系统造成什么影响。

——如单台设备能影响系统的整体操作，那么该设备具有重要价值，价值等级应是“5”。如一台不具有热备功能，也没有备用部件的 SCADA 服务器。

——如单台设备能影响该系统的一部分，应给定的等级为“4”。如一台接收站的 PLC，可能会关断一条或多条管线，但是不会关闭整个系统。

——如单台设备能影响一个站场，但长期下去可能会影响到其他站场，应给定的等级为“3”。如一台不重要的辅助 PLC，管线仍然可运行，但降低了运行效率。

——如单台设备能影响一个站场，但不会影响到其他的站场，应给定的等级为“2”。如水处理 PLC。

——如单台设备有没有实际的影响，应给定的等级为“1”，如一台站场备份的 HMI。

B. 3. 1. 2. 2 检查每个设备的类别，确定该类别设备对 SCADA/控制系统可能产生的影响，并进行等级划分（1—影响最小，5—影响最大）。

每个业务单位都将制定和记录影响等级划分标准。

前面部分中提到多种设备，每类的设备对系统的运行都是很重要的；但是，有些设备比其他设备更重要，有些是十分重要的。需要对每类设备进行等级划分，这样，能优先处理最重要的系统。最不重要的设备等级为“1”，最重要的设备等级为“5”。每个业务单位都应制定等级划分标准。

B. 3. 1. 2. 3 对每类设备进行检查，确定其受网络攻击的整体敏感性，并进行等级划分（1—敏感性低，5—敏感性高）。

每个业务单位都应制定和记录敏感性等级划分标准。

——检查设备的类别，确定其内部安全防护的等级。

——检查设备的类别，确定其变异性。判断顶层设备如防火墙或终端设备等，是否具有不同层次安全防护级别，访问时不会被破解。

——检查设备的类别，确定破解该设备所使用工具的共性。

——检查设备的类别，确定破解系统所需要的知识水平。Windows 知识是广泛传播的；控制系统的知识虽然有限，却是可学的。

——确定设备组受网络攻击的整体敏感性，并进行等级划分。

B. 3. 1. 2. 4 对设备进行检查，确定设备给 SCADA/控制系统带来的整体风险，并进行整体风险等级划分（1—低风险，5—高风险）。

每个业务单位都将制定和记录整体风险的等级划分标准。

——对比上述每件设备的等级，确定整体风险。

——设备风险等级中，“1”代表整体风险低，“5”代表整体风险高。

B. 3. 1. 3 对这样情景进行评估：某人可完全访问 SCADA/控制系统，而且他具备控制或更改系统中所有逻辑的知识和所需工具。

B. 3. 1. 3. 1 识别可能会导致人和/或环境受到危害。

——对于确定属于该种情况，需要考虑采取措施。安全设备需要采用硬接线，这样设备就能独立运作，即使控制系统已经被入侵，安全设备也能发挥作用。

B. 3. 1. 3. 2 识别可能会导致长期的服务中断，对公众造成影响。

——对于确定属于该种情况，需要制定应急计划或者安装必要的设备，防止事故影响到社会公众。

B. 3. 1. 3. 3 识别可能会对［企业］造成重大财务影响。

——对于确定属于该种的情况，需要制定减轻财务影响的计划，并提交给管理层。

B. 3. 1. 3. 4 识别可能产生的其他影响。

——对于属于该种的情况，应进行风险评估，以确定风险产生的可能性、可能产生的财务影响、对业务操作的影响，以及实施预防性措施所需的成本。

——应根据风险和影响实施预防性措施。

B. 3. 1. 3. 5 如适用，应对上述确定的情况建立系统备份，制定 DRP。

注： 制定 DRP，能够在任何紧急情况（包括网络攻击）下快速恢复。系统备份是所有计划的一个重要组成部分，并可使网络快速重建。要经常对 DRP 进行演习，确保计划有效，且工作人员对计划保持熟悉。以计划演习中吸取的经验教训为基础，对 DRP 做出适当的修改。

——备份和 DRP 的目标是能够从任何网络攻击中恢复，将对业务操作造成的影响降到最低。

——该计划应包括从最坏情况下的攻击情景中一步一步地恢复规程，该计划可以进行修改，通过跳过一些步骤从轻微事故中恢复。

——该计划应说明如何进行涉及多个工作中心的全面演习，演习可模拟系统遭到网络攻击的真实情景。此外，该计划还应说明如何进行只涉及 SCADA/控制系统工作人员的小型演习，模拟多种网络攻击情景，这些演习可用于评估计划的有效性。如演习结束表明需要对计划进行更改，则应修改计划。

——该计划应为全面演习和小型演习制定一个时间表。

B. 4 预防措施

B. 4. 1 每个［企业］单位都将采取以下措施，保护和控制对 SCADA/控制系统的访问。

B. 4. 1. 1 建立有效的配置管理流程。

注： 维护网络安全的基本管理流程就是配置管理。应包括硬件配置和软件配置。更改硬件或软件，很可能引入破坏网络安全防护的漏洞。需要建立评估和控制所有变化的流程，以确保网络保持安全。配置管理从良好测试和记录的安全防护基线开始，保护各种系统。

B. 4. 1. 1. 1 每个业务单位都将建立一个配置管理流程，能对发生的变化进行有效沟通，从而评估这些变化对系统安全防护可能造成的影响。

——目前的变更管理（MOC）流程就是用于该目的，但该流程也未必足以处理所有的配置更改。

B. 4. 1. 2 使用内部和外部 IDS，并建立有效的事故监视。

注： 为了能够有效应对网络攻击，要建立入侵检测策略，该策略包括向网络管理员发出的来自内部或外部发起的恶意网络活动警示。IDS 的监视要每天 24h 进行；这个功能能通过页面调度程序轻松实现。此外，制定事故响应程序对所有攻击做出有效响应。为了配合网络监视，启动所有每日系统日志和审计系统日志以迅速检测可疑活动。

B. 4. 1. 2. 1 每个业务单位在将当前配置和技术允许的前提下建立对系统有效的监视系统。

B. 4. 1. 3 断开与 SCADA 网络的不必要连接。

注：为了确保 SCADA 系统最高程度的安全防护，宜将 SCADA 网络与其他网络连接隔离开。任何与另一个网络的连接都可能带来安全防护风险，特别是这个连接与互联网存在连接途径时。虽然与其他网络直接连接可能提高重要信息的传递效率和方便性，但是，不安全的连接完全不值得冒险；为提供必要保护，SCADA 网络的隔离必须是主要目标。如利用 DMZ 和数据库等策略，能辅助从 SCADA 网络到企业网进行安全数据传输。但必须准确设计和使用这些策略，避免因为配置不当引入的额外风险。

B. 4. 1. 3. 1 宜将 SCADA/控制系统网络与其他所有网络隔离。

包括独立系统上其他 SCADA /控制系统网络。

——将一个网络上的漏洞与其他网络隔离。如一个网络被攻击，漏洞就会被隔离在该网络内。

——防止一个网络的问题影响其他网络。

——通过这样对 SCADA/控制系统进行访问，实现有效控制。

——限制 SCADA/控制系统网络上与相关设备连接的设备数量。

——限制可访问 SCADA/控制系统网络的人员数量。

B. 4. 1. 3. 2 断开不再使用的所有连接。

B. 4. 1. 3. 3 考虑断开收益低的连接。

B. 4. 1. 3. 4 断开风险高、收益低的连接。

B. 4. 1. 3. 5 考虑断开风险/收益等级低的连接。

B. 4. 1. 4 对现有 SCADA 网络连接的安全防护进行评估和加强，以深度防御原则为基础，建立网络保护策略。

注 1：对 SCADA 网络的所有连接进行渗透测试或漏洞分析，评估与这些连接途径相关的保护情形。利用这些信息，结合风险管理流程，为进入 SCADA 网络的所有路径制定一个强大的保护策略。因为 SCADA 网络的安全性取决于最薄弱的连接点，所以应在每个接入点使用防火墙、IDS，以及其他适当的安全防护措施。配置防火墙规则，禁止访问 SCADA 网络，并且尽量明确允许的连接。例如，一个独立系统运营商（ISO），不应仅因为其需要连接到 SCADA 系统的某个组件而被授予“全局（blanket）”网络访问权限。将 IDS 有策略地放在每个接入点，网络安保人员可及时地发现潜在的网络安全防护缺口。组织管理层必须理解连接到 SCADA 网络的相关风险，并承担相应的责任。

注 2：深度防御是构成所有网络保护策略的一个基本原则。必须在流程开发的早期设计阶段考虑深度防御，并且所有与网络相关的技术决策都必须考虑进去。利用技术和管理控制，将各级网络已确定的风险带来的威胁尽可能减轻到最小。必须避免单点故障，必须分层设置网络安全防护防御措施，限制和控制所有安全防护事故的影响。此外，必须有保护每一层的安全防护措施，防止被同一层的其他系统破坏。例如，为了防止内部威胁，应限制用户只能访问那些履行工作职能所必需的资源。

深度防御的原则是拥有多个安全防护级别。例如，设置一台连接到 DMZ 的网络连接点的防火墙与另一个连接 DMZ 与个人网络的防火墙。此外，网络上的设备需要设置访问密码。应设置多个安全防护层，在网络攻击者能够影响系统之前，只能横向活动。

B. 4. 1. 4. 1 其余连接的风险等级＞1 时，应考虑采取以下步骤。

——对可能更加安全的备用连接类型进行评估。

——判断多个不同的连接是否能集中在一个单一的安全连接。

——如串行连接到外部系统，可考虑安装一个 DMZ 设备，可作为两个系统的从服务器，或安装其他系统，防止外部系统将数据写入控制系统。

——宜用防火墙和/或 ACL 来限制特定的设备之间的连接。如一个特定的移动设备需要与 SCADA/控制系统网络以外的另一设备通信，那么应将通信限制在需要进行通信的设备之间，所有其他端口和路由都需要锁定。

B. 4. 1. 4. 2 应严格控制对被用作后门进入 SCADA 网络的任何媒介。

注：如 SCADA 系统中确实存在后门或供应商的连接，必须实施强验证，以确保安全通信。用于通信和维护的调制解调器、无线和有线网络是 SCADA 网络和远程站场间的重大漏洞。成功的“war dialing”或“war driving”攻击可让攻击者绕过所有其他控制，直接对 SCADA 网络或资源进行访问。要将此种攻击的风险降

到最低，应禁止拨入连接，取而代之某种类型的回拨系统。

——后门连接应已确定，并列入风险分析中。

——任何收益<4 的后门（供应商/维护）连接都应被断开。

——所有临时后门（供应商/维护）连接都应集中到一个单一的连接。这些连接最少需要有一个用户名和密码验证。个人令牌例如安全的 ID、磁卡或视网膜扫描、手指/拇指纹等高级生物识等认证方式，可用来提供超越密码验证的额外安全防护级别。

——一直有效的后门（供应商/维护）连接的访问权限应受到防火墙或 ACL 的限制。

B. 4. 1. 4. 3 对连接到两个不同的网络的双宿计算机进行评估，并保证其安全性。

对计算机进行双宿设置，可为计算机连接到两个不同的网络提供一种便利的方式；但是，如利用双宿连接使两因为安全防护原因而被隔离的网络，是重大的安全防护风险。如双宿计算机被攻击，会同时对这两个网络造成破坏。

如双宿计算机用于处理同一个网络或者同一个系统内的两个网络的冗余，则是允许的。

——在隔离网络之间连接的双宿计算机应断开，应通过一个防火墙访问第二网络。

B. 4. 1. 4. 4 通过删除或禁用不必要的端口或路由，禁止连接。

——对运行和支持 SCADA/控制系统所需要的通信端口和路由进行评估。

——禁用所有不必要的端口。

——应限制不同站场间不相关设备的连接，或路由器上未使用 ACL 的连接。如 WAN 的一部分受到攻击，访问就会受到限制。

B. 4. 1. 4. 5 保护无线连接，防止出现未经授权的拦截和连接。

——对于未加密的以太网无线数据节点之间应有一个安全通道，阻止未授权的连接通过拦截无线链路连接到加密网络。

B. 4. 1. 5 为系统重要设备提供额外的安全防护措施。

B. 4. 1. 5. 1 重要设备应采用额外的安全防护措施。

——确保重要设备与其他网络之间设置物理或实际隔离，另一个网络应只能通过防火墙来访问重要设备，或访问要受到 VLAN 之间路由器 ACL 的严格控制。

——重要设备上软件的当前完整备份应存储在本地和异地。

——应为重要设备提供安装有最新软件的离线备份设备。

B. 4. 1. 6 采取措施，确保连接到 SCADA/控制系统网络上设备的安全性，重点放在风险最高的设备上。

B. 4. 1. 6. 1 通过删除或禁用不必要的服务，强化 SCADA 网络。

注：以商业或开放源代码操作系统为基础的 SCADA 控制服务器，可能通过默认的网络服务暴露。宜删除或禁用未使用的服务和网络后台进程，减少风险和直接攻击。在 SCADA 网络与其他网络互相连接时，这一点尤为重要。除非对服务/功能的运行做过彻底的风险评估，能证明服务/功能的收益远远大于漏洞利用的可能性后，才允许在 SCADA 网络上运行服务或功能。删除 SCADA 网络服务的例子包括：自动抄表/远程计费系统、电子邮件服务和互联网接入，功能禁用的一个例子是采用远程维护。公共域上有很多商业和开放源代码操作系统的安全配置指南。此外，要与 SCADA 供应商紧密合作，确定安全配置，协调对业务系统所做的所有更改，确保删除或禁用服务不会造成停机、服务中断或支持缺失。

——对 SCADA/控制系统的 HMI 和服务器进行评估，禁用或删除所有系统操作或维护中不需要的服务或程序。

——对维护中使用的服务或程序进行风险—收益分析，判断这些服务和程序是否需要或者能被删除。

B. 4. 1. 6. 2 部署设备和系统供应商所提供的安全防护功能。

注：大多数早期的 SCADA 系统（大多数系统在使用中）没有任何安全防护功能。SCADA 系统所有者必须坚持要求他们的系统供应商启动产品补丁或程序升级等形式的安全防护功能。一些最新的 SCADA 系统设备都带

有基本的安全防护功能，但是为了安装方便，这些功能通常被禁用。对每个 SCADA 设备进行分析，以确定是否具备安全防护功能。此外，出厂默认的安全防护设置（例如计算机网络防火墙）通常把可用性设置为最大，而把安全防护设置为最低。设置所有的安全防护功能，以提供最高级别的安全防护。只有对安全防护级别降低的后果进行彻底的风险评估之后，才允许设置低于最高安全防护级别。

——宜对连接到 SCADA/控制系统的每台设备的安全防护功能进行评估，以识别安全防护功能的开启是否会对 SCADA/控制系统造成影响。要确定改变出厂默认密码设置而不会对系统造成影响。

——在不影响 SCADA/控制系统的操作的情况下，可部署设备的安全防护功能，或者更改出厂默认密码设置。

——宜开启域安全防护功能。

——消除连接到电脑的所有可能的本地登录账户，尤其是具有管理员访问权限的账户，其权限应被限制到提供业务支持所需的最小权限。

——不应使用默认的管理员账户。应改变用户名，并进行密码设置。

——如系统能够成为一个域的成员，可通过域安全防护控制所有其他对该计算机的管理访问权限。

——如使用自动登录，该账户对系统的运行应只有最小权限。此外，这个账户应只能从一个指定的工作站进行登录。

——应对所有共享文件夹的必要性进行评估，而且对这些文件夹的访问权限应设置严格的域控制。

B. 4. 1. 6. 3 不宜打开未使用的连接。

——不宜访问未使用的端口。如一个位置只需要一个连接，那么应使用双绞线直接与路由器连接。

——如有开放的连接，宜保证集线器或交换机的物理安全。

——所有路由器应使用 ACL，防止未知的连接进入 WAN。

B. 5 监督

B. 5. 1 每个［企业］单位将设置一个监督计划，以确保 SCADA/控制系统的维护，和/或提高其安全防护级别。

B. 5. 1. 1 对 SCADA/控制系统设备、网络，以及其他任何连接的网络进行技术审计，识别其安全防护问题。

注： 对 SCADA 设备和网络进行的技术审计对持续安全防护有效性非常重要。很多商业和开放源代码安全防护工具可让系统管理员对系统/网络进行审计，识别活动服务、补丁级别，以及常见漏洞。使用这些工具不能解决系统性问题，但会消除攻击者可利用的“阻力最小路径”。应对已发现的漏洞进行分析来确定它们的重要性，并采取适当的纠正措施，跟踪纠正措施并分析这些信息，确定发展趋势。此外，采取纠正措施后还需对系统进行重新测试，确保真正消除漏洞。主动检查非生产环境，识别并解决潜在问题。

——应进行内部审计，以确保 B. 2 和 B. 3 创建的文件为当前文件，以及系统的任何更改能得到及时更新，并且 B. 4 中的措施能得到积极开展。

——应定期进行第三方审计，确保与该安全防护文件保持一致。

B. 5. 1. 2 执行例行的自我评估。

注： 需要进行强性能评估，并为组织提供有关网络安全防护策略和技术实施有效性的反馈。一个组织成熟的标志是能够自我进行故障识别，分析根本原因，并实施有效的纠正措施，解决个人和系统性问题。自我评估过程通常是有效网络安全防护计划的一部分，包括定期漏洞扫描、自动网络审计、进行组织和个人的自我评估。

——每个业务单位应定期对 SCADA/控制系统进行评估，提高系统的安全防护性能。这包括评

估新的技术和供应商的工具。

B.6 安全防护管理

B.6.1 每个［企业］单位都应明确网络防护负责人、系统管理员和用户的网络安全防护角色和职责。

注：组织人员需要通过清晰而有逻辑的角色和职责定义，了解保护信息技术资源相关的具体要求。此外，需要给予关键人员足够的权力开展分派的职责。良好的网络安全防护取决于个人的主动性，主动性不强通常会导致执行的不一致和安全性失效。应建立一个网络安全组织机构，对角色和职责进行定义，并明确网络安全问题如何逐步解决，以及紧急情况下应通知谁。

B.6.1.1 每个单位应为 SCADA/控制系统确定一名网络安全防护负责人。

B.6.1.1.1 作为［企业］网络安全团队的成员之一的网络安全防护经理，应向［企业］网络安全防护协调员报告所有的网络安全防护问题。

——在本单位或其他单位发生网络攻击时，应与安全防护负责人联系。

——如本单位检测到入侵访问，安全防护负责人应负责通知［企业］安全防护协调员。

——如其他单位检测到入侵访问，安全防护负责人负责在本单位开展纠正措施。

——如其他单位因为入侵访问被迫关闭系统，安全防护负责人负责识别并减轻影响。

B.6.1.1.2 网络安全防护负责人应与网络安全防护团队合作，在本单位或其他单位入侵时，负责制定行动计划。

——应识别不同等级的威胁。

——应确定应采取的步骤，减轻具体单位或其他单位各个级别威胁带来的风险。

——应确定采取的具体行动，以及人员分配。

B.6.1.1.3 网络安全防护负责人将负责指定 SCADA/控制系统管理员。

——管理员应有责任确保遵守安全防护策略。

——管理员应识别系统内的所有安全防护威胁。

——管理员应对 IDS 日志和系统日志进行监视，防止可能的攻击。

——管理员应为需要访问权限的人员提供技术支持，并进行监督。

B.6.1.1.4 网络安全防护负责人将与 SCADA/控制系统管理员合作，确定 SCADA/控制系统所有用户的访问级别。

——访问级别应被限制在工作人员完成任务必需的最低级别。

——任何级别的访问都应限制在人员直接负责的设备。

——应记录每个人的访问级别。

——宜对所有的访问级别进行集中控制，便于维护和有效控制。

B.6.1.1.5 作为网络安全防护团队，来自各业务单位的网络安全防护负责人与 IT 安全防护负责人将每半年见一次面。

——该团队应根据法规、技术和其他问题负责对安全防护计划进行审查和更新。

——该团队应共同努力，确保每个业务单位的安全防护计划符合企业的网络安全防护计划。

——该团队应携手开发和更新统一的威胁通知和响应计划，计划需包括所有 IT 系统和 SCADA/控制系统受攻击期间的协调。

B.6.1.2 识别敏感材料和开展培训活动，将组织人员因疏忽而透露 SCADA 系统的设计、操作、安全防护控制等敏感信息的可能性最小化。

注：只有在严格的、须知的基础上，才能发布 SCADA 网络相关的数据信息，而且只能发布给明确获得授权接收此类信息的人。“社会工程”通过调查初级用户，收集关于计算机或计算机网络的信息，往往是对计算机网

络发动恶意攻击的第一步。透露越多有关计算机或计算机网络的信息，该计算机/网络就越容易受到攻击。除非某人明确获得授权接收此类信息，否则决不要通过电话或面对面将 SCADA 网络的相关数据，包括系统操作员/管理员的姓名和联系方式、计算机的操作系统、和/或计算机和网络系统的物理和逻辑位置泄露出去。任何身份不明的人发出的获取信息的请求，都应被发送到中央网络安全防护系统进行验证和请求回复。在安全网络中员工本身可能是一个薄弱环节，应开展培训和信息宣传活动，确保员工在敏感网络信息，尤其是在他们的密码保护上时刻保持警惕。

SCADA/控制系统的独特之处是它在使用传统安全防护措施方面的局限性；但是因为它的独特性，如要对其成功进行攻击，就需要了解系统的内部信息。因此，保护这方面的信息对系统的整体安全防护是非常重要的。

B. 6. 1. 2. 1 以下信息只能发布给须知这些信息的人，发布的信息内容限制于必需的信息。不能仅仅因为有人在责任范围内需要获知地址信息，就向其提供完整的寻址机制。

——寻址机制，包括异步多点地址、IP 地址和 TCP 端口。

——PLC 寄存器分配。

——数据库配置，包括 PLC/ RTU、HMI、SCADA、通信服务器、路由器和防火墙。

——协议信息。

——通信类型。

——系统布局示意图。

——通信布局示意图。

——使用的 SCADA 设备类型。

——SCADA/控制系统的其他任何信息。

——已制定的安全防护措施。

B. 6. 1. 2. 2 SCADA/控制系统的数据应存放在安全位置。

——SCADA/控制系统的数据不应向所有人公开，包括一般公众和整个企业人员。

——SCADA/控制系统的数据可能对其他业务功能有用，但原始数据不应直接提供给所有用户。如在 SCADA/控制系统之外有数据的需求，应对数据进行概括归纳，并存放在一个终端用户能访问的数据库中。对原始数据的直接访问应加以限制。

——程序文件和/或配置文件应保存在一台有访问控制的服务器上，只有授权人员才能访问这些文件。

——其他任何包含系统相关信息的文件，例如寻址机制和系统布局，应保存在一个安全位置。

B. 6. 1. 2. 3 对 SCADA/控制系统的敏感文件进行标识。

——应对 SCADA/控制系统包含敏感信息的文件进行标识，表明其敏感度。应有这样的标签，例如“仅供官方使用，不得分发”、“保密的”或其他表明该信息是不可自由发布的。

B. 6. 1. 2. 4 培训非常重要，可确保人们了解 SCADA/控制系统数据的敏感性。

——将信息的敏感性告知对 SCADA/控制系统数据有访问权限的人员。

——告知他们正确处理 SCADA/控制系统信息的重要性。

——告知他们该信息不能发布给任何人。任何信息请求都应直接转至安全防护经理进行处理。

中华人民共和国
石油天然气行业标准
油气输送管道监控与数据采集（SCADA）系统安全防护规范
SY/T 7037—2016
*
石油工业出版社出版
（北京安定门外安华里二区一号楼）
北京中石油彩色印刷有限责任公司排版印刷
新华书店北京发行所发行
*
880×1230 毫米 16 开本 3.25 印张 95 千字 印 1—1000
2016 年 5 月北京第 1 版　2016 年 5 月北京第 1 次印刷
书号：155021·7343　定价：39.00 元