



中华人民共和国电力行业标准

DL / T 860.3 — 2004
/ IEC 61850-3: 2002

变电站通信网络和系统 第 3 部分: 总体要求

Communication networks and systems in substations-
Part 3: General requirements

(IEC 61850-3: 2002, IDT)

2004-03-09 发布

2004-06-01 实施

中华人民共和国国家发展和改革委员会 发布

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 定义和缩略语	2
4 质量要求	2
5 环境条件	4
6 供电要求	7
附录 A (资料性附录) 访问安全	8

前 言

本部分根据原国家经济贸易委员会《关于下达 2002 年度电力行业标准制定和修订计划的通知》(国经贸电力[2002] 973 号)第 6 项制定。

国际电工委员会 TC57 制定了《变电站通信网络和系统》系列标准,该标准为基于通用网络通信平台的变电站自动化系统唯一国际标准。该系列标准具有以下特点和优点:分层的智能电子设备和变电站自动化系统;根据电力系统生产过程的特点,制定了满足实时信息和其他信息传输要求的服务模型;采用抽象通信服务接口、特定通信服务映射以适应网络技术迅猛发展的要求;采用对象建模技术,面向设备建模和自我描述以适应应用功能的需要和发展,满足应用开放互操作性要求;快速传输变化值;采用配置语言,配备配置工具,在信息源定义数据和数据属性;定义和传输元数据,扩充数据和设备管理功能;传输采样测量值等。并制定了变电站通信网络和系统总体要求、系统和项目管理、一致性测试等标准。迅速将此国际标准转化为电力行业标准,并贯彻执行,将提高我国变电站自动化水平,促进自动化技术的发展,实现互操作性。

本部分是 DL/T 860(变电站通信网络和系统)系列标准的一部分,本部分出版时,下述其他部分也将成为 DL/T 860 系列标准的一部分。DL/T 860 系列标准包括:

DL/T 860.1 变电站通信网络和系统 第 1 部分:概论

DL/T 860.2 变电站通信网络和系统 第 2 部分:术语

DL/T 860.3 变电站通信网络和系统 第 3 部分:总体要求

DL/T 860.4 变电站通信网络和系统 第 4 部分:系统和项目管理

DL/T 860.5 变电站通信网络和系统 第 5 部分:功能和设备模型的通信要求

DL/T 860.6 变电站通信网络和系统 第 6 部分:有关变电站 IED 的配置描述语言

DL/T 860.71 变电站通信网络和系统 第 7-1 部分:变电站和馈线设备的基本通信结构-原理和模型

DL/T 860.72 变电站通信网络和系统 第 7-2 部分:变电站和馈线设备的基本通信结构-抽象通信服务接口(ACSI)

DL/T 860.73 变电站通信网络和系统 第 7-3 部分:变电站和馈线设备的基本通信结构-公共数据类型

DL/T 860.74 变电站通信网络和系统 第 7-4 部分:变电站和馈线设备的基本通信结构-兼容的逻辑节点类和数据类

DL/T 860.81 变电站通信网络和系统 第 8-1 部分:特定通信服务映射(SCSM)-映射到 MMS(ISO/IEC 9506 第 1 部分和第 2 部分)以及 ISO/IEC 8802-3

DL/T 860.91 变电站通信网络和系统 第 9-1 部分:特定通信服务映射(SCSM)-通过串行单方向多路点对点链路传输采样值

DL/T 860.92 变电站通信网络和系统 第 9-2 部分:特定通信服务映射(SCSM)-通过 ISO/IEC 8802-3 传输采样值

DL/T 860.10 变电站通信网络和系统 第 10 部分:一致性测试

本部分等同采用国际电工委员会标准《IEC 61850-3: 2002 变电站通信网络和系统 第 3 部分:总体要求》(英文版)。

本部分的附录 A 是资料性附录。

本部分由中国电力企业联合会提出。

本部分由全国电力系统控制及其通信标准化技术委员会归口。

本部分由电力自动化研究院负责起草，国电南京自动化股份有限公司、中国电力科学研究院、烟台东方电子信息产业股份有限公司参加起草。

本部分主要起草人：徐劲松、马文龙、刘佩娟、何卫、曾庆禹、徐田军。

本部分由全国电力系统控制及其通信标准化技术委员会负责解释。

变电站通信网络和系统

第3部分：总体要求

1 范围

本部分适用于变电站自动化系统（SAS），它定义了站内智能电子设备（IED）之间的通信及相关的系统要求。

本部分属于通信网络的总体要求，重点是质量要求。它也述及环境条件和供电要求的指导方针，根据其他标准和规范，对相关的特定要求提出了建议。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB 9254—1998 信息技术设备的无线电骚扰限值和测量方法（idt CISPR 22：1997）

GB/T 15153.1—1998 远动设备及系统 第2部分：工作条件 第1篇：电源和电磁兼容性（idt IEC 60870-2-1：1995）

GB/T 15153.2—2000 远动设备及系统 第2部分：工作条件 第2篇：环境条件（气象、机械和其他非电影响因素）（idt IEC 60870-2-2：1996）

GB/T 17463—1998 远动设备及系统 第4部分：性能要求（idt IEC 60870-4：1990）

GB/T 17626.3—1998 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验（idt IEC 61000-4-3：1995）

GB/T 17626.4—1998 电磁兼容 试验和测量技术 电快速瞬变脉冲群抗扰度试验（idt IEC 61000-4-4：1995）

GB/T 17626.5—1999 电磁兼容 试验和测量技术 浪涌（冲击）抗扰度试验（idt IEC 61000-4-5：1995）

GB/T 17626.6—1998 电磁兼容 试验和测量技术 射频场感应的传导骚扰抗扰度试验（idt IEC 61000-4-6：1996）

GB/T 17626.8—1998 电磁兼容 试验和测量技术 工频磁场抗扰度试验（idt IEC 61000-4-8：1993）

GB/T 17626.10—1998 电磁兼容 试验和测量技术 阻尼振荡磁场抗扰度试验（idt IEC 61000-4-10：1993）

GB/T 17626.12—1998 电磁兼容 试验和测量技术 振荡波抗扰度试验（idt IEC 61000-4-12：1995）

IEC 60654-4：1987 Operating conditions for industrial-process measurement and control equipment-Part 4:Corrosive and erosive influences

IEC 60694：1996 Common specifications for high-voltage switchgear and controlgear Standards

IEC 61000-4-16：1998 Electromagnetic compatibility（EMC）-Part4-16:Testing and measurement techniques-Test for immunity to conducted, common mode disturbances in the frequency range 0 Hz to 150 kHz

IEC TS 61000-6-5: 2001 Electromagnetic compatibility (EMC) -Part6-5:Generic standards -Immunity for power station and substation environments

IEEE C37.90.2: 1995 Withstand capability of relay systems to radiated electromagnetic interference from transceivers

3 定义和缩略语

为满足本部分的需要,应用了如下定义和缩略语:

3.1 定义

见本标准系列第2部分。

3.2 缩略语

a.c.	交流 alternating current
AIS	空气绝缘开关 air insulated switchgear
d.c.	直流 direct current
GIS	气体绝缘开关 gas insulated switchgear
HMI	人机接口 human-machine interface
IED	智能电子设备 intelligent electronic device
IP	网际协议 inter-networking protocol
MTTF	平均无故障时间 mean time to failure
SAS	变电站自动化系统 substation automation system
SCADA	数据采集和监视控制 supervisory control and data acquisition
SF ₆	六氟化硫 sulphur hexafluoride
TCP	传输控制协议 transport control protocol

4 质量要求

4.1 概述

本章描述了用于站内过程的监视、配置和控制的通信系统的可靠性、可用性、可维护性、安全性、数据完整性以及其他性能要求。

本章包含了大量对其他标准的引用,频繁地引用了 GB/T 17463—1998。GB/T 17463—1998 规定了远动系统的性能要求,并根据那些影响系统性能的内容对这些要求进行分类。这些内容包括诸如可靠性、可用性、可维护性、安全性、完整性之类的条目。对每一项内容,GB/T 17463—1998 又列出了一些等级,从而使站内系统才能有望真正满足全部范围的性能要求。制造厂商在实际应用时必须按照 GB/T 17463—1998 中的规定来声明其产品符合这些等级中的某一特定等级。

4.2 可靠性

4.2.1 概述

按照“故障弱化”的原则,当 SAS 的任一通信元件发生故障时,变电站仍应是可持续运行的。不应存在这样一个故障点,即由于它而使整个站不可运行。应保持足够的当地监视和控制功能。任何元件的故障不应导致不可检出的功能失效,也不应导致多个和级联的元件故障。

在某些应用场合,特定的预防措施对于 SAS 的实施是必须的,通信系统也必须采取预防措施,例如,变电站主站系统可以是冗余的,使其具备故障自恢复功能。

如果 SAS 的通信元件是冗余的,则不应存在一种故障模式,使得冗余元件同时失效。只要存在分离的相互独立的电源,SAS 的冗余通信元件就应该分别由这样的电源来进行供电(例如独立的电池或站内供电线路)。冗余不是强制性的,它取决于站的重要程度,换言之,取决于该变电站的停电的后果和经营者的理念。

故障安全设计应当是必不可少的。不应该存在任何可能导致 SAS 产生非预期控制行为的故障模式，例如，导致跳开或合上一个线路开关设备。另外，SAS 的故障应当不会使变电站任何可用的就地计量和就地控制功能失效。

可靠性要求在 GB/T 17463—1998 的 3.1 中加以描述。制造商和用户应当就 GB/T 17463—1998 的 3.1.2 所定义的可靠性等级（R1、R2 或 R3）达成一致。

4.2.2 MTTF

制造商应明确地表述所提供设备的 MTTF，包括所采用的计算的标准方法。

4.2.3 站内关键性功能及其对 SAS 的相依性

关键性功能（保护、主要的控制功能、计算等）不应因某个单一故障而失效。为满足这一要求，SAS 应具备以下性能：

- 保护功能应当是自治的；
- SAS 可以执行诸如一台变压器故障后的自动恢复供电这样一些没有严格时间要求的控制逻辑行为，如果运用了这些逻辑行为，厂家应明确表明完成故障恢复的时间（以毫秒计）；
- SAS 的 HMI 应能独立于与控制中心的远动通信接口而运行。

4.3 系统的可用性

4.3.1 概述

正如 GB/T 17463—1998 中 3.2 所定义的，可用性应为 SAS 正常运行时间与总的运行时间的比值。正常运行时间是 SAS 能够执行其重要功能的时间。例如，当存在后备保护时，主保护故障应不能归到故障时间。再比如，如果存在另外的控制点，HMI 的故障也不能归到故障时间。

可用性要求应符合 GB/T 17463—1998 中 3.2.1 的描述。制造商和用户应就 GB/T 17463—1998 中 3.2.2 定义的可用性等级（A1、A2 或 A3）达成一致。

变电站自动化系统的可用性的规范不属本部分的范围。

4.3.2 自动恢复

可以为 SAS 提供系统和数据备份。当有备份时，SAS 单个元件的故障不应导致数据的丢失，也不应妨碍系统的正常运行。修复后，可以由人工干预切换回正常构型。

SAS 功能的关键性通信链路应当是冗余的或者具有替代路径，以防止由于信息传输的底层中断而造成系统停用。

4.3.3 故障弱化和差错恢复/备用

差错率的增加不应导致系统突然崩溃而只能是引起性能下降。应当有差错恢复功能以恢复 SAS 的可靠运行。

4.4 可维护性

参见 GB/T 17463—1998 中 3.3，可维护性要求应符合 GB/T 17463—1998 中 3.3.1 的描述。制造商和用户应就 GB/T 17463—1998 中 3.3.2 定义的可维护性等级（M1、M2、M3 或 M4）达成一致。

4.5 安全性

参见 GB/T 17463—1998 中 3.4。

4.6 数据的完整性

SAS 通信系统在出现传输和过程错误、传输延迟变化和和设备故障时应能可靠地传输数据。它必须提供：

- 在存在噪声的变电站环境下检测出传输错误；
- 链路拥塞的恢复；
- 可选的链路、媒介和设备的冗余支持。

SAS 传输数据的完整性和一致性应符合完整性级别 I 1、I 2 或 I 3（GB/T 17463—1998 中 3.5）。具体采用的完整性级别取决于传输数据的应用场合。

4.7 总的网络要求

4.7.1 地理要求

变电站内的通信网络应能覆盖 2km 以内的范围。

4.7.2 装置数量

变电站内通信网络应能应用到高压开关场的所有典型配置中, 包括 $1\frac{1}{2}$ 断路器接线方式和环形母线接线方式 (变电站配置的详细内容参见本标准系列的第 1 部分和第 5 部分)。

5 环境条件

5.1 概述

本章描述了气象、机械和电气对通信媒介及接口 (用于变电站内过程的监视和控制) 的影响。当通信设备是变电站内另外一个装置的一部分时, 对此装置本身的环境要求应同样适用于该通信设备。

本章包含了对其他标准文件的一系列引用, 频繁地引用了 GB/T 15153 和 IEC 60694。GB/T 15153 本身列举了许多环境气象条件类别, 并且每个类别都考虑了一种或一组针对不同环境气象参数的严酷等级。期望安装在变电站的设备必须真正满足环境类别的全部范围, 包括通常在户外的过程层设备, 户外或户内的间隔层设备, 户内/封闭的变电站层设备。在应用时, 制造商应当按照 GB/T 15153.2—2000 所述的环境气象条件的类别和严酷等级加以陈述。那些与高压开关设备和控制设备一体化的设备 (例如过程总线设备) 则应符合 IEC 60694。

5.2 温度

通信设备应能在 GB/T 15153.2—2000 中表 1 所推荐的温度范围内正常工作。

在存储和运输过程中, 设备应能承受 GB/T 15153.2—2000 中表 2 所推荐的大气温度范围。

大气温度在 GB/T 15153.2—2000 中的 3.3.1 中定义。

与高压开关设备和控制设备一体化的设备应符合 IEC 60694 第 2 章的要求。

5.3 湿度

通信设备应能在 GB/T 15153.2—2000 中表 1 所推荐的相对湿度下正常工作。

与高压开关设备和控制设备一体化的设备应符合 IEC 60694 中第 2 章的要求。

5.4 大气压力

通信设备应能在 GB/T 15153.2—2000 中 3.3.2 所推荐的大气压力下正常工作。

与高压开关设备和控制设备一体化的设备应符合 IEC 60694 中第 2 章的要求。

5.5 机械和振动

通信设备的机械和振动条件应根据其安装地点及服务要求符合国家和国际标准。在应用时, 制造商应当按照 GB/T 15153.2—2000 的第 4 章所定义的机械条件和振动应力的等级加以陈述。

与高压开关设备和控制设备一体化的设备应符合 IEC 60694 中第 2 章的要求。

5.6 污染和腐蚀

IEC 60654-4: 1987 被认为是在腐蚀和侵蚀影响方面的应用准则。应特别注意固体物质 (例如沙或灰尘) 和腐蚀性因素 (如盐) 的影响, 因为前者可能对通信设备的热性能产生影响, 后者会影响设备的连通性。

与高压开关设备和控制设备一体化的设备应符合 IEC 60694 中第 2 章的要求。

5.7 电磁干扰抗扰性

通信设备必须能够抵抗变电站内的各种类型的传导和辐射电磁骚扰, 这一点在设计和测试时必须做到。常见骚扰源有如下几种:

——闪电和开关浪涌;

——气体绝缘介质 (如通常使用的 SF₆) 的放电和冲击, 产生快速瞬变;

——GIS 内的行波，产生快速瞬变。

工业环境的一般抗骚扰要求对变电站来说并不够，因此，专用的要求在 IEC TS 61000-6-5：2001 中定义，这些要求和测试过程的具体内容在 GB/T 17626 系列的部分标准中给出。最重要的标准文档将在下面引用。

是否遵从标准必须通过型式试验加以证明，验证的准则在 5.7.4 中叙述。

5.7.1 传导骚扰

5.7.1.1 感应骚扰

射频场会产生骚扰，并通过变电站的电线进行传导。设备必须满足 GB/T 17626.6—1998 中的 3 级或 IEEE C37.90.2 中有关感应骚扰的部分。制造商和用户应当就这个问题达成明确的要求。

5.7.1.2 浪涌

浪涌按照 GB/T 17626.5—1999（测试等级为 4 级），波形为 1.2/50μs 和 10/700μs，峰值最高到 4kV 进行测试。

5.7.1.3 振荡波

振荡波按照 GB/T 17626.12—1998 中的 3 级标准进行测试，最高到 150kHz 的共模骚扰按照 IEC61000-4-16 中的 4 级进行测试。若数据通信和信号电路只能进行共模测试，此时的浪涌幅值应与差模测试相同。

5.7.1.4 快速瞬变

快速瞬变按照 GB/T 17626.4—1998 中的 4 级及以上标准进行测试。此外，电源和输出回路还必须在差模电压下进行测试。

5.7.2 辐射电磁骚扰

设备必须满足 GB/T 17626.3—1998 中的 3 级标准或 IEEE C37.90.2 中有关辐射射频电磁场的部分。制造商和用户应当就这个问题达成明确的要求。验证的准则在 5.7.4 中叙述。

5.7.3 工频骚扰

通信设备可能会面临各种各样的电磁骚扰，这些骚扰通过电源线、信号线传导或者直接来自环境辐射。骚扰的种类和电平取决于通信设备运行的特定环境。应参照的标准是 IEC 61000-4-16，磁场部分则参照 GB/T 17626.8—1998 和 GB/T 17626.10—1998。

除此之外，现在也认识到在变电站内铜导线中会产生一定程度的工频感应电压，特别是当一次故障电流流入变电站及其周围的情况时。这将是一种共模效应，由磁通链路引起，并在每根导线中产生几乎相同的感应电压。对于串行数据通信，需要进行线路测试以保证设备有能力经受一定的感应电压而不会妨碍设备的正常运行。变电站设备应能在表 1 所示的工频电压下正确运行。

表 1 工 频 电 压 等 级

级别	通信线路长度 m	非平衡式通信 V	平衡式通信 (1%非平衡) V	平衡式通信 (0.1%非平衡) V
1	1~10	0.5	0.005	0.0005
2	10~100	5	0.05	0.005
3	100~1000	50 ^a	0.5	0.05
4	大于 1000	500 ^a	5	0.5

a 非平衡式通信电路包括象 RS232 这样的电路。实际上，这样的通信系统被认为仅仅是在站内很短距离的通信或者是与便携机这样的智能测试设备的连接。当站内通信实际距离超过 20m 时建议不要使用。标准的平衡式电路是采用 PT0 电路相关类型，高达 500V 的共模电压仅引起不到 1%的不平衡，此外采用象变压器耦合这样的技术可以进一步获得 0.1%以内的阻抗平衡。

工频感应横向电压是变电站环境的基准值，表明设备设计允许的工作耐受水平。

设备应当采用一个将所要求的通信信号和工频干扰信号混合的注入式网络来测试。随着干扰的适当注入, 通信信号电平的大小应降低到制造厂声明的接收电平, 并且通信设备应保持正常工作。

5.7.4 验证的准则

5.7.4.1 应用的准则

下面列出的准则适用于直接被测试的设备和任何与该设备直接或远方连接的装置。连接的例子有电流环和电压回路(直流、音频、载波或微波), 串行、并行、光纤、无线电频率的连接也包括在内。

5.7.4.2 必须满足的条件

对于设备和与其相连的装置, 如果在测试时或测试的结果满足以下条件的要求, 则可认为设备通过了测试:

- 没有硬件损坏;
- 没有因测试引起的超过正常允许范围的校准值变化;
- 没有已存储的内存或数据损坏或丢失, 包括激活的或已存储的设置;
- 没有发生系统自复位, 并且无需人工复位;
- 已建立的通信不会一直中断;
- 已建立的通信如果中断, 应在允许的时间范围内自动恢复;
- 如果发生通信错误, 不应危害保护或控制的功能;
- 没有电气、机械、通信信号输出状态的变化;
- 没有视觉的、听觉的、信息输出状态的错误或永久的改变, 测试时这些输出的瞬间改变是允许的;
- 没有超出数据通信信号(SCADA 模拟信号)正常容差的错误发生。

5.7.4.3 设备功能

在测试时或测试后, 设备和与其相连的装置仍然具有与设计相同的完整和准确的功能, 除非制造商另行说明。

5.7.4.4 例外

制造商应在设备说明书中对设备中不符合验证准则的例外事项加以陈述。

5.7.4.5 测试点

测试点应包括:

- 每个装置的电源输入;
- 报警和辅助 I/O 连接;
- 永久连接的站内计算机;
- 间隔设备和远程通信接口设备之间的连接所和输出连接;
- 到任何以太网集线器, 以及电源输入、报警、端口(使用平衡双绞线输入)的金属性的连接。

测试点不包括:

- 非金属性的连接, 例如光纤;
- 维护计算机的临时连接;
- 制造商声明的长度必须小于 2m 的连接。

5.8 电磁干扰发射

通信设备也可能是在宽频范围内的多种电磁骚扰源, 骚扰可能会通过电源线、控制线传导, 或直接通过通信设备辐射。

通信设备应当满足 GB 9254—1998 中 A 级和 B 级(欧洲标准 EN 55022A 与 EN 55022B)或 FCC 条例第 15 部分中数字装置 A 级和 B 级(美国标准)的要求¹⁾。

1) 联邦规范条例, 47 条-远程通信, 第 15 部分: 射频装置, 由联邦通信委员会(FCC)2000 年出版。

6 供电要求

6.1 概述

本章规定了本部分所描述的通信设备的电源性能。通信设备运行所需的电源可能由以下几种方式提供：

- 直接连接到电源；
- 连接到位于电源和通信设备之间的供电设备；
- 主电源维修或故障时为设备运行提供的辅助备用或后备电源。

6.2 电压范围

本条仅涉及公用电网提供的具有同样基本性能的 50Hz 或 60Hz 交流电源和直流电源。

交流电源的电压范围应符合 GB/T 15153.1—1998 中表 1 的规定。

直流电源的电压范围应符合 GB/T 15153.1—1998 中表 5 的规定。

6.3 电压容差

交流电源的电压容差等级应符合 GB/T 15153.1—1998 中表 2 的定义。

直流电源的电压容差等级应符合 GB/T 15153.1—1998 中表 6 的定义。

制造商和用户应当就 GB/T 15153.1—1998 中的相关等级达成一致。

直流运行设备在输入电压降到规定的下限以下或者输入电压极性颠倒，应不会遭受损坏。

6.4 电压中断

直流电源 10ms 以内的中断应不会影响通信设备运行。不管多长时间的电源中断都不应对设备造成损坏，不管什么方式的中断也都不应对其他设备和人员造成危险。

6.5 电压质量

6.5.1 交流电源

交流电源的标称频率应符合 GB/T 15153.1—1998 中表 3 所规定的允许范围。

交流电源的谐波含量应符合 GB/T 15153.1—1998 中表 4 所规定的允许范围。

6.5.2 直流电源

直流电源的接地应符合 GB/T 15153.1—1998 中表 7 的规定。

电压纹波（GB/T 15153.1—1998 中 4.3.3 定义）应符合 GB/T 15153.1—1998 中表 8 所规定的允许范围。

附 录 A
(资料性附录)
访 问 安 全

在一定的使用者范围内,且在成本的约束以内,SAS 应能提供安全性能,抵制下列威胁:

A.1 服务拒绝——这种威胁试图故意阻止合法访问

为了应对这种服务拒绝的攻击,应当采用通信链路、通信关联和目标的联合保护。尽管通信链路保护取决于所采用的通信媒介/数据链路,但是至少通信关联的保护方法能够详细地加以说明。

服务拒绝的主要形式有两种,需要加以反击:

(1) 链路层拒绝——这种攻击中,攻击者试图阻塞对物理通信路径的合法使用。

例如:攻击者对属于 SAS 的拨号调制解调器进行拨号,电话和调制解调器之间建立了连接,然后攻击者让电话占线。这就阻止了受攻击的调制解调器的远端与 SAS 系统的通信。

对于链路层服务拒绝的正确的反击方法很大程度上依赖于 SAS 的物理媒介和通信的拓扑结构,远程访问 SAS 的例子也只是一个典型。因此,正确的反击方法取决于系统的基本构造并且也不属于本标准的标准化范围。

(2) 关联拒绝(资源耗尽)——在这种攻击中,攻击者试图通过攻击锁定许多或者所有的系统通信资源。面向连接的通信协议集特别容易受到这类攻击。高安全数据访问级别关联的建立应有用户授权机制保证其安全。

例如:基于 TCP/IP 的系统的套接字耗尽。TCP 是一种面向连接的传输层协议,特别容易受到这类攻击。攻击者一直不停地与 TCP 端口进行关联,但并不进行任何应用层的合法操作。每个 TCP 关联都消耗一定的通信资源(套接字),那些套接字在攻击者释放它们或者远方系统断开与攻击者的关联之前一直被占用着。

这类攻击可以通过 SAS 在一定时间内强制进行应用层的关联来检测。超时时间从 SAS 通信协议集的任意层的面向连续的资源(如套接字)被占用开始。SAS 在超时时间到期以后,必须收回通信资源。

注:这也是保护拨号调制解调器免受攻击的一种有效机制。

A.2 非法使用——攻击者试图通过一种未经授权的途径来使用 SAS

SAS 应当提供防止非法使用的保护手段。至少在关联建立过程中对 SAS 的访问应当受到授权批准的限制。这种批准应当出现在 SAS 通信协议集的应用层,并且支持关联访问权限的概念。至少应当支持以下几种级别的权限:

(1) 无权限。

这种权限表示,关联,哪怕是 SAS 的最基本的访问,也是不允许的。这种权限实际上是没有权限,并且可能导致关联不恰当地被中止。当然,关联中止杜绝了 SAS 系统被攻击事件的发生。

为了让监视系统能识别这样一种侵入,系统应当对因无权限而被中止关联的次数的轨迹保持跟踪。

为了能对攻击者进行揭露或拒绝,SAS 系统应最大可能地记录任何一个攻击者的相应的通信寻址信息,如果 SAS 资源允许作这样的记录,系统也应允许对这些信息进行检索。

(2) 监视。

这种权限表示关联仅被批准具有对 SAS 系统的属性或数值进行监视(例如读取)。但是,关联并没有被批准能够执行任何会影响 SAS 运行的行为(例如控制或者改变配置)。

(3) 控制。

这种权限表示关联被批准允许控制 SAS 系统的运行。这种权限总是连同监视一起被批准,但是这

种权限不允许关联进行配置修改。

(4) 配置

这种权限表示关联被批准允许对 SAS 的系统配置进行修改。这种权限总是连同监视一起被批准。

(5) 安全管理。

这种权限表示关联被批准允许对与安全有关的属性、数值或配置信息进行修改或检索。

也可能允许有其他的权限，这不属于本部分的范围。

权限级别的实现及粒度属于应用问题，不属于本部分的范围。

在 SAS 工作过程中，还有其他一些威胁需要考虑，这些都不属于本部分的范围。
