ICS 29.240.01
F 21
备案号：16985-2006

DL

中华人民共和国电力行业标准化指导性技术文件

DL / Z 981 — 2005 / IEC TR 62210: 2003

电力系统控制及其通信
数据和通信安全

Power system control and associated communication
Data and communication security

(IEC TR 62210:2003, IDT)

2005-11-28 发布　　2006-06-01 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

本指导性技术文件是根据《国家发展和改革委员会　关于下达2004年行业标准项目计划通知》（发改办工业［2004］872号文）的安排制定的。

随着计算机、通信和网络技术的发展，电力系统使用计算机、通信和网络技术实现调度中心、电厂、变电站之间的数据通信越来越普遍。同时，由于Internet技术已得到广泛使用，E-mail、Web和PC的应用也日益普及，随之而来的是病毒和黑客等问题。为此，国际电工委员会57技术委员会（IEC TC 57）对有关电力系统控制的数据和通信安全进行了研究，并于2003年发布了技术报告IEC TR 62210《电力系统控制及其通信　数据和通信安全》。

此外，IEC TC 57还在进行《数据和通信安全 IEC 60870－5安全及导则》（57/675/NP）、《数据和通信安全　端对端网络管理的管理信息基本要求》（57/676/NP）、《数据和通信安全 IEC 61850协议集的安全》（57/677/NP）、《数据和通信安全　包含MMS协议集的通信网络和系统安全》（57/678/NP）、《数据和通信安全　包含TCP/IP协议集的通信网络和系统的安全》（57/679/NP）等安全文件的研究和编写工作。技术报告IEC TR 62210《电力系统控制及其通信　数据和通信安全》是该系列文件的第一个。

为防止电力二次系统的计算机感染病毒和受黑客攻击，我国对电力系统二次安全防护进行了深入研究，并在此基础上发布了一系列安全防护规定。这些安全防护规定涉及面比IEC TR 62210广，内容也更深入。IEC TR 62210是在通信协议的应用层采取防护措施，与我国的安全防护规定有互补性，对我国电力系统二次安全防护具有指导意义。

本指导性技术文件等同采用IEC TR 62210：2003《电力系统控制及其通信 数据和通信安全》。

本指导性技术文件的附录A、附录B和附录C是资料性附录。

本指导性技术文件由中国电力企业联合会提出。

本指导性技术文件由全国电力系统控制及其通信标准化技术委员会归口并负责解释。

本指导性技术文件起草单位：国家电力调度通信中心、中国电力科学研究院、国电自动化研究院、福建省电力调度通信中心、华东电力调度通信中心、华中电力调度通信中心。

本指导性技术文件主要起草人：南贵林、杨秋恒、许慕梁、邓兆云、姚和平、李根蔚、韩水保、陶洪铸。

电力系统控制及其通信
数据和通信安全

1 范围和目的

本指导性技术文件适用于电力部门的计算机化的监视、控制、计量和保护系统。文件涉及这些系统的使用、访问以及内部和系统之间的通信协议有关的安全方面问题。

注：本文件不包含与物理安全问题相关的建议或开发准则。

本文件讨论了对系统及其运行的实际威胁，举例说明了安全隐患和入侵的后果，讨论了改善目前状况的行动和应对措施，但解决方案将考虑作为将来的工作项目。

2 概述

安全性和可靠性一直是电力部门中系统设计和运行的重要问题。监视、保护以及控制系统都按尽可能高的安全性和可靠性要求进行设计，已经开发了接近于零的残留差错率的各种通信协议。采取这些措施的目的是为了使危及人体及设备的风险最小，并促进电网的高效运行。

对易受攻击对象的物理威胁已经通过传统的方法，即靠封闭建筑物、围栏和警卫等方法处理，但忽略了通过搭接的通信电路伪造 SCADA 命令跳开关键开关的这种十分可能的恐怖威胁。在目前使用的协议中没有确保控制命令来自授权来源的功能。

随着电力市场解除管制又带来新的威胁：了解竞争方的资产和其系统的运行有可能获利，获取这些信息是十分可能的现实。

通信协议愈开放、愈标准化，集成到企业的和全球化的通信网络中的通信系统愈多，通信协议和系统就愈需要防范有意或无意的入侵。

本文件讨论了电力部门的安全防护过程，涉及企业安全防护策略、通信网络安全以及端对端的应用安全等。

整个系统的安全依赖于网络设备的安全，也就是依赖于能通信的所有设备的安全。安全的网络设备必须能进行“安全”的通信并能验证用户的访问级别。对各种入侵攻击的有效检测、记录和处理（起诉）必须作为主动审计系统的一部分。

对威胁的分析要基于系统的可能后果，也就是说，如一个非法入侵者既有野心又有智谋，会发生的最坏结果是什么？要把电力部门及其资产的易攻击性与威胁放在一起来分析。

在分析了电力部门的各个系统中存在对易攻击点的威胁之后，本文件着重于 GB 18657， GB 1870 和 DL 790 系列的通信协议，讨论了应对措施。

本文件还提出了在这些通信协议中列入安全议题的新工作项目的建议。

3 规范性引用文件

下列文件中的条款通过本文件的引用而成为本文件的条款。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文件，然而，鼓励根据本文件达成协议的各方是否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文件。

GB 18657（所有部分）远动设备和系统　第 5 部分：传输协议（IDT IEC 60870--5）

GB 18700（所有部分）远动设备和系统　第 6 部分：与 ISO 标准和 ITU-T 建议兼容的远动协议（IDT IEC 60870－6）

GB/T 9387.1－1998 信息技术　开放系统互连　基本参考模型　第1部分：基本模型（IDT ISO/IEC 7498－1：1994）

GB/T 9387.2－1995 信息处理系统　开放系统互连　基本参考模型　第2部分：安全体系结构（IDT ISO/IEC 7498－2：1989）

DL 860（所有部分）变电站通信网络和系统（IDT IEC 61850）

DL 790（所有部分）采用配电线载波的配电自动化（IDT IEC 61334）

ISO/IEC 10181－1：1996 信息技术　开放系统互连　开放型系统安全框架：概述

ISO/IEC 10181－7：1996 信息技术　开放系统互连　开放型系统安全框架：安全审计和报警框架

ISO/IEC 15408－1　信息技术　安全技术　IT 安全评估标准　第1部分：引言和基本通用模式

ISO/IEC 15408－2　信息技术　安全技术　IT 安全评估标准　第2部分：安全功能需求

ISO/IEC 15408－3　信息技术　安全技术　IT 安全评估标准　第3部分：安全保障需求

4　术语、定义和缩略语

下列术语和定义适用于本标准。

4.1　术语和定义

4.1.1

可追溯性　accountability

确保一个实体的活动可以被唯一地追溯到该实体的特性。

4.1.2

资产　asset

对组织有经济价值的任何事物。

[ISO/IEC TR 13335－1：1997]

4.1.3

真实性　authenticity

确保一个主体或资源的身份与声称相一致的特性。真实性适用于实体，如用户、过程、系统和信息。

4.1.4

违反授权　authorization violation

为一个用途而被授权使用某个系统的实体，将该系统用于另一个未经授权的用途。

4.1.5

可用性　availability

只要被授权实体需要就能访问和使用的特性。

[ISO7498－2：1989]

4.1.6

安全底线控制　baseline controls

为系统或组织所设定的最低的安全防护的集合。

[ISO/IEC TR 13335－1：1997]

4.1.7

机密性　confidentiality

使信息不被未经授权的个人、实体或过程使用或不泄露的特性。

[ISO 7498－2：1989]

4.1.8

数据完整性　data integrity

使数据不被未经授权方式改变或破坏的特性。

[ISO 7498－2：1989]

4.1.9

拒绝服务　denial of service

授权的通信流被有意阻遏。

4.1.10

窃听　eavesdropping

信息被暴露于监视通信信号的未授权人员。

4.1.11

黑客　hack

以下一种或多种威胁的组合：违反授权、信息泄露、完整性破坏和伪装。

4.1.12

散列函数　hash function

将大的（可能非常大的）数值集合的各数值映射到较小数值范围的数学函数。

4.1.13

信息泄露　information leakage

未经授权实体获得安全信息或受限制的信息。

4.1.14

完整性破坏　integrity violation

信息被未经授权实体生成或修改。

4.1.15

截获/篡改　intercept/alter

通信包被截获、修改，然后像原通信包一样继续发送。

4.1.16

伪装　masquerade

未经授权实体企图假装可信方的身份。

4.1.17

可靠性　reliability

预期行为和预期结果一致的特性。

[ISO/IEC TR 13335－1：1997]

4.1.18

重放　replay

通信包被记录，然后在不适当的时间再次传送。

4.1.19

抵赖　repudiation

发生信息交换后，交换的两个实体之一否认这次交换或否认交换的内容。

4.1.20

残留风险　residual risk

在实施安全防护后剩余的风险。

[ISO/IEC TR 13335－1：1997]

4.1.21

资源耗尽　resource exhaustion

参见“拒绝服务”。

4.1.22

风险　risk

某一给定威胁充分利用一个或一组资产的安全隐患造成资产损失或破坏的可能。

[ISO/IEC TR 13335－1：1997]

4.1.23

安全审计员或安全审计程序　security auditor

被允许访问安全审计的踪迹记录并以此生成审计报告的个人或过程。

[ISO/IEC 10181－7：1996]

4.1.24

安全机构　security authority

负责定义、实施或强制执行安全防护策略的实体。

4.1.25

安全域　security domain

安全域是元素的集合、安全防护策略、安全机构以及与一套安全相关的活动。其中元素的集合按照安全防护策略从事指定的活动，安全防护策略由安全域的安全机构管理。

4.1.26

安全域机构　security domain authority

安全域机构是负责实施安全域安全防护策略的安全机构。

4.1.27

安全令牌　security token

安全令牌是由一个或多个安全服务保护的一组数据，与提供这些安全服务使用的安全信息一起，在通信实体之间进行传送。

4.1.28

安全相关事件　security-related event

已经由安全防护策略规定为可能违反安全或与安全有关的任何事件。达到预定义的界限就是安全相关事件的实例。

4.1.29

欺骗　spoof

一种或多种以下威胁的组合：窃听、信息泄露、完整性破坏、截获/篡改及伪装。

4.1.30

系统完整性　system integrity

系统以不受损害方式执行其预定功能的特性，不受有意或无意未经授权的系统操作影响。

[ISO/IEC TR 13335－1：1997]

4.1.31

安全威胁　threat

可能产生导致有损于系统或组织的有害偶发事件的因素。

[ISO/IEC TR 13335－1：1997]

4.1.32

信任　trust

当且仅当实体 X 就一组行为以一种特殊方式表现出它依赖于实体 Y，就称实体 X 在这组行为上信任实体 Y。

4.1.33

可信实体　trusted entity

假设已适当地执行各种安全对策的实体。有了这假设，该实体可以有理由免除其他安全对策。

例如：一个可信的授权实体声明一个用户被授权可以进行控制，因而不需采用通常需要的质询认证过程。

实体可能违反安全防护策略，例如执行安全防护策略所不允许的动作或者无法执行安全防护策略所允许的动作。

4.1.34

脆弱性 vulnerability

脆弱性包括资产或一组资产的弱点，它可用威胁说明。

[ISO/IEC TR 13335－1：1997]

4.1.35

已开发的技术 developed technology

在EAL－5级质量及安全保障导则或者为更高级别的ISO/IEC 15408－3中所规定的配置和指导下所开发的软件代码或算法。

4.2 缩略语

AMR	Automatic Meter Reading	自动抄表
CC	Common Criteria	通用准则
COTS	Commercial off the Shelf Software	现货供应的商业软件
DISCO	Distribution Company	配电公司
DLC	Distribution Line Carrier	配电线载波
DLMS	Distribution Line Messaging System	配电线报文系统
DMS	Distribution Management System	配电管理系统
EAL	Evaluation Assurance Level	安全保障评估等级
EMS	Energy Management System	能量管理系统
GENCO	Generation Company	发电公司
HMI	Human-Machine Interface	人机界面（如：操作员工作站）
HV	High Voltage	高电压
IED	Intelligent Electronic Device	智能电子设备
IT	Information Technology	信息技术
LAN	Local Area Network	局域网
LV	Low Voltage	低电压
MMS	Manufacturing Message Specification	制造报文规范
MV	Medium Voltage	中电压
NT		Windows NT,是微软视窗个人计算机操作系统，专为需要先进性能的个人用户或商务而设计
OASIS	Open Access Same-Time Information System	开放访问即时信息系统
PLC	(user)Programmable Logic Controller	（用户）可编程逻辑控制器
POTS	Plain Old Telephone System	普通老式电话系统
PP	Protection Profile	防护方案
RTU	Remote Terminal Unit	远方终端设备
SCADA	Supervisory Control And Data Acquisition	监视控制和数据采集
ST	Security Target	安全目标

TASE	Telecontrol Application Service Element	远动应用服务元素
TCP/IP	Transmission Control Protocol/Internetworking Protocol	传输控制协议/网间协议
TOE	Target of Evaluation	评估目标
TRANSCO	Transmission Company	输电公司
VAA	Virtual Application Association	虚拟应用关联
VDE	Virtual Distribution Equipment	虚拟配电设备
WAN	Wide Area Network	广域网

5 安全问题介绍

通信和信息安全正成为商业或私有部门信息网络的一个基本要求。对于用通信和信息技术作为关键服务基础设施或关键服务组成部分的部门特别是这样。中断这些服务（例如中断供气、供水、供电）可能影响到广大地区及大量的个人和公司。

无论在公司内部还是公司之间，通信网络化和信息交换在电力基础设施内正日益普遍。尽管在过去，公用事业部门牢牢把握着他们的信息并且控制着他们通信基础设施的大部分，但这已成为历史。在共享通信网络以及公共网络上信息交换愈来愈多。这种趋势使不可信方（如黑客、低素质的员工和恐怖分子）会考虑采取系统性的攻击。这种趋势以及大量可在攻击中使用的技术，预示着攻击数量会更多，攻击得逞的几率也会上升。

注：几乎没有能推导出未来威胁模型或攻击模型的公开的可用信息。然而，这方面信息的缺乏并不意味着没有发生攻击，而只说明公用事业部门检测攻击的工作不到位，或这类攻击的信息没有公开发表。另外，攻击几率不断上升的趋势可能反映财务动机在不断增长（例如由于解除管制）和容易进行攻击（例如由于技术进步）。

不像军队那样，计算机或公用事业部门的信息系统和协议的大多数用户基本上或还没有意识到对他们的信息和基础设施的可能威胁。更糟的是，虽然用户有时意识到但不重视着手解决已知的安全风险。目前，偶发事件（检测到的攻击）的次数还相对较低。然而，检测出的攻击日益增多而且已经证实主要基础设施（如煤气、水和电）都是极易被攻击的。

可以从多方面考虑安全问题，本文件仅涉及通信安全。它不涉及计算机系统内与信息安全有关的安全问题，而只针对信息通过 IEC TC 57 规定的一些协议传送时的信息安全。

本文件的使用方法：本文件是用于向 IEC TC 57 及其工作组提出建议，可视为建立新工作项目的基础，而不应视为已经完善。

应进一步考虑与其他 IEC 技术委员会（TC）建立密切的联系，这样，他们也能考虑本文件提出的建议。

6 安全分析过程

本文件的建议将直接影响常规的企业安全防护过程，而且必须以与这个过程一致的方式来构想建议。因此，理解典型的企业安全防护过程的需求以及它们对本文件范围的影响是很重要的。

图 1 描绘了那些通常认为是常规企业的安全防护策略，这些企业需要建立相对“安全”的公司基础设施。图 1 清楚地表明，为了建立安全的企业基础设施，企业安全防护策略必须先由企业管理者制定和采纳。

企业安全防护策略的规则涉及安全域、安全域机构、安全审计员（或安全审计程序）的责任规定和指派。此外，一旦企业安全防护策略付诸行动和实施，通常就决定了可接受的残留风险。很明显，企业会制定自己的安全防护策略，不一定要依靠本文件的建议。

然而，向企业管理者说明本文件论及的通信协议相关的威胁和后果，却在本文件的范围内。所以，企业安全防护策略应仔细对照本文件的以下部分：

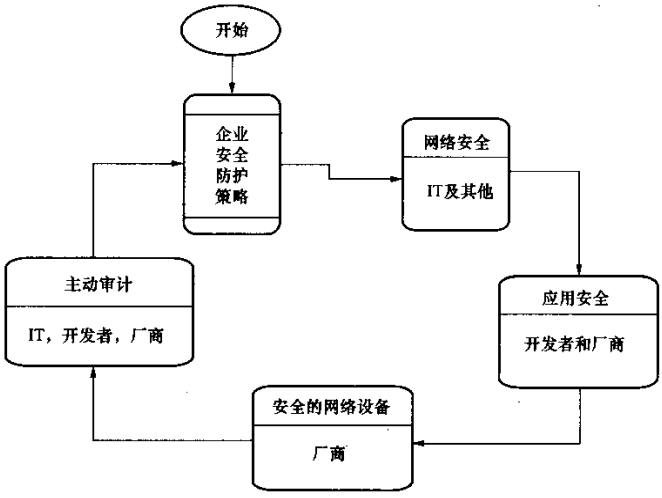

图 1　常规的企业安全过程

a）定义（见 4.1）：有助于建立一致的词汇表；

b）在防护方案（PP）中考虑的特定威胁（见 7.2.3）：列出了这种威胁的集合及它们的定义，这些在本文件中论及；

c）安全隐患（见第 8 章）：涉及已知存在于本文件讨论的通信协议中的通信系统安全隐患；

d）安全分析过程（见第 6 章）：也许这是企业安全防护策略编制人员所关心的，但这更应是企业安全防护策略团队其他成员关心的。

企业的安全防护策略往往针对某个防护目标层面，因此应使用所关心的章节以有助于对防护目标制订方案，并告知企业的管理者。不管怎样，企业防护目标都要转化为在网络安全、应用安全以及安全网络设备防护过程中的实施策略以及各安全对策。

应用安全主要涉及端对端的应用层面的安全。安全防护步骤需要强有力和明确的指导，这样主计算机的应用才只需要一些适当的限制、维护和审计。本文件不讨论基于主机应用的防护技术和方法。

在企业安全防护过程中网络安全通常涉及对防火墙和子网的访问。在这个域中的安全防护策略必须解决由一个子网到另一个子网的访问权限问题。本文件对网络安全的企业安全防护策略过程没有任何直接影响。

然而，应用的用户和通过远程通信与终端设备和应用批准的权限之间的关系很密切。所以，在制定安全防护策略时主要应考虑以下问题：

a）某些应用可能需要根据使用哪台主机或终端来确定安全权限。

例如，在 SCADA 主站中，可以允许任何经认证的终端或用户看 SCADA 信息，但是，只有位于物理安全（如控制中心）环境中的终端才有权真正控制远方设备或进行远方应用，或改变其配置。

在以上例子中，即使应用的用户有相应的权限，这权限还会进一步受到执行应用的主机或终端的限制。

b）某些应用可能需要制定它们自己的安全防护策略，虽然这很少见。

对不一定能确定应用用户的共享应用尤其如此（如 NT 的服务）。

因此，建议在构建应用安全防护策略时要考虑的层次是：

a）能否通过远方应用进行用户认证并把它转换成可用信息；

b）用户认证的场所能否确定；

c）应用执行的网络位置能否确定。

从通信的角度看，最安全的是制定这样的安全防护策略：可以通过远方设备或远方应用来认证用户

而不仅认证用于连接的节点。

安全网络设备：本文件主要论及可以增强电力部门联网设备的安全性的问题、技术和建议。根据本文件的目的，“联网设备”是指任何能互相通信的设备。

本文件的读者应明确，通信系统的总体安全将由联网设备的安全程度来决定，这一点很重要。这主要是因为设备是大多数信息的来源，也是能直接影响电力部门服务的实体（例如断开一个开关导致了停电）。所以，重要的是这些设备有能力鉴别用户的访问级别。另外，更为重要的是这些设备能成为审计过程的一部分，从而使攻击能被迅速检测、应对和起诉。

多数电力部门不愿在安全防护方面开销额外费用，然而安全教育和本文件将论及许多问题，并就为什么说目前实施得不够作有力的陈述。

主动审计：作为连续的企业安全防护过程的一部分，对任何一套安全防护策略和实施都必须不断进行监视和修正。如没有能力去审计和分析安全攻击、系统的运行及系统的薄弱点，一个安全的系统最终将变得不安全。

为了具备主动审计过程和连续的企业安全防护过程，必须有人专门致力于这项工作。因此，需要对电力部门进行与采取这样措施有关的风险的教育。在还没有遭受一次得逞的攻击之前，要证明这种过程的投入效益，即使不是完全不可能，也是很困难的。需要用如不实施安全防护过程会具有怎样可能风险的代价来证明它。

该过程的所有部分都需要仔细研究，并针对特定的环境进行取舍。但是所有方面都需要加以分析，并在某些方面着手解决。

6.1 网络拓扑

可以用很多不同方式来观察通信拓扑结构。就高层说来，分析信息源和使用者之间的信息流是必需的。见图 2。

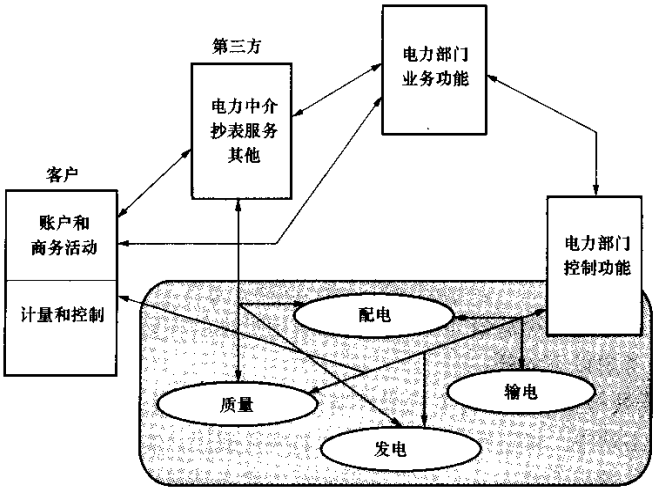

图 2 业务信息流

图 2 中有以下几种主要业务实体：

a）客户：这个业务实体代表电力和服务的消费者。有一些为客户期望的服务类型，从出电费账单到电力质量控制作为送电的一部分来提供。客户通常期望以下服务：

1）账户和商务活动：包括客户服务、出单和购电售电（电力中介）。在这些活动之间进行信息交换的方法通常是电话、传真或电子邮件。但发展趋势是通过互联网或其他电子商务方法进行信息交换。

此外，这些信息交换现在不仅可通过电力部门的业务功能提供，也可由第三方提供。在许多

情况下，两个相互竞争的组织常常可以在同一信息基础设施上和同一客户进行信息交换。

2）计量和控制活动：这些活动主要与控制供电和控制送达终端客户的电力质量的通信有关。即使可以委托第三方监视营业表计信息，但抄表是当地配电部门的责任。

b）第三方：解除电力行业管制的趋势导致多种业务实体出现，这些实体代理电力部门，执行第三方表计的读数和出单，还提供其他服务。第三方与客户以及电力部门业务功能交换信息，也可能直接监视营业表计和电力的质量。

c）电力部门业务功能：这些功能向客户和第三方（按法律要求）提供信息。在解除管制的环境中，可能需要将这些活动的一部分看作相当于第三方。

d）电力部门控制功能：这些功能是当前提供的典型的 SCADA、EMS、DMS 功能。控制功能包括决定发电，配电或电力产品的质量的所有活动。而通信活动的范围包括配电自动化、电力部门到电力部门、电力部门到变电站、电力部门到发电厂等。

本文件的主题是确定在 IEC TC57 范围内使用的通信类型和对这些技术的威胁的影响。然而，许多威胁涉及到通信体系结构和通信拓扑结构中的弱点。在最高层，如图 2 所示，业务实体之间任何直接或间接的接口点出现安全相关事件的几率都很高。然而，为了保护接口点上已有的信息，以及为了推荐适当的安全防护策略规则，需要讨论这些接口点的实际通信拓扑结构。

客户对可能的三种不同的业务实体实际上有两个主要接口点，如图 2 所示。然而，用于账户活动和商务活动功能的拓扑结构通常基于电子商务或因特网技术（或拓扑结构）。但是，计量和控制功能表现为类似于电力部门所使用的质量、配电、输电、发电和变电站那样的拓扑结构。

图 3 表示连接一个或多个设备或数据源的主通信路径和可选的第二通信路径。这些路径中任何一条都可能是引入安全威胁的接口。对每个接口点，甚至对实际设备，都需评估它的风险。作为安全分析的一部分，协议和通信介质也往往会涉及风险。本技术文件的范围是根据这些因素确定主要威胁的影响，并在此分析基础上提出安全底线控制的建议。

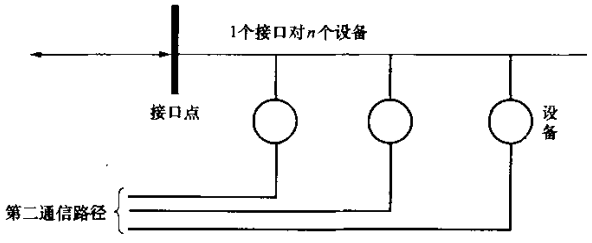

图 3　通常的通信拓扑

6.2　基于用户后果的安全分析

很明显，信息的重要性以及公司因此而愿意为保护信息付出的努力是极具主观性的。信息的重要是由实体或被攻击方根据得逞的攻击对其业务或其利益的后果决定的。为此制订了基于被攻击方和后果的安全分析方法。

6.2.1　被攻击方

被攻击方的定义是：业务过程会遭受攻击得逞影响的任何实体。对本技术文件[1)]来说，图 2 中能识别为被攻击方的是：

a）发电公司（GENCO）：这些业务实体的最终产品是电力，它们在发电设施上常投资很多。

b）输电公司（TRANSCO）：这些业务实体的最终产品是传输发电公司生产的电能。一般是向配电公司传输电能。输电公司常是发电公司的客户。

1）被攻击方和业务过程的定义及叙述可能随区域而不同。详情要向相应的区域管理机构查询。

c）配电公司（DISCO）：这些业务实体的最终产品是把电能交付给客户。这些被攻击方在很大地域范围内分布有资产及通信的要求，并服务于很多客户。配电公司是输电公司的客户。

d）数据汇集者：这些业务实体为每个供电商汇集客户抄表数据，大批量地处理数据，计算支付给每个发电公司、输电公司和配电公司的电能和传输设施的使用费用。

e）表计服务提供者：这些业务实体提供安装、维护（表计运行）以及读取客户表计（数据收集）的服务。

f）供电商：这些业务实体从批发市场上购电再售给各终端客户，他们的运营不受网络地域限制，并向配电公司支付系统使用费。

g）风险管理市场参与者：这些业务实体以出售、交易、中介或其他派生的财务行为而参与市场。派生财务行为的例子是期货、期权、现买现卖、期货的期权、以货易货或设立和交易其他有价证券。他们的目的是控制与前期的电能购销合同相关的电能价格波动和非预期事件的风险。

h）终端客户：这些是业务实体或个人，他们购买电能或电力部门的服务，并需确认合同的约定是否在履行。

每个被攻击方可能要求来自一个或多个业务活动的信息。因而，为了确定本技术文件应当集中分析的范围，已设计出这些活动的矩阵表。

表 1 是为一般的被攻击方和业务过程考虑的矩阵表。“×”号表明某特定被攻击方需要的或能提供的与该特定业务过程有关的信息。被攻击方或业务过程的区域性变化可以通过这些类别的组合形成。

表 1　确定业务过程重要性的矩阵表

业务过程	被攻击方							
	发电公司	配电公司	输电公司	数据	表计	供电商	风险管理	终端客户
购电售电	×					×	×	×
发电（包括电力质量）	×	×	×	×	×	×	×	×
输电（包括电力质量）	×	×	×	×	×	×		
配电（包括电力质量）		×	×	×	×	×		×
交易计量（营业抄表）	×	×	×	×	×	×		×
资产管理	×	×	×		×			
节能	×	×	×			×		×
信息挖掘				×		×	×	
第三方资产借用[a]						×		×
风险管理	×					×	×	×
a　这方面的例子是为用于其他业务过程的资源提供互联网连接。								

被攻击方并不与业务组织一一对应，这一点对于理解表 1 是很重要的。例如，似乎应将“×”号放在“第三方资产借用”行和“配电公司”列交叉点的方块中，因为具有配电公司作用的业务组织会对借出它的配电线路（例如用以承载消息通信）感兴趣。然而，提供消息传送市场的业务活动是供电商的活动，不是配电公司的活动。这样，即使该业务组织或许被认为是配电公司而不是供电商，“×”号还是在“供电商”列中，而不在“配电公司”列中。

根据对被攻击方利害关系和业务过程的分析，需要防护的最重要的业务过程是：

a）发电；

b）输电；

c）供电；

d）交易计量；

e）资产管理；

f）节能。

6.3 需要考虑的后果

为了进行基于后果的安全分析，要确定被攻击方和他们的业务实践需考虑的主要后果。对于在IEC/TC 57中被推荐为今后安全工作的焦点的那些业务过程，需要考虑的主要的后果的类别是：财务、资产破坏及降级，以及无法恢复服务。

6.3.1 财务类后果

财务类后果包括导致一个被攻击方财务损失或另一个被攻击方获益的任何活动。财务后果也受到资产损失或资产降级的影响（见6.3.2）。产生财务后果的活动或事件如下：

6.3.1.1 收入损失

收入损失可能由以下一些因素引起：

a）不断增加的竞争

例如，由于被攻击方的系统缺乏安全防护，竞争者合法地或非法地入侵被攻击方的市场。这也可能是被攻击方本身信息泄漏的结果。

b）客户流失

可能由于以下事件而使被攻击方的客户不稳定：

——合同争议；

——定价无竞争力；

——缺乏信任，例如由消费者信用低引起；

——服务的可靠性降低；

——无交付服务的能力；

——对市场波动和趋势的反应迟缓；

——对消费需求的反应迟缓。

c）无能力赢得客户

被攻击方可能因为与上述类似的原因而不能赢得客户，例如对市场波动和趋势的反应迟缓、定价无竞争力等。不能赢得客户也可以由客户流失，信誉败坏导致。

6.3.1.2 收益率降低

收益率可能由于以下原因降低：

a）产品资源成本上升；

b）现金周转困难。

这可能由于一些事件引起：例如内部人士的电力期货交易买空卖空，对账单数据库的攻击导致无法开账单等。

6.3.1.3 篡改生产数据和消费数据

可能由于以下原因引起：

a）抄表信息错误，例如故意篡改消费数据或生产数据；

b）需求预测错误；

c）在汇集或开账单时改动计量信息；

d）信息丢失。

6.3.1.4 人为的股票价值降低

以上任何活动或事件都可以导致股票价值降低，然而也有其他违法事件可以人为地引起股票价值变动：

a）谣言；

b）分析人员的预测。

6.3.2 资产破坏或降级

本类后果包括所有因无法完成资产所需要的服务或运作而有意地或无意地导致资产破坏或降级的活动。这类活动或事件有：

a）不恰当的资产运作；

b）不恰当的资产维护；

c）没有得到适当的保护或安全防护；

d）人力资源过度消耗。

可能会受到攻击并应成为分析的组成部分的典型资产有：

a）电力系统资源（电力线路、变压器、发电机、母线等）；

b）控制系统（SCADA，EMS 等）；

c）抄表系统（数据采集、表计等）；

d）信息系统（例如 OASIS）。

表 2 表明了这些资产和它们的信息与具体的业务过程的关系。另外，表中也注明了已知的有关 IEC 技术委员会（IEC TC）。

表 2 资产与业务过程的关系

资产的业务过程	EMS（IEC TC 57）	SCADA（IEC TC 57）	发电机（IEC TC×x）（IEC TC 57）	电力线（IEC TC 38）（IEC TC 57）	变压器（IEC TC 14）（IEC TC 57）	开关设备（IEC TC 17）（IEC TC 57）	抄表值（IEC TC13）（IEC TC 57）	信息系统（TC ××）
购电售电	√		√				√	√
发电（包括电力质量）	√	√	√		√	√	√	√
输电（包括电力质量）	√	√		√	√	√	√	√
配电（包括电力质量）	√	√		√	√	√	√	√
交易计量（营业抄表）		√	√	√			√	√
资产管理	√	√	√	√	√	√	√	√
节能	√	√	√				√	√
信息挖掘		√					√	√
第三方资产借用				√	√			√
风险管理	√	√						√

6.3.3 无法恢复服务

本类后果包括有意或无意地导致被攻击方无法维持必需服务的各种活动。导致这种情况的活动或事件有：

a）相关服务或运行必需的信息丢失；

b）由于对电网状态理解不正确而导致信息错误；

c）资产损失或降级（参看 6.3.2）；

d）人员动作不恰当（或不动作）；

e）不能对收到的正确信息作出反应（例如数据泛滥）；

f）通信容量耗尽；

g）其他资源枯竭。

6.4 后果和安全威胁

现在已经定义了进行基于可能业务后果的安全分析的必要条件。它们是：

a）确认在通信环境中的被攻击方；

b）确认与被攻击方有关的业务过程；

c）确认对业务过程会产生不利影响的后果；

d）确认能使后果成为现实的事件。

如攻击得逞，下一步是确定能使后果成为现实的安全威胁。

图 4 给出了“无法恢复服务”后果的一部分的示例分析。

图 4 表明“资产损失”能导致无法恢复服务（后果）。下一步是分析什么事件或什么事件序列会导致“资产损失”。

会导致“资产损失”的事件序列可能经若干途径发生。然而，所有涉及通信的途径都判定为“拒绝服务”或“违反授权”的攻击得逞导致的后果。

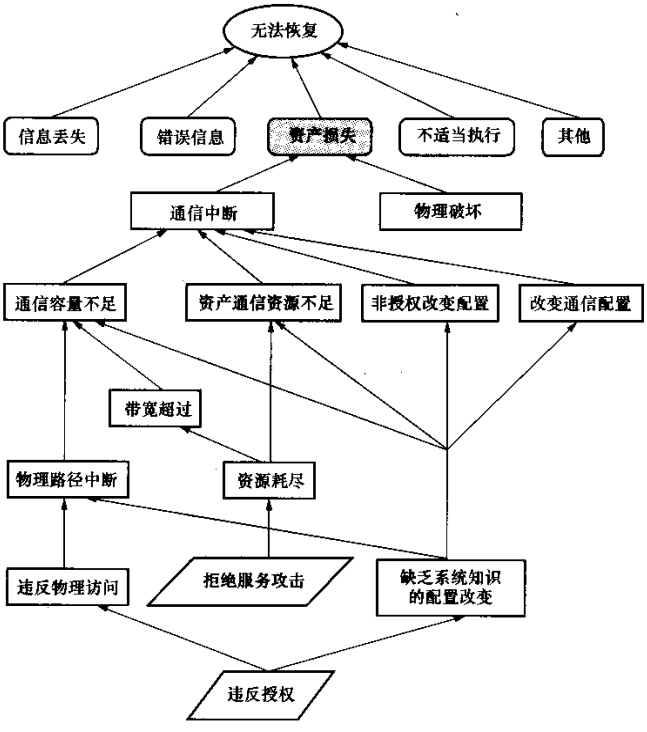

图 4 “无法恢复服务”后果图

注：附录 C 中列出了一个后果图示例。但电力部门为了确定要应对（或至少要检测）的那些主要安全威胁，需作出更详细更完整的后果图。

7 本文件安全工作的焦点

如要对 IEC TC 57 主持下所有协议进行全面的安全分析，并提出防护措施建议，需要编写数量惊人的文件。另外，发布本文件有时间限制，只能对一些重点进行分析。

因此，本文件的重点在于采用各种 IEC TC 57 协议的通信框架时，被认为是最易受攻击的范围，以及可以最大程度降低风险的防护措施。为了确定本文件的重点，下面按照通信模型简要说明通常考虑的威胁和风险。所考虑的通信参考模型为 OSI 7 层通信参考模型（ISO/IEC 7498－1）。

7.1 应用层安全焦点的论证

应指出，根据后果分析，可能需要应对不同的各种攻击。然而，一般安全技术或防护技术通常适用于以下几层：物理层、传输层、应用层。对通信模型安全矩阵表的仔细研究表明，在应用域或用户域内适当采用安全功能，就可以应对绝大多数可能发生的典型的安全威胁。另外，只有在应用层的采取安全防护措施，才能使未经授权的访问和非法使用带来的安全风险降到最低。

表 3 详述了已知的与 OSI 层几个通信功能有关的典型安全风险。本技术文件将着重于应用层的安全问题。建议将来进行更低层的工作，考虑从传输层开始。

表 3 通信模型安全矩阵表

层	通信功能	典型风险	典型安全攻击
应用层	以标准协议传送用户信息或业务信息	信息泄漏[a] 未经授权访问 非法使用 拒绝服务	伪装 旁路控制 违反授权 服务欺骗 信息截获/更改/重放 拒绝服务 资源耗尽
表示层	将本地表示转变为标准的或熟知的传输表示	信息泄漏	
会话层	维护面向连接的会话	信息泄漏	
传输层	维护面向连接的会话	信息泄漏 拒绝服务	拒绝服务 资源耗尽
网络层	在通信段之间选择路由（如从局域网到广域网）	信息泄漏 拒绝服务	拒绝服务 伪装 信息截获/更改/重放
链路层	本地寻址以及介质访问算法的实现	信息泄漏 拒绝服务	拒绝服务
物理层	传输介质的物理接口以及任何需要的调制	信息泄漏 拒绝服务	物理破坏 窃听 拒绝服务
a 信息泄漏可能通过直接（例如包解码）或间接（例如流量分析）方式产生。			

7.2 安全分析技术

建议用基于后果的安全分析（见 6.2）给对系统的有关威胁列表。应将这些威胁用作推荐的正式文档方法的输入。

在全面研究了几种不同的安全问题的文档方法之后，建议 IEC TC 57 为此目的采用 ISO 15408 国际标准。ISO 15408 详述了如何制定防护方案（PP）、评估目标（TOE）和安全目标（ST）。

根据 ISO 15408 的定义，防护方案叙述评估目标的假设，确认对基于这些假设的 TOE 的威胁，制定应对威胁的具体防护目标，并最终确定满足这些具体防护目标的安全防护功能。PP 的实施被定义为能抵御安全威胁及攻击的安全目标。

然而，IEC TC 57 面临的工作要求制定多个 TOE，应将 7.2.1、7.2.2、7.2 用作制定适当的 TOE 的基础。建议 IEC TC 57 为在电力行业中使用的 IEC TC 57 的协议制定 TOE。作为 IEC TC 57 未来工作项目，建议第一组 TOE 包括：

a）IEC 60870—6 TASE.2;

b）IEC 60870－5；

c）IEC 61334；

d）IEC 61850。

在本文件发布时，尚未决定是否需要为 IEC TC 57 第 13、14 工作组的成果制定 TOE。将来还需要考虑系统或应用的其他特定的 TOE（例如密钥管理、系统级认证及企业系统等。）

注：附录中有更多细节及一个防护方案的示例。

7.2.1 安全防护目标

安全防护目标及功能包括：

a）保密性：确保信息没有透露给未经授权人员；

b）完整性：确保系统中的信息是它的固有表示，即信息是预期的，确保信息未被未经授权人员改动、生成或删除；

c）可用性：确保信息处理资源不会因恶意动作而无法使用；

d）不可抵赖：确保以电子方式作出的协议能被证明已经完成；

e）管理：安全防护系统的管理；

f）起诉：可能需要根据适用的法律起诉，从而能够并推动用合法行动打击恶意犯罪分子。

7.2.2 一般威胁

威胁针对业务过程和/或被攻击方（见 6.2.1 中的定义）使用的资产或信息。威胁的来源包括：

a）自然灾害；

b）设备故障；

c）合法用户的疏忽行为影响到防护不够的系统；

d）合法用户超出授权限度的恶意行为（内部威胁）；

e）入侵者连贯地或逻辑地渗透入系统；

f）入侵者不连贯地或非逻辑地渗透入系统；

g）战争；

h）人为或计算机出错；

i）上述几项的组合。

7.2.3 防护方案考虑的特定威胁

下面一些表包含了针对采用 IEC TC 57 通信协议的远动系统和远方保护系统的预计的可能威胁。这些威胁针对端系统以及端系统之间的通信。对每种特定实例，可能只适用威胁的某一子集。并不是所有的威胁都适用于每一个实例。例如，对未与其他系统互连的远动系统或远方保护系统而言，就没有用远动系统或远方保护系统来攻击其他互连系统的威胁。与此相似，对不将签订电子协定作为其功能的远动系统或远方保护系统而言，就没有抵赖威胁。

这里，确定威胁所使用的形式是便于在公共准则下准备防护方案文件时使用这些威胁。其意图是简化防护电力远动、远方保护设备/系统中所使用产品的防护方案的最终准备过程。一个公共准则的防护方案文件表述了用户的防护要求。所提供产品的防护描述包含在安全目标文件中。这些文件及其他文件还定义了产品测试和其他应遵守的保障过程。这些公共准则的标准意在促进能符合规定要求的合格产品的开发，以及促进需要安全保护的系统需求方与系统供应商之间进行需求和所提供能力的交流。

自然灾害的威胁不在本技术文件的讨论范围以内。

7.2.3.1 至 7.2.3.4 列出了一组威胁定义。它们定义了通常适用于系统级评估目标的威胁（一般威胁），也定义了一组可用于协议的威胁（协议威胁）。

这些威胁定义是定义一个系统威胁的总表的第一步，这总表可以作为建立一个包含多个评估目标的系统的结果。

通常，威胁定义有其层次：一般威胁、协议威胁、TOE 特定威胁（例如定义为 TOE 开发的一部分

的特定威胁)。

7.2.3.1 保密性威胁

7.2.3.1.1 一般保密性威胁

T.CONF 1	授权用户不适当地获得未经授权的 TOE 信息
T.NOAUT-VIEW	未经授权用户查看 TOE 数据
T.CONF 2	授权用户不适当地访问 TOE 而获得来自其他互联系统的未经授权的信息
T.CONF 3	入侵者用 TOE 渗透，获得未经授权的来自其他互联系统的信息
T.TRAFFIC-ANALYSIS	入侵者通过观察报文通信方式或其他特点推断未经授权的信息，而对这些报文通信的访问或未经授权，或仅授权加密形式的访问，这取决于通信采用的介质和相关国家用于该介质的法律

7.2.3.1.2 协议保密性威胁

T.NOAUT-VIEW	未经授权用户查看 TOE 数据
T.TRAFFIC-ANALYSIS	入侵者通过观察报文通信方式或其他特点推断未经授权的信息，而对这些报文通信的访问或未经授权，或仅授权加密形式的访问，这取决于通信采用的介质和相关国家用于该介质的法律

7.2.3.2 完整性威胁

7.2.3.2.1 一般完整性威胁

T.INTEG 1	授权用户在未经授权可命令或操作某 TOE 的情况下，向 TOE 恶意下达命令或非法操作
T.INTEG 2	入侵者未经授权命令或操作某设备，通过伪装 SCADA 主站或修改和重新传输 SCADA 主站发出的合法报文而下达命令和非法操作设备
T.HIJACK	入侵者通过劫得的已认证的关联，非法操作 TOE
T.REPLAY	入侵者通过重放旧报文，导致 TOE 的非法操作或传输旧信息
T.IMPERSONATE	未经授权用户伪装成授权用户身份
T.CHANGE	敌对方修改或破坏 TOE 数据
T.INTEG 3	授权用户未经授权访问某远方设备而将错误参数恶意装入该设备
T.INTEG 4	授权用户不适当地访问 TOE，将错误信息放入未经授权的其他互联系统
T.INTEG 5	入侵者侵入 TOE，将错误信息放入未经授权的其他互联系统

7.2.3.2.2 协议完整性威胁

T.INTEG 2	入侵者未经授权命令或操作某设备，通过伪装 SCADA 主站或修改和重新传输 SCADA 主站发出的合法报文而下达命令和非法操作设备
T.HIJACK	入侵者通过劫得的已认证的关联，非法操作 TOE
T.REPLAY	入侵者通过重放旧报文，导致 TOE 的非法操作或传输旧信息
T.IMPERSONATE	未经授权用户伪装成授权用户身份
T.CHANGE	敌对方修改或破坏 TOE 数据

7.2.3.3 拒绝服务威胁

7.2.3.3.1 一般拒绝服务威胁

T.AVAIL 1	授权用户恶意拒绝对 TOE 访问
T.AVAIL 2	入侵者恶意拒绝对 TOE 访问
T.AVAIL 3	授权用户不适当地访问 TOE，恶意拒绝授权合法用户使用其他互联系统
T.AVAIL 4	入侵者访问 TOE，恶意拒绝授权合法用户使用其他互联系统

7.2.3.3.2 协议拒绝服务威胁

T.DENIAL-OF-SERVICE	用户恶意拒绝对 TOE 访问，是 T.AVAIL 1 和 T.AVAIL 2 的组合

7.2.3.4 抵赖威胁

7.2.3.4.1 一般抵赖威胁

T.REPUD1	授权用户抵赖 TOE 事务

7.2.3.4.2 协议抵赖威胁

还未识别出来。

7.2.3.5 管理威胁

7.2.3.5.1 一般管理威胁

T.ADMIN1	授权用户无意操作 TOE，而该操作按策略未得到授权，但并不违反该系统的任何授权限制（该系统的授权并不反映该组织的策略）
T.ADMIN2	授权用户不适当地获得对安全功能的未经授权访问
T.ADMIN3	入侵者获得对安全功能的访问
T.ADMIN4	授权用户不适当地停止功能或改变参数，以避免未经授权活动被记录
T.ADMIN5	入侵者停止功能或改变参数，以避免未经授权活动被记录
T.ADMIN6	授权用户不适当地对记录系统进行拒绝服务攻击（例如强迫存储容量溢出），以避免未经授权活动被记录
T.ADMIN7	入侵者对记录系统进行拒绝服务攻击（例如强迫存储容量溢出），以避免未经授权活动被记录
T.ADMIN8	授权用户不适当地删除未经授权活动的记录
T.ADMIN9	入侵者删除未经授权活动的记录

7.2.3.5.2 协议管理威胁

T.ADMIN3	入侵者获得对安全功能的访问
T.ADMIN7	入侵者对记录系统进行拒绝服务攻击（例如强迫存储容量溢出），以避免未经授权活动被记录
T.ADMIN9	入侵者删除未经授权活动的记录

8 安全隐患

8.1 针对拓扑结构的威胁

图 3 的通常通信拓扑模型可用图 5 的局域网（LAN）和广域网（WAN）描述。

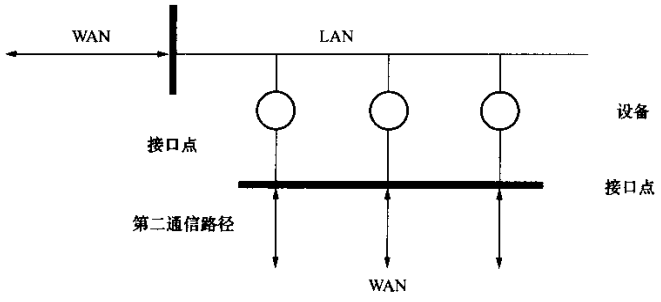

图 5　广域网和局域网拓扑

图中各接口点就是被攻击点。假设局域网处于物理安全的环境中。

该网络拓扑的典型示例为：

a）EMS/SCADA 的应用实例是操作员工作站（HMI）和数据库服务器（正常情况下两者均无第二广域网）以及与变电站广域网连接的前置处理机。

b）局域网，通常是以太网，有与宽带企业网或互联网的接口点，可以提供与其他应用的连接。

c）变电站设备的实例是各种变电站的智能电子设备（保护装置、抄表设备、当地 HMI 等），它们可能通过以太局域网、现场总线局域网、串行局域网或类似的网络连接。

d）有些智能电子设备可能配有到本地或远方设备的第二链路（广域网链路），该链路具有信息接口、配置接口以及传送批量数据的能力。

e）进入变电站的主接口点，即从广域网（WAN）到局域网（LAN）的接口，通常由 RTU、PLC 或网关/路由器实现。

对局域网的威胁不同于对广域网的威胁。从原理上说，如没有连接广域网，企图入侵者渗透进它的前提是能物理地访问客户。因而局域网的威胁来自心存不满的员工或未经授权的员工，而非第三方入侵者。

接口点代表了客户局域网和外部通信基础设施之间连接的关键点，这些接口点和位于这些接口点的关联通信介质是监测威胁的主要重点。用于广域网的各种技术都有其不同的安全问题。现在用的广域网典型技术是：

a）无线（须或无须申请批准）；

b）配电线载波（DLC），电力线载波；

c）专用线、专用光缆；

d）租用线路；

e）独立网络供应商（普通老式电话，移动电话系统，无线分组，X.25 等）。

表 4 给出了基于以上提及的存在协议威胁的广域网技术拓扑结构的安全隐患，不管它只是一个广域网/局域网（WAN/LAN）接口点的配置还是有第二个或冗余广域网/局域网（WAN/LAN）接口点的配置。下面的风险评估表示按获得资源和实施攻击所需知识的难易程度尝试攻击的几率。风险等级不考虑攻击的动机，也不考虑物理损坏的或然性（偶然的或恶意的）。

表 4　安全隐患等级

		无线	电力线载波	专用线或光缆	租用线	普通老式电话等	冗余广域网
保密性	T.NOAUTH-VIEW	H	H	L	M	M	—
	T.TRAFFIC-ANALYSIS	H	H	L	L	M	—

表 4（续）

		无线	电力线载波	专用线或光缆	租用线	普通老式电话等	冗余广域网
完整性	T.INTEG2, T.CHANGE, T.REPLAY	H	H	L	L	H	—
	T.IMPERSONATE	H	H	M	M	H	—
	T.HIJACK	H	H	L	M	L	—
拒绝服务	T.DENIAL-OF-SERVICE	H	H	H	H	H	M
管理	T.ADMIN3, T.ADMIN7, T.ADMIN9	H	H	M	M	H	—
H=高风险，M=中等风险，L=低风险							

表 4 的目的在于突出最易受攻击的地方，从而能确定需要在哪里进行进一步的安全分析，定义应对措施。因而，在这些最易受攻击点，需要对使用中的 IEC TC 57 通信协议加以分析，以确定是否以及如何提供有关的应对措施。

注：表 4 用以说明已确定的介质和威胁的安全隐患，而不是所有介质及威胁的详尽清单。

关于威胁，表 4 突出了以下方面：

a）保密性、完整性及管理

普通老式电话及第三方网络，无线方案及电力线载波方案属入侵者攻击的中到高风险程度。有关网络、协议等的信息可以从一些公开资料中得到。所以，对入侵者说来，窃听进而获得保密信息，更改信息，重放及交换信息，欺骗或伪装都不很困难。

使用专线或租用线属入侵者攻击的较低风险程度，因为入侵者对介质进行物理访问的难度不断增加。

b）拒绝服务

普通老式电话及第三方网络特别易受这种攻击。入侵者常能非常容易地从公共信息中确定网络地址或网络号，建立到接口点的链路，一旦链路建立，合法用户就无法使用该链路，除非另有可用的第二链路。

无线网络同样特别易受这种攻击，易受到频率干扰。入侵者常可容易地从公共资源中获得使用频率等信息。

其他介质也容易受到拒绝服务攻击，但更多的是系统资源耗尽形式的拒绝服务攻击。入侵者通过产生大量通信内容到接口点，增加响应时间，甚至使该装置处于饱和状态乃至无法工作，阻碍合法使用该介质。

以上分析表明，在广域网接口点的通信安全方面存在需要解决的实质性问题。许多问题以及安全威胁的危险程度，随通信体系结构及介质变化。但还是可以得出以下结论：

a）通信安全防护开始于通信信道的受限的/安全的访问；

b）如设备只有一个信道，拒绝服务攻击可能有高度风险，必须采取应对措施或提供多个通信路径，将整体拒绝服务风险降到最低；

c）设备需要具有强大的审计能力和防伪能力，改善通信安全；

d）如多种应用（例如 SCADA 和其他各种企业应用）采用同一拓扑，风险要比上述更高——对于一种应用的威胁会影响到其他应用。

8.2 IEC TC 57 的现有协议

在 IEC TC 57 范围内下列协议已经标准化或已作了规定。

8.2.1 TASE.1

IEC TC 57 第 07 工作组活动之一是制定 IEC 60870—6 系列标准（与 ISO 标准和 ITU-T 建议兼容的远动协议）。该系列的各部分涉及“远动应用服务元素 1（TASE.1）”：

a）IEC 60870—6—502：TASE.1 协议定义；

b）IEC 60870—6—504：TASE.1 用户约定；

c）IEC 60870—6—701：提供端系统的 TASE.1 应用服务的功能协议集。

该系列由欧洲执行包含在 ELCOM 协议中的工作发展而来的（ELCOM 协议最初为 ELCOM—83，后来更新为 ELCOM—90）。TASE.1 和 ELCOM—90 不完全相同，尽管有大量的 ELCOM—90 在实际应用，但是至今没有供应商在其产品中提供 TASE.1。对 TASE.1 的缺少支持使我们得出这样的结论：不应花费精力进行 TASE.1 的安全评估。

8.2.2 TASE.2

IEC TC 57 第 07 工作组的另一项活动就是制定“远动应用服务元素 2（TASE.2）”系列标准，它以美国“公用事业通信体系结构（UCA）”的工作为基础，UCA 提交的产品之一是从一个控制中心向另一个控制中心传送信息的协议——控制中心间通信协议（ICCP）。07 工作组对 ICCP 进行了标准化：

a）IEC 60870—6—503：TASE.2 服务和协议；

b）IEC 60870—6—702：在端系统中提供 TASE.2 应用服务的功能协议子集；

c）IEC 60870—6—802：TASE.2 对象模型。

本特别工作组已经开始对 TASE.2 进行安全分析，分析结果见附录 B。工作组认为完成 TASE.2 的安全分析是将来工作的重中之重。这结论来自 TASE.2 使用广泛，控制方面的因素以及对 TASE.2 系统的攻击得逞带来的经济损失。

IEC 61334 和 IEC 61850 的体系结构和技术相似，工作项目建议应将类似的工作项目结合起来进行。特别工作组希望能为这三个协议开发出一致的安全防护方法。

8.2.3 IEC 60870—5

IEC TC 57 第 03 工作组已经制定了 IEC 60870—5 系列标准，提出了建立适用于特定应用的协议（或协议子集）的建议。IEC TC 57 第 03 工作组已经按这些建议制定了以下协议子集：

a）IEC 60870—5—101：基本远动任务的配套标准；

b）IEC 60870—5—102：在电力系统中传输累加总量的配套标准；

c）IEC 60870—5—103：保护设备非格式化信息接口的配套标准；

d）IEC 60870—5—104：采用标准传输协议集的 IEC 60870—5—101 的网络访问。

IEC 60870—5 系列的基本建议没有涉及有关访问控制、加密或认证方法的机制问题。因此 IEC 60870—5—101，IEC 60870—5—102 和 IEC 60870—5—103 这些配套标准目前不具备实现附加安全措施的条件。IEC TC 57 第 03 工作组应对这些配套标准的安全需求进行分析，制定防护方案，并用分析结果提出加强这些标准的必要建议。必须认识到为这些协议增加安全强度会是困难的，并几乎可以肯定这些协议不会向后兼容已有的实现。

8.2.4 IEC 61334

IEC TC 57 第 09 工作组的主题是“采用配电线载波的配电自动化”，并已制定了 IEC 61334 系列标准。它的范围包括用于低压和中压电网的配电自动化和客户自动化的通信协议。主要文件是：

a）IEC 61334—4—41；

b）IEC 61334—4—42。

这些标准涉及的大多是远方抄表而非配电自动化，而抄表通信也在 IEC TC 13 的 14 工作组工作范围内。因此 IEC 划分了范围：协议和配电线载波介质由 IEC TC 57 第 09 工作组负责，抄表应用（以及抄表对象）和其他介质由 IEC TC 13 14 工作组负责。虽然 IEC 标准把 DLMS 称为“配电线报文规范”，但是 DLMS 在商业推广时被称为“装置语言报文规范”，目的是明确它适用于其他通信介质。

DLMS 原是 MMS（ISO/IEC 9506）的子集，但发现它对低成本装置和有限传输能力的信道（如配电线载波）的支持不足。特别是发现必须引入扩展“无确认广播”以实现如时钟同步等的操作。后来又作了一些其他改变，以至现在的 MMS 和 DLMS 两者不能互操作。最近 IEC TC 57 第 09 工作组已着手解决这些不能兼容的问题，但迄今为止还没有解决方案。

DLMS（IEC 61334—4—41）以及 IEC 61334—4—42 中描述的应用层有访问控制机制和一些允许加密的“钩子”（hooks）函数，但没有明确认证方法。

DLMS 定义了虚拟配电设备（VDE）对象。例如，具有 VDE 特定访问范围的有名变量是能随意访问的。它还为访问控制定义了虚拟应用关联（VAA）。VAA 特定的访问范围限制了对某些有名变量的访问，而这些变量只对以前创建了 VAA 对象的 DLMS 用户开放。

提供应用的加密/解密功能是为了确保传输数据的安全性和保密性。据说算法与应用有关，所以算法的定义工作被推迟到一个配套标准中。定义了两种密钥：全局加密密钥和专用加密密钥。全局加密密钥的目的是允许加密广播。专用加密密钥包含在 DLMS 上下文中，而且特定于应用关联的实例。

为了避免已发送的报文未经授权而重放，可以预见会将一次性复制检查域作为加密算法的一部分。

本文件不涉及密钥管理。

IEC TC 57 第 09 工作组已试着开始进行进一步的安全工作，但由于缺少资源，尚未获得进展。

特别工作组希望能为 IEC 61334 系列、IEC 61850 系列和 TASE.2 制定一致的安全防护方法。

8.2.5 IEC 61850

IEC TC 57 第 10、11 和 12 工作组的活动都涉及 IEC 61850 系列标准（变电站通信网络和系统）。该系列标准定义了下列模型：

a）信息元素的基本结构；

b）变电站设备和馈线设备；

c）服务模型，如“时间”、“报告”、“控制”、“关联”等。

并给出这些模型映射到一个标准协议栈的方法，如基于 TCP/IP 的 MMS、IEC 60870—5 系列、Profibus 等。

IEC 61850（及其对 MMS 的映射）中定义的关联模型的设计，使它能满足讨论中的通信系统的安全需求，即关于认证、加密和数据访问控制（安全防护角度）的建模能力。IEC TC 57 第 10、11 和 12 工作组应通过安全分析，即制定 IEC 61850 系列的防护方案，证明 IEC 61850 系列的关联模型的适用性。

特别工作组希望能为 IEC 61334 系列、IEC 61850 系列和 TASE.2 制定一致的安全防护方法。

9 IEC TC 57 对未来安全防护工作的建议

a）建议 IEC TC 57 第 06 特别工作组转为一个工作组，从而：

1）使本文件的意见得到解决；

2）工作组能继续完成特别工作组原承担的工作：协调 IEC TC 57 内部的安全防护工作和解决方案；

3）工作组能帮助执行 IEC TC 57 范围内对其他标准建议的工作项目；

4）建议工作组负责为个别工作组中尚未获得支持的安全防护工作项目（标准或技术文件）（例如该工作项目在投票表决中失败）建立与特定协议安全有关的工作项目。

b）建议用基于后果的安全分析技术进行 IEC TC 57 的有关安全的活动。

1）改进业务过程的集合，应考虑业务过程的后果。

建议目前考虑的业务过程为：

——发电；

——输电；

——配电；

——交易计量；
——资产管理；
——节能。

2）改进和进一步定义应作为基于后果的安全分析一部分的后果类别的集合。
目前建议考虑的后果有：
——财务；
——资产破坏或降级；
——无法恢复服务。

c）对于将来基于单个协议或标准的工作项目，建议除考虑应用层外还应考虑其他 OSI 通信层的安全应对措施。

d）建议与过渡性的 IEC TC 57 第 06 特别工作组联系，在安全方面考虑以下标准的工作项目：

1）建议负责以下标准的各工作组建立联合工作项目，以便能将一致的安全机制用于这些标准：
——IEC 60870—6 TASE.2，建议最优先地解决 TASE.2 问题；
——IEC 61850 系列；
——IEC 61334—4—41（DLMS）；
——IEC 61334—4—42（应用层）；
——也建议联合任务组与 IEC TC 13 第 14 工作组和 IEC TC 95 建立联系。

注：该建议主要基于这些标准采用的底层协议的共同性。

2）建议 IEC TC 57 第 03 工作组为 IEC 60870—5 系列建立工作项目。

3）建议过渡性的 IEC TC 57 第 06 特别工作组（例如作为一个工作组）负责为个别工作组尚未获得支持的安全防护工作项目（例如该项目在投票表决中失败）建立与特定协议安全防护有关的工作项目。

e）不建议将以下标准作为加强安全或工作项目。
IEC 60870—6 TASE.1。

注：该建议主要基于该标准的使用情况。

f）建议将承担的工作项目作为应用层和表示层功能的一部分集中在 A-Profile 的安全上。

1）建议将加密作为表示层的功能，与 ISO 定义一致（通用上层安全——GULS）。

2）建议将应用层认证机制作为工作项目的一部分。

3）建议至少提供三个级别的认证机制：
——无认证；
——口令认证；
——强认证。

4）建议工作项目着手解决最低级别的安全问题（例如不提供安全认证的实例的缺省值）。

g）建议将制定防护方案作为工作项目的一部分。

h）建议将与通信协议特定使用有关的后果图的开发包含在工作项目中。

i）建议过渡性的 IEC TC 57 第 06 特别工作组承担未来有关加密密钥管理的工作项目。

j）用现代密码学对协议运行的信道进行防护等同于通过使用加密和其相关的密钥，进行从应用协议数据单元到传输句法的表示转换。表示转换所使用的密钥在 IEC TC 57 工作范围以外的系统上维护。IEC TC 57 协议的安全性只能与维护密钥的系统的安全性相等。启动并管理信道的系统需要防护，该任务应成为 IEC TC 57 的工作项目。该安全体系应采用公共准则的防护方案。

k）建议过渡性 06 特别工作组承担拟订系统级 TOE 的未来工作项目。

l）一个重要的观点是：制定防护方案不仅为了协议本身，而且也为了支持这些协议的系统。这些防护方案可能用作制定组件级安全、子系统级安全及系统级安全的度量标准的基础。

m）该工作项目需要对由其他工作项目开发的 TOE 的接口边界进行分析。

n）建议过渡性的 IEC TC 57 第 06 特别工作组将来承担一个工作项目，确定 IEC TC 57 内各系统采用的体系结构模式（例如变电站的 LAN 的模式），并完成这些模式的后果分析。

o）该结果将是在系统体系结构以及在这些体系结构上运行的协议的基础。这些模式可以用作开展特定系统的体系结构后果分析的模板，这能用于推断对该特定系统的威胁。开展这样的后果分析是向确定和减轻 IEC TC 57 用的体系结构存在的系统威胁迈出的重要一步。

p）建议过渡性的 IEC TC 57 第 06 特别工作组将来承担一个工作项目，负责定义物理安全和信息安全之间的边界。

q）一旦制定了具有一定保障级别的信息安全措施，就需要保证制定相应的物理安全保障级别。重要的是如何准确地定义信息安全和物理安全问题（TOE）之间的边界。

r）建议 IEC TC 57 考虑建立一个能解决内线威胁问题的过程。

s）应特别注意“内线”威胁（B.4），这最难防范，而且有以最少资源给予最大损害的可能。

附 录 A
（资料性附录）
防护方案是什么

为使《信息技术公共准则》与国际标准 ISO/IEC 15408（所有部分）符合，已将它修订为 2.1 版即 CCIMB—99—031（1999 年 8 月）。防护方案（PP）由修订后的《信息技术公共准则》导出，包含以下内容：

部　分	内　容
1	PP 介绍 ——PP 标识 ——PP 概述
2	评估目标（TOE）说明
3	TOE 安全防护环境 ——假设 ——威胁 ——组织的安全对策
4	安全防护目标 ——TOE 的安全防护目标 ——环境的安全防护目标
5	信息技术（IT）的防护需求 ——TOE 的安全功能需求 ——TOE 安全保障需求 ——IT 环境的安全防护需求
6	PP 应用注意事项
7	防护原理阐述 ——安全防护目标原理阐述 ——安全防护需求原理阐述

PP 介绍——标识 PP，以叙述方式提供适于列入 PP 目录和注册的 PP 概要。

评估目标（TOE）说明——提供 TOE（或 TOE 类型）的背景信息，以帮助理解其安全需求和准备使用的方法。

TOE 安全防护环境——提供 TOE 要说明的“安全需要”的定义，包括要求防护的资产、已确定的对这些资产的威胁、TOE 必须遵循的组织的安全防护策略以及其他定义安全需要范围的假设。

安全防护目标——根据由 TOE 保证的防护目标及由 TOE 环境内非技术措施保证的防护目标，准确地描述对安全需要的预期响应。

IT 的防护需求——定义 TOE 的安全功能需求［如可以，采用公共准则第 2 部分（CC2）的功能部分—引自 ISO/IEC 15408－2］、TOE 的安全保障需求［如可以，采用公共准则第 3 部分（CC3）的保障部分—引自 ISO/IEC 15408－3］以及 TOE 的 IT 环境中的软件、固件、硬件的需求。

PP 应用注意事项——可选部分，提供 PP 作者认为有用的额外支持信息。

防护原理阐述——提供具体说明一个完整的、综合的、内在一致的防护目标与 IT 防护需求的集合的示例，适于说明已确定的安全需要。

在 TOE 安全防护环境、防护目标、IT 防护需求部分的段落中，以及在说明它们的防护原理的段落

中，防护方案（PP）和安全目标（ST）都有高度的共同性。确实，如仅需求一个 ST 与一个没有其他功能需求或保障需求的 PP 保持一致，则该 ST 的这些段落会与 PP 中相应段落完全相同。ST 中的以下段落提供了 PP 中没有涉及的详细情况：

a）TOE 规范概要，包括信息技术安全功能、安全防护机制或安全防护技术及保障措施；

b）PP 声明（ST 中防护原理阐述的一部分），声明与各参照的 PP 一致；

c）ST 中防护原理阐述部分，说明 IT 安全功能和保障措施可以满足 IT 防护需求。

附 录 B
（资料性附录）
TASE.2的防护方案

B.1 背景

防护方案（PP）给出了关于TOE（评估目标）的假设，确定了基于这些假设的TOE面临的威胁，提出了应对这些威胁的防护目标，并确定了安全防护功能以实现这些防护目标。防护原理阐述说明了不同决策的原因。最后一部分将本PP推广到任何应用层协议。

我们期望会有第三方将TOE作为COTS（现货供应的商业软件）解决方案来开发。客户不可能控制开发环境。任何客户所进行的测试很可能要在开发商提交TOE后进行。定性地说，这类环境下能提供的防护水平处于评估安全保障等级（EAL）2。

EAL2的防护目标（防护目标引自ISO/IEC 15408－3）：

a）EAL2需要开发商就提交设计信息和测试结果进行合作，但不应要求开发商比优良的商业实践付出更多努力。因此，EAL2不应要求实质性地增加成本或时间的投入。

b）因此，EAL2可以在这样的环境中应用：在没有立即可用的完整的开发记录情况下，开发商或用户需要中级或低级的独立保障安全级别。这种情形可能发生在传统的防护系统或对开发商的访问受到限制时。

c）对于EAL2，防护方案不决定于实施。对于一个具体的实例，要写出比PP更具体的安全目标。PP是一组通用的指南。

B.2 防护方案（PP）介绍

PP标识

a）标题：电力部门环境中的远动应用服务元素（TASE.2）安全防护方案。

b）保障级别：<2>。

c）注册：<待定>。

d）关键词：远动、电力、网络安全、信息协议、MMS。

PP概要

本TASE.2PP的目的在于为电力部门采用TASE.2协议进行信息交换定义基本的安全防护需求。

B.3 评估目标（TOE）说明

TASE.2的目的是用客户机/服务器模型提供电力部门之间的实时数据交换。作为客户机的电力部门或作为服务器的电力部门均可将连接启动。客户机和服务器之间的互动可以包括请求信息及发控制指令。在这个意义上，TASE.2是监视和控制从本地环境（或SCADA内部环境）到SCADA之间的环境的延伸。参见图B.1。

控制中心1所在域的现场装置可以包含在控制中心2所在域中。这就建立了一个域间控制区。

B.4 TOE安全防护环境

适应PP的TOE用于电力部门环境中。在该环境里可以处理业务敏感信息但不处理分类后的信息[1)]。这样，信息因被业务专用而有了价值。所以，可以假设最可能的对手是竞争者或具有竞争利益的实体（包

1) 如支持的EAL高于2级，需对PP加以增扩。

括专业人士及懂行的业余人士)。目标在于败坏公司信誉的实体也包括在“具有竞争利益的实体”之列。专业人士和业余人士之间的明显区别在于他们可以使用的资源水平以及攻击的系统性不同。由于业务和一些政府部门之间有内在关系，竞争者名单上很可能出现拥有大量资源的政府所属机构。这样的威胁所需要的安全防护水平比本防护方案提出的更高。现在假设威胁来自仅拥有中等资源的对手。下面将“内线”定义为经过认证的用户。这些内线在得到认证后才通过 TOE 以外的某机制与 TOE 互动。其他非内线的竞争者则定义为“外线”。

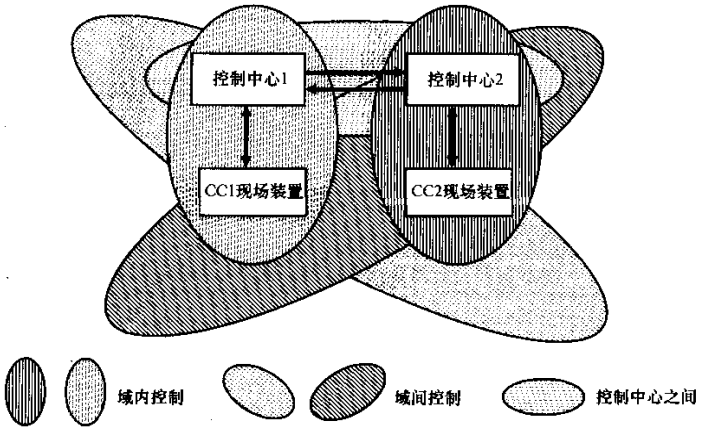

图 B.1　需说明的 TASE.2通信域

表 B.1　假　　设

假设名	说　　明
A. ADMIN	TOE 的安全特性得到不断、充分及适当的管理；但管理员也可能出错
A. ADVERSARY	假设对手为有竞争利益、资源有限及仅拥有关于 TOE 的公共信息的外线
A. ADVERSARY-IMPERSONATE	对手未伪装成授权用户[a]
A. BILAT	服务器对客户机数据对象的访问权受双边表中的规范控制
A. BILAT-ACCESS	授权管理者维护并提供对双边表的访问
A. CIIENT	请求信息的实体被视为客户
A. COTS	TOE 是通过商用现货供应（COTS）信息技术而建立的
A. INFO-FLOW	如信息从客户机传递到服务器，它要经过 TOE
A. INFO-VALUE	假设 TOE 携带的信息是业务专用的
A. KEYS	所有加密密钥均安全地生成、分发，并在期满后销毁
A. KEY-TRUST	通过 TOE 无条件信任的第三方（即 CA/RA）建立密钥的信任
A. NO-DENIAL	不期望 TOE 阻碍拒绝服务攻击
A. NO-INSIDER	不期望 TOE 减轻内线的攻击
A. PHYSEC	TOE 在物理上是安全的
A. REMOTE-ACCESS	授权管理者可能远程访问 TOE
A. SERVER	提供信息的实体为服务器
A. TIME-SERVER	TOE 已访问可信的时间服务器
A. TRANSACTION	定义为两实体间的数据交换的事务
A. TRANSACTION-ENTITY	就事务而言，实体可以是客户机也可以是服务器
A. USER	所有 TOE 的操作人员均假定是已通过在本 TOE 范围外的某用户接口得到识别的授权用户
A. USER-TRUST	经认证的用户通常被信任会按照安全防护对策进行任意动作
a 数字签名可以减少伪装问题，除非对手获得了授权用户的密钥	

表 B.2 安全防护策略相关事项

策略名	说　明
P. ACCESS	对特定数据对象的访问权取决于赋予该对象的对象属性、用户身份、用户属性以及安全防护策略定义的环境条件
P. COMPLY	组织的信息技术系统的实施和使用应遵循所有现行法律、规章以及施加于该组织的合同协议
P. TOE-HOST	为 TOE 所在的系统制定安全防护策略的系统管理者对用户进行认证

表 B.3 威　胁

威胁名	说　明
T. CHANGE	对手可以修改或破坏 TOE 数据
T. IMPERMISSIBLE	用户可能通过 TOE 发送未经允许的信息
T. NOAUTH-VIEW	对手可能查看 TOE 数据
T. REPLAY	对手在截获有效数据后可能试图重新传输该数据

表 B.4 防护目标

防护目标名	说　明	注　释
O. CONFIDENTIALITY	TOE 提供便于防范对手的促进数据保密的服务	
O.DATA-AUTHENTICATION	TOE 提供保证和原始数据相同的数据认证服务。注意：数据认证可提供数据的完整性	例如散列函数
O. DATA-INTEGRITY	TOE 提供保证数据完整性服务	例如：数据是否可接受，是否具有正确格式（例如海明码、校验和等）。（不必是“是否是原始数据”，而可以是“是否是有效数据”）
O. SECURITY-LEVEL	为达到这些防护目标选择的安全防护算法必须达到一定水平，使对手不能用计算方法获得算法隐藏的秘密	
O. SOURCE-AUTHENTICATION	TOE 提供有验证数据源能力的服务。注意：源完整性隐含提供了数据认证，因为如数据改变，该源也会改变	例如，签名
O. TRANS-INTEGRITY	TOE 提供保障数据的唯一性和及时性的服务	

B.5 信息技术（IT）防护需求

表 B.5 TOE 安全功能需求 [1)]

功能需求名	说　明
FCO_NRO.1.3	假设发起方使用可信的密钥和适当的认证算法，TSF（TOE 安全功能）应向经认证的用户提供校核信息源的证据的能力
FCS_COP.1.1	TSF 应按规定的加密算法（DSA，RSA，3DES，AES），用符合 FIPS 186（DSA），FIPS 81（DES），FIPS 48-3（3DES）要求的加密密钥，长度为 1024 位 DSA，1024 位 RSA，64 位双密钥 3DES，128 位 AES，进行数字签名和加密
FDP_DAU.1.1	TSE 应能生成用作（数据）有效性保证的证据

1) 有这样的担心：控制中心定义的安全功能不能完全满足防护目标的要求。防护目标包括数据完整性、事务完整性、数据认证以及源认证。源认证不能严格地映射到源的不抵赖（FCO_NRO），但是不抵赖并不是人们希望进行源认证的唯一理由。因此，应将这两者加以区别。有些防护目标应既适用于静态数据又适用于传输中的数据，即使 FDP_DAU 仅指静态数据。

表 B.5（续）

功能需求名	说　明
FPT_RPL.1.1	TSF 应检测下列实体（未经认证的用户）进行的重放
FPT_STM.1.1	TSF 应能提供 TSF 自用的可靠时间戳
注：这里采用 ISO/IEC 15408（所有部分）的符号表示及术语。	

B.6 防护原理阐述

表 B.6 假设的原理阐述

假设名	说　明
A. ADMIN	除非对系统进行不断、充分及适当的管理，否则系统是不安全的。所以该假设是必需的也是合理的
A. COTS	该假设表示在 CS2 开发中采用的主要设计限制
A. NO-INSIDER	不期望 TOE 能充分降低由于恶意滥用授予的特权所导致的风险。期望 COTS 的近期产品对授权个体的恶意动作提供充分的防护也是不现实的
A. USER-TRUST	组织大多以这种方式信任经认证的用户。用户具有较高的判定力，而且应相信他们会恰当地运用这种判定力。因此该假设是必需的也是合理的
A. REMOTE-ACCESS	允许管理者远程访问系统，使它具备应急响应能力

安全防护目标的原理阐述：

a）以 O. CONFIDENTIALITY 应对 T. NOAUTH-VIEW 威胁；

b）以 O. DATA-INTEGRITY 应对 T. IMPERMISSIBLE 威胁；

c）以 O. TRANS-INTEGRITY 应对 T. REPLAY 威胁；

d）以 O. DATA-AUTHENTICATION 应对 T. CHANGE 和 T. IMPERMISSIBLE 威胁；

e）以 O. SOURCE-AUTHENTICATION 应对 T. CHANGE 和 T. IMPERMISSIBLE 威胁。

功能性安全防护需求的原理阐述：

a）FCS_COP. 1.1 有助于满足安全防护目标 O. CONFIDENTIALITY, O. DATA-AUTHENTICATION, O. SOURCE-AUTHENTICATION, O. TRANS-INTEGRITY 和 O. SECURITY-LEVEL 的要求；

b）FCO_NRO. 1.3 有助于满足安全防护目标 O. SOURCE-AUTHENTICATION 的要求；

c）FDP_DAU. 1.1 有助于满足安全防护目标 O. DATA-INTEGRITY 和 O. DATA-AUTHENTICATION 的要求；

d）FPT_RPL. 1.1 和 FPT_STM. 1.1 有助于满足安全防护目标 O. TRANS-INTEGRITY 的要求。

将 TASE. 2 防护方案推广于任何应用层协议：

为使本防护方案通用化，可取消 TASE. 2 的特定假设 A. BILAT 和 A. BILAT-ACCESS。以本通用防护方案为基础，对其他通信协议可以增加假设和威胁。

附 录 C
（资料性附录）
后 果 图 示 例

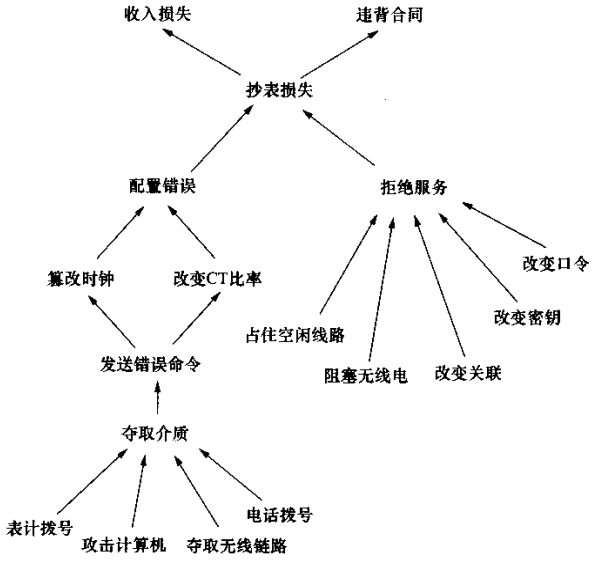

图 C.1 DLMS 后果图