ICS 29.240.30
F 21

中华人民共和国国家标准化指导性技术文件

GB/Z 25320.1—2010/IEC TS 62351-1:2007

电力系统管理及其信息交换 数据和通信安全 第1部分:通信网络和系统安全 安全问题介绍

**Power systems management and associated information exchange—
Data and communications security—
Part 1: Communication network and system security—
Introduction to security issues**

(IEC TS 62351-1:2007, IDT)

2010-11-10 发布　　2011-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

国际电工委员会57技术委员会（IEC TC 57）对电力系统管理及其信息交换制定了IEC 62351《电力系统管理及其信息交换　数据和通信安全》标准。我们采用IEC 62351，编制了GB/Z 25320指导性技术文件，主要包括以下部分：

——第1部分：通信网络和系统安全　安全问题介绍；

——第2部分：术语；

——第3部分：通信网络和系统安全　包含TCP/IP的协议集；

——第4部分：包含MMS的协议集；

——第5部分：IEC 60870-5及其衍生标准的安全；

——第6部分：DL/T 860的安全；

——第7部分：网络和系统管理的数据对象模型；

——第8部分：电力系统管理的基于角色访问控制。

本部分等同采用IEC TS 62351-1：2007《电力系统管理及其信息交换　数据和通信安全　第1部分：通信网络和系统安全　安全问题介绍》（英文版）。

本部分增加了资料性附录NA，以反映规范性引用文件IEC 60870-5（所有部分）中的各部分与对应的我国标准以及一致性程度。

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管理及其信息交换标准化技术委员会（SAC/TC 82）归口。

本部分起草单位：国网电力科学研究院、国家电力调度通信中心、中国电力科学研究院、福建省电力有限公司、华中电网有限公司、华东电网有限公司、辽宁省电力有限公司。

本部分主要起草人：许慕樑、南贵林、邓兆云、杨秋恒、韩水保、李根蔚、曹连军、袁和林、林为民。

本指导性技术文件仅供参考。有关对本指导性技术文件的建议或意见，向国务院标准化行政主管部门反映。

引　言

计算机、通信和网络技术当前已在电力系统中广泛使用。通信和计算机网络中存在着各种对信息安全可能的攻击，对电力系统的数据及通信安全也构成了威胁。这些潜在的可能的攻击针对着电力系统使用的各层通信协议中的安全漏洞及电力系统信息基础设施的安全管理的不完善处。

为此，我们采用国际标准制定了GB/Z 25320《电力系统管理及其信息交换　数据和通信安全》，通过在相关的通信协议及在信息基础设管理中增加特定的安全措施，提高和增强电力系统的数据及通信的安全。

电力系统管理及其信息交换 数据和通信安全 第1部分:通信网络和系统安全 安全问题介绍

1 范围和目的

1.1 范围

GB/Z 25320的本部分范围是电力系统控制运行的信息安全。本部分的主要目的是"为IEC TC 57制定的通信协议的安全,特别是IEC 60870-5、IEC 60870-6、IEC 61850、IEC 61970和IEC 61968的安全,承担标准的制定;承担有关端对端安全的标准和技术报告的制定"。

1.2 目的

具体目的包括:

- GB/Z 25320.1介绍了GB/Z 25320的其他部分,主要向读者介绍应用于电力系统运行的信息安全的各方面知识;
- GB/Z 25320.3～GB/Z 25320.6规定了IEC TC 57通信协议的安全标准。可以用这些标准提供各种层次的协议安全,这取决于为一个特定实现所选定的协议和参数。同样它们已被设计为具有向后兼容能力并能分阶段实现;
- GB/Z 25320.7涉及端对端信息安全的许多可能领域中的一个领域,即加强对支持电力系统运行的通信网络进行全面管理;
- GB/Z 25320后续的其他部分涉及更多的信息安全领域。

电力行业中安全性、安全防护和可靠性始终是系统设计和运行的重要问题,随着该行业越来越多依赖于信息基础设施,其信息安全正变得日益重要,这就是制定信息安全标准的理由。一些新威胁已经影响到解除管制的电力市场,因为对竞争对手的资产和其系统运作的了解可能是会从中得益的,于是截获此类信息是十分可能发生的。此外,无意的行为(如不小心和自然灾祸)能够像蓄意行为一样对信息造成危险。当前恐怖主义的外加威胁已经变得非常明显。

虽然存在"端对端"安全的许多定义,一个标准定义(多种陈述)是:"1. 对采用密码技术的安全通信系统或被保护的分布系统中的信息进行安全防护意味着从起始点到目的点的防护。2. 对信息系统中的信息,从起始点到目的点进行安全防护"[1)]。以这个定义为基础开始的四个标准是针对IEC TC 57通信协议集的安全增强,因为这些通信协议集被认为是对电力系统控制操作进行安全防护明显的第一步。然而这些安全增强仅能解决两个系统之间的安全需求,并不解决包含内部安全需求的真正"端对端"安全,包括安全对策、安全防护执行、入侵检测、内部系统和应用的健壮以及更广泛的安全需求。

因此,本章的本结束语是非常重要的:认识到增设防火墙或仅简单使用协议的加密,例如增加链路端加密盒(bump-in-the-wire)或甚至虚拟专网(VPN)技术,在许多情况下似乎并不是足够的。安全是真正的"端对端"的要求,以确保对敏感的电力系统设备的认证访问、对敏感的市场数据的授权访问、可靠且及时的设备功能执行和设备故障信息、关键系统的备份以及容许检测和再现决定性事件的审计

1) ATIS(Alliance for Telecommunications Industry Solutions)[美国为通信和相关信息技术快速制定和促进技术和运行标准的组织。ATIS得到了美国国家标准学会(ANSI)的认可。]:FS-1037C的扩充,US联邦政府电信项目的标准术语。

能力。

2 规范性引用文件

下列文件中的条款通过 GB/Z 25320 的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/T 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(IEC 60870-6[2)]，IDT)

DL/T 860(所有部分) 变电站通信网络和系统 (IEC 61850[3)]，IDT)

IEC 60870-5 (所有部分) 远动设备和系统 第5部分 传输规约(Telecontrol equipment and systems—Part 5: Transmission protocols)

IEC TS 62351-2 电力系统管理及其信息交换 数据和通信安全 第2部分：术语(Power systems management and associated information exchange—Data and communications security—Part 2: Glossary of terms)

3 术语、定义和缩略语

IEC 62351-2 中给出的术语和定义及缩略语适用于 GB/Z 25320 的本部分。

4 信息安全标准的背景

4.1 电力系统运行的信息安全所涉及的论据

通信协议是电力系统运行的最关键部分之一，它负责从现场设备取回信息和发送控制命令至现场设备。虽然通信协议具有关键作用，但迄今这些通信协议还很少加入任何安全措施，这些安全措施包括对无意错误，电力系统设备功能丧失，通信设备故障或蓄意破坏进行的防护。由于这些协议是非常专业化的，“依靠难以理解获得安全”一直是主要手段。毕竟，只有操作员才被允许从高度防护的控制中心去控制断路器。谁会去关心线路上的电功率，或者说对近百种通信协议中某个适用协议，谁可能具有如何读取其特殊比特和字节的知识，并且为什么有人会想破坏电力系统呢？

然而，依靠难以理解获得安全不再是有效的观念。特别是电力市场正迫使市场参与者去获取他们所能获得的任何优势。即使一点信息就有可能使失败的投标转变为成功的投标，或者说持有你竞争对手的信息就能使他们成功的投标变为失败的投标。因而破坏电力系统运行的欲望可能出自单纯的十来岁青少年对电力市场的竞争搏弈游戏吹牛式的恐吓行为，直到实际恐怖行动。

的确，不仅市场力使安全成为至关重要。运行电力系统的绝对复杂性在这些年一直在增加，这使设备故障和操作错误更有可能发生，并且影响的范围和代价更大。此外，较旧的，“难以理解”的通信协议正被标准化的、良好文本的协议代替，对骇客和工业间谍而言这样的协议更易攻击。

随着电力行业日益依赖信息来运行电力系统，现在必须管理两种基础设施：不仅应管理电力系统基础设施(Power System Infrastructure)，还应管理信息基础设施(Information Infrastructure)。因为自

2) 也称为控制中心间通信协议(Inter-control Centre Communications Protocol，ICCP)，使得能在电力部门控制中心与其他控制中心、其他公用事业部门、电力联营体、区域控制中心和非电力部门发电商之间经广域网(WAN)进行数据交换。

3) DL/T 860(IEC 61850，IDT)标准，用于继电保护、变电站自动化、配电自动化、电能质量、分布能源、变电站对控制中心和其他的电力行业运行功能。它包括为满足极其快速的继电保护响应时间和为被测值进行采样的协议集，以及专注于对变电站和现场设备进行监视和控制的协议集。

动化不断代替人工操作，市场要求更精确且更及时的信息以及电力系统设备变得陈旧，管理电力系统基础设施已经变得依靠于信息基础设施。因而信息基础设施可能遭受的任何问题都日益影响到电力系统的可靠性。

4.2 IEC TC 57 数据通信协议

国际电工委员会(IEC)的"电力系统管理及其信息交换"技术委员会(TC 57)负责制定电力系统数据通信协议的国际标准。它的范围是"为电力系统控制设备和系统，包括 EMS(能量管理系统)、SCADA (数据采集和监控)、配电自动化、远方保护，以及用于电力系统的规划、运行和维护的实时和非实时信息的相关信息交换制定国际标准。电力系统管理是由控制中心、变电站和个别一次设备内的控制组成，包括设备、系统和数据库的远动和接口，而这些接口可能是在 TC 57 所辖范围之外。在高压环境中的特殊工况必须要考虑。"

IEC TC 57 已经制定了三种广泛接受的协议标准并已是第四个协议的发起者。这三个协议是：

IEC 60870-5　在欧洲和其他非美国的国家广泛用于 SCADA 系统与 RTU 的数据通信。同时用于串行链路(IEC 60870-5-101，对应于我国的 DL/T 634.5101)和网络(IEC 60870-5-104，对应于 DL/T 634.5104)。DNP3 是为了在美国使用，从 IEC 60870-5 衍生出来而现在许多其他国家也广泛使用，主要用于 SCADA 系统与 RTU 的数据通信。

IEC 60870-6(对应于我国的 GB/T 18700)　也称为 TASE.2 或 ICCP，国际上用于控制中心之间通信，并经常用于控制中心内 SCADA 系统和其他工程系统之间通信。

IEC 61850(对应于我国的 DL/T 860)　用于继电保护、变电站自动化、配电自动化、电能质量、分布能源、变电站对控制中心和电力行业的其他运行功能。它包括为满足极其快速的继电保护响应时间和对被测值进行采样的协议集，以及专注于对变电站和现场设备进行监视和控制的协议集。

这些协议现在广泛地使用于电力行业中。然而，它们都是在信息安全成为该行业的主要问题之前制定的，所以原先标准中根本不包括任何安全措施。

4.3 制定这些安全标准的历史

直到 1997 年 IEC TC 57 才认识到对这些协议进行安全防护是必要的。因而，TC 57 首先成立研究安全防护问题的临时工作组。该组发布了关于安全需求的技术报告 IEC/TR 62210(对应于我国的 DL/Z 981)。该技术报告的一个建议是组成工作组，为 IEC TC 57 协议和它们的衍生协议制定安全标准。

最初国际标准化组织(ISO)的通用评估准则(Common Criteria)被选定为确定安全需求的方法。这种方法用评估对象(Target of Evaluation，TOE)的概念作安全分析的焦点。可是，在不同电力系统环境中多样性和多变的安全需求下，确定防护 TOE 的特征非常麻烦，因此最终这种方法没被采用。代之使用的是威胁减轻分析。该方法先确定最常见威胁，然后制定应对这些威胁的安全措施。

因此，IEC TC 57 WG15 在 1999 年成立并且已经承担了这项工作。WG15 的名称是"电力系统管理及其通信 数据和通信安全"，它的工作范围和目的是"为 IEC TC 57 制定的通信协议的安全，特别是 IEC 60870-5、IEC 60870-6、IEC 61850、IEC61970 和 IEC61968 的安全，承担标准的制定，承担有关端对端安全课题的标准和技术报告的制定。"

这样做的理由是：安全性、安全防护和可靠性始终是电力行业中系统设计和运行的重要问题，随着该行业越来越多依赖于信息基础设施，该行业中计算机安全正变得日益重要。解除管制的电力市场已带来了新威胁，因为对竞争对手资产以及他的系统运作的了解可能会从中得益，于是收集此类信息是现实可能的。当前恐怖主义的外加威胁也已经变得更明显。

在范围和目的陈述中的结束语是非常重要的：认识到仅增加数据的简单加密，例如增加链路端加密盒(bump-in-the-wire)或甚至 VPN 技术，对于许多情况似乎并不是足够的。安全是真正的"端对端"的要求，以确保对敏感的电力系统设备的认证访问、可靠而及时的关于设备的功能及故障的信息、关键系统的备份和容许再现关键事件的审计能力。

5 GB/Z 25320 涉及的安全问题

5.1 安全的一般信息

本章内容是资料性的，提供与安全问题有关的额外信息。这些信息虽然并不被这些规范性标准明确论及，但可能有助于理解这些规范性标准的上下文和范围。

5.2 安全威胁的类型

5.2.1 概述

安全威胁通常被看作对资产的攻击是潜在的。这些资产可能是物理设备、计算机硬件、楼房甚至人员。然而，在计算机世界中资产也包括信息、数据库和软件应用。所以对安全威胁的应对措施应该包括对物理攻击和计算机攻击的防护。

对资产的安全威胁不仅可能是蓄意攻击，而且可能由无意事件导致。事实上，经常更实际的危险可能是安全性突降、设备故障、疏忽大意和自然灾害所导致的而不是蓄意攻击所造成的。然而，对成功的蓄意攻击的反应可能具有巨大的法律、社会和经济的后果，这些会远超过物理危险。

电力部门习惯于担心设备故障及与安全性相关的疏忽大意，自然灾害也包含在考虑范围内，特别对那些经常受飓风、地震、龙卷风、冰雹等自然灾害影响的电力部门。即使这些自然灾害被看作并非电力部门所能控制的。正在起变化的是对信息进行保护的重要性，信息正日益成为安全、可靠和高效电力系统运行的重要方面。

在正确确定对什么攻击需要防护什么和需要防护到怎样的安全级别时，安全风险评估是至关重要的。关键是决定于成本效益：要“量体裁衣”[4)]（变电站），多层次安全防护比单一方案更好，而且任何时候对攻击的防护都不是完全绝对的。尽管如此，为提供现代电力部门运行所需的安全等级，从什么不做到一切都做这两个极端之间存在相当大的空间。

安全防护在其他方面也能带来益处，如果对可能的蓄意攻击实现了外加的安全防护，就能够使用这种监视去改善安全性，使疏忽概率减至最小，并提高了设备维护的效率。

以下条款讨论一些最重要的威胁，以便了解和防护。这些威胁中的大多数包括在 GB/Z 25320 中，至少在监视层面上是如此。

5.2.2 无意威胁

5.2.2.1 安全事故

安全性始终是电力部门主要关心的，特别对那些工作于变电站的高电压环境中的现场人员。一些极其细致的规程已经被制定和一再反复地精心修改，以改进安全性。虽然这些规程是安全性步骤的最重要组成部分，然而通过电子手段对关键设备的状态进行监视和对符合于安全规程情况进行日志记录或告警，能把安全性提高到相当程度并且在其他方面带来益处。

特别是虽然主要出于安全性原因，已经实施了仅允许授权人员进入变电站的访问措施，然而对这些安全性措施进行电子监视同样能有助于防止某些蓄意攻击，比如故意破坏和窃取。

5.2.2.2 设备故障

对电力系统的可靠运行，设备故障是最通常且料想得到的威胁。多年来已经采取了有效措施去监视变电站设备状态，比如油温、冷却系统、频率偏差、电压水平和电流过负荷。除这些额外信息能提供更多的物理安全外，GB/Z 25320 的本部分并不关心这些监视的类型。

然而，对设备的物理状态进行监视经常也能有利于维护效率，可能防止某些类型的设备故障，实时检测以前没被监视的故障以及对设备故障的处理和影响进行探讨分析。因此，考虑到这些额外价值，对物理安全进行某种监视的总成本效益就能有所提高。

5.2.2.3 疏忽大意

疏忽大意是对变电站资产进行防护的“威胁”之一，无论允许尾随进入变电站还是没锁门或不小心

4) “一个尺寸不会适合于所有”，一种解决方案不可能用于所有情况。所以，在此意义上，应允许多种解决方案。

使得未经授权人员接触口令、钥匙和其他安全措施。这种疏忽大意经常是由于过于自信("还从没有人破坏过变电站的设备")或懒惰("哎呀！关这门多麻烦，一会儿我就要去别的地方")或愤怒("这些安全措施正在影响我的工作")所造成。

5.2.2.4 自然灾害

自然灾害，例如暴风雨、飓风和地震，能够导致大范围的电力系统故障、安全性破坏和为窃取、蓄意破坏和恐怖行为造成机会。对现场设施和设备的物理和信息状态的实时监视能够为电力部门提供"眼睛和耳朵"以了解什么正在发生，并采取纠正行为使这些自然灾害对电力系统运行的影响降至最小。

5.2.3 蓄意威胁

5.2.3.1 概述

相对于无意威胁，对变电站中设施和设备的恶意威胁能够导致更突出的危害。采用这些蓄意威胁的诱因正在增加，因为对攻击者来说，成功攻击的结果可能日益具有经济和"社会或政治"的益处。通过实时通告和司法追踪，对成功攻击的极坏影响有所抑制的同时，对设施和设备采用先进技术的监视能够有助于防范这些威胁中的某些威胁。

5.2.3.2 心怀不满的雇员

心怀不满的雇员是攻击电力系统资产的主要威胁之一。具有破坏知识的不满雇员实质上比非雇员的危险更大，特别是在电力系统行业中，那里的许多系统和设备是完全独特的。

5.2.3.3 工业间谍

在电力系统行业中工业间谍正成为更大的威胁，因为解除管制和竞争涉及数百万美元，这提供了对信息的未经授权访问的不断增长的动力，并进而出于邪恶目的可能危及设备。除了经济利益外，通过揭示竞争者的无能或不可信任，某些攻击者会获得"社会或政治"益处。

5.2.3.4 故意破坏

故意破坏行为能够危及设施和设备，而对攻击者而言，除了进行故意破坏的行为以及向他们自身和其他人证明了他们能够实施故意破坏之外，并不具有任何特定利益。故意破坏者常常意识不到或不关心他们行为的可能后果。

对进入已锁设施的通道和入口进行实时监视，和对任何访问异常进行实时告警能有助于防止大多数故意破坏。然而一些故意破坏，比如从变电站外对开关场中设备进行射击或关闭设备和软件应用，似乎需要另外的监视类型。

5.2.3.5 计算机骇客

骇客就是为获取利益寻求突破计算机安全防护的人。所获利益可以直接是金钱的、工业知识的、政治的、社会的利益，或仅是个人的挑战以证实该骇客能够获得访问。多数骇客使用因特网作为他们的主要进入通路，因此大多数电力部门使用各种防火墙、隔离技术和其他应对措施，把电力系统的运行系统和因特网隔离。

在公众眼中计算机安全常仅被看作是对骇客及其相关问题、计算机病毒和蠕虫进行防护。由于电力运行的计算机系统大概一直与因特网隔离，许多电力部门人员根本不理解在这些系统中增加安全措施的道理。然而正如从这些条款文字中可清晰看到的那样，这可能不再是正确的，因为网络化变得更普遍而且额外的信息访问需求也在增长(例如厂商远程访问、便携电脑的维护访问、继电保护工程师取回特殊数据的访问等)。

5.2.3.6 病毒和蠕虫

如同骇客那样，病毒和蠕虫通常通过因特网进行攻击。然而一些病毒和蠕虫能嵌入到软件里，而此软件却被装载进已经与因特网相隔离的系统中，或病毒和蠕虫有可能会从某个不安全的便携电脑或其他系统经过安全通信而传播。它们可能包括中间人病毒、截获电力系统数据的间谍软件和其他木马。

5.2.3.7 窃取

窃取有一个直接了当的目的，即攻击者取得他们无权得到的某种东西(设备、数据或知识)。通常就

动机而言，此目的有经济利益，虽然其他动机也是可能的。

此外，对已锁设施的进入通道和入口进行监视和对设备的物理状态和状况的异常（如不响应或断连）告警是警示运行人员窃取可能正在发生的主要方法。

5.2.3.8 恐怖行为

恐怖行为是最少可能发生但却可能具有最严重后果的威胁，由于恐怖行为的主要目的就是要造成最大程度的物理、经济和社会、政治的危机。

对可能的恐怖分子袭击（比如物理上炸掉变电站或其他设施），对变电站设施（包括物理上靠近）的进入通道和入口进行监视和异常告警，可能是警示运行人员的最有效手段。然而，恐怖分子在他们的行动中会变得更有经验，而能够寻求对整个电力系统暗中做到比仅爆炸一个变电站更大损害的方式，来破坏特定设备或使得关键设备无效。所以额外增加监视类型（包括设备的状态和状况）是很重要的。

5.3 安全的需求、威胁、脆弱性、攻击和应对措施

5.3.1 安全需求

无论用户是人还是软件应用，他们或多或少都有四种基本安全需求，保护他们免于四种基本威胁。在每种情况中作为基本前提，授权要求认证用户：

- 机密性（Confidentiality）：防止对信息的未经授权访问；
- 完整性（Integrity）：防止未经授权修改或窃取信息；
- 可用性（Availability）：防止拒绝服务和保证对信息的授权访问；
- 不可抵赖性或可追溯性（Non-repudiation or Accountability）：防止否认已发生行为或伪称并没发生行为。

5.3.2 安全威胁

通常存在四种类型计算机安全威胁：

- 未经授权访问信息；
- 未经授权修改或窃取信息；
- 拒绝服务；
- 抵赖或不可追溯。

然而，存在许多不同类型的脆弱性和利用这些脆弱性使这些威胁得以成功的攻击方法。安全应对措施应该考虑这些不同类型的脆弱性和攻击方法。

5.3.3 安全脆弱性

计算机安全脆弱性指的是系统中的薄弱点或其他漏洞，会使有意或无意的未经授权行为实现威胁。脆弱性可能由系统中的程序错误或设计缺陷造成，但也可能由设备故障和物理动作造成。脆弱性可能仅在理论上存在或是已知的行为。

5.3.4 安全攻击

有多种不同类型的攻击能实现威胁，在图1中说明了一些攻击类型。正如看到的，同样的攻击类型常可能涉及不同的安全威胁。呈网状的各种潜在攻击意味着为满足一个特定安全需求并不存在恰好一种方法；对一种特定威胁的每种攻击类型都需要设法应对。

此外，虽在“攻击链”中存在一系列攻击，可能涉及不同资产以及可能随时发生；但是也还能认为“攻击链”是一种特定的威胁。

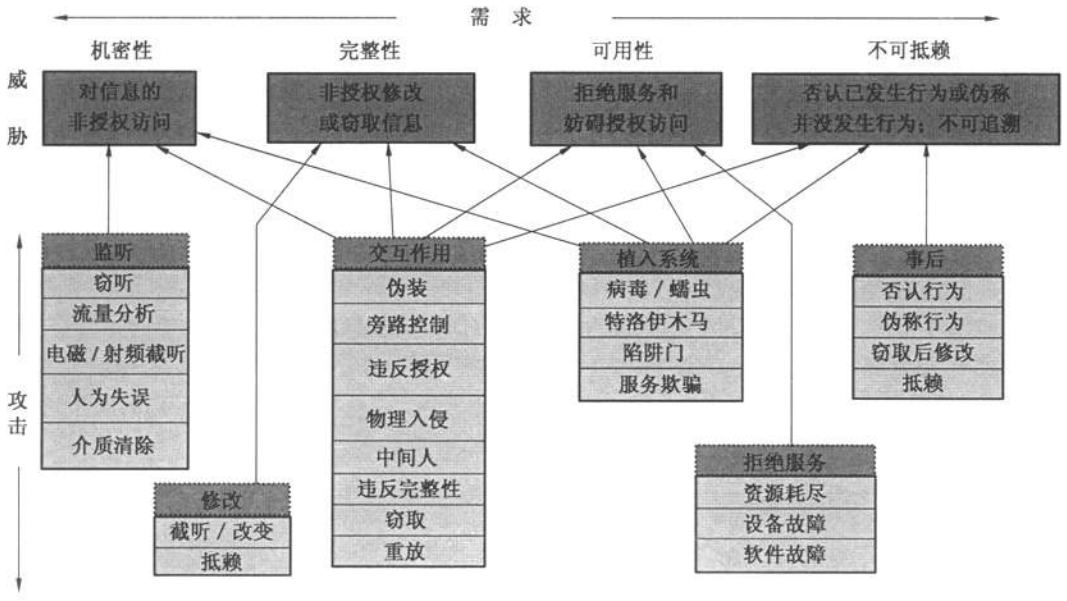

图 1 安全需求、威胁和可能的攻击

5.3.5 安全类别

出自一种安全观点，计算机安全能分为四个类别，见图 2。说明如下：

所有这四类通常都需要有为达到“端对端”安全所使用的安全措施。只对一类进行安全防护通常肯定是不够的。例如，只实现虚拟专网(VPN)，只处理对通信的传输协议的威胁，既不防止一个人伪装成另一个人，也不防止主计算机中恶意的软件应用经此 VPN 对现场装置进行通信。

这些安全措施很好地综合起来使用，就不会发生疏漏问题。

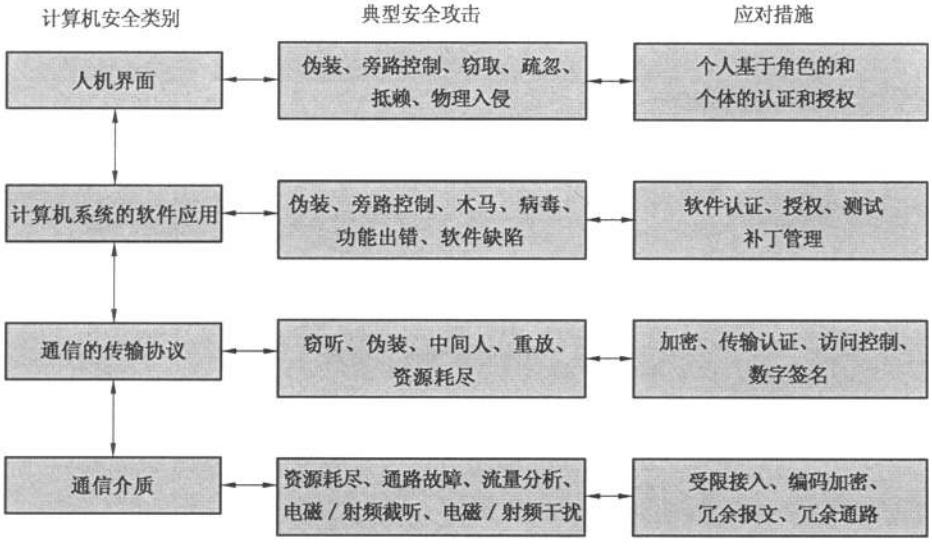

图 2 安全类别、典型攻击和通用应对措施

5.3.6 安全应对措施

安全应对措施如图 3、图 4、图 5 和图 6 所示，同样是网状的相关技术和对策。并非所有安全应对措施对所有系统在所有时间都是需要或希望的，而这可能会造成大量过度杀伤且可能会使整个系统趋向于不可用或非常慢。因而首要的一步就是确定哪些应对措施对于满足哪些需要是有益的。所有应对措施都表示在图 7 中。

这些图仅是资料性的，并不是图中所有项都在 GB/Z 25320 中处理。

在图 3～图 7 中，四种安全需求(机密性、完整性、可用性和不可抵赖性)显示在每幅图的顶部。基本的安全威胁显示在每种需求下面。应对这些威胁所使用的关键安全服务和技术显示在紧接于威胁下面的各方框中。这些只是普遍使用的安全措施的例子，以箭头指明哪些技术和服务参与支持在技术和服务上的安全措施。例如，加密用于许多安全措施中，包括传输层安全协议(TLS)、虚拟专网(VPN)、无线安全和“链路端加密盒”(bump-in-the-wire)技术。这些技术本身又支持 IEC 62351 和公钥基础设施(PKI)。通常用这些标准和 PKI 是为了认证，因此就能够指定口令和证书。在每幅图的底部，安全服务和技术下面是安全管理和安全对策，为所有安全措施提供基础。

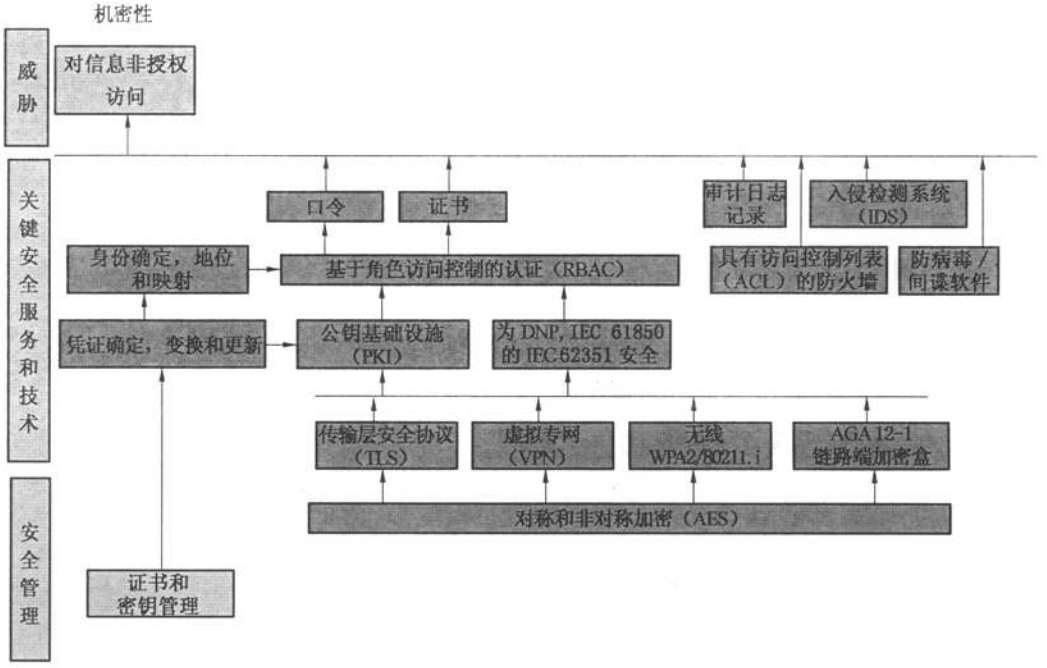

图 3 机密性安全应对措施

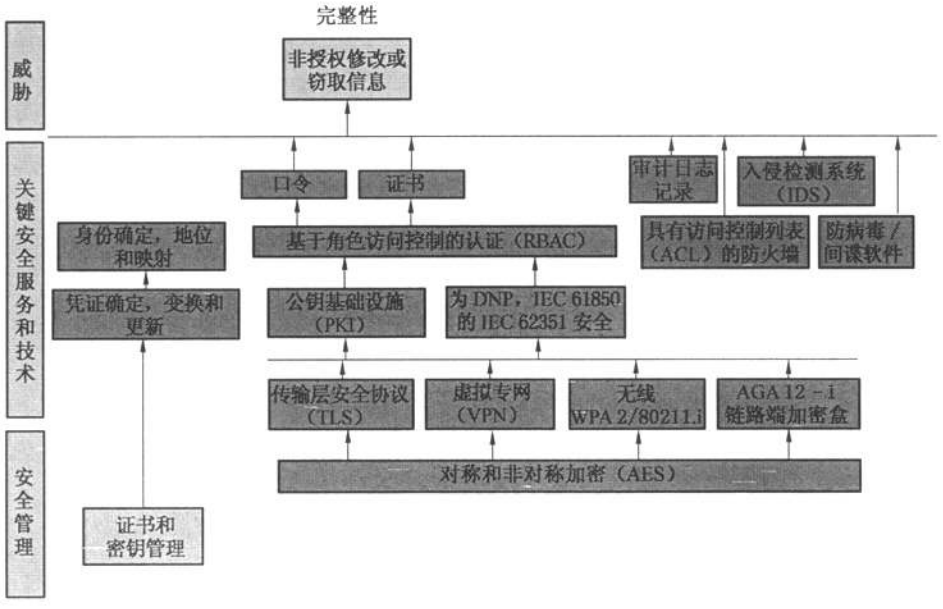

图 4　完整性安全应对措施

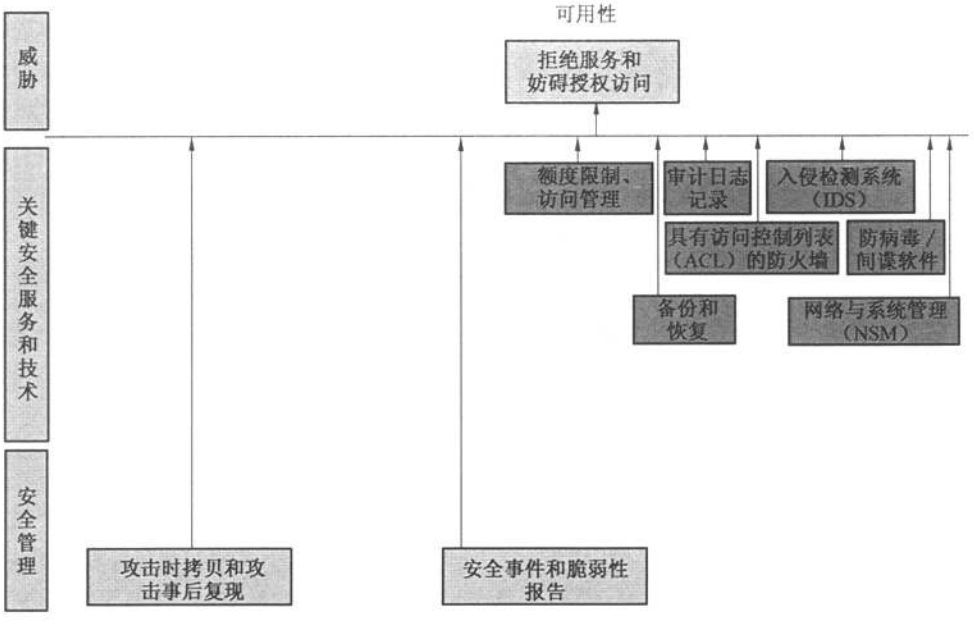

图 5　可用性安全应对措施

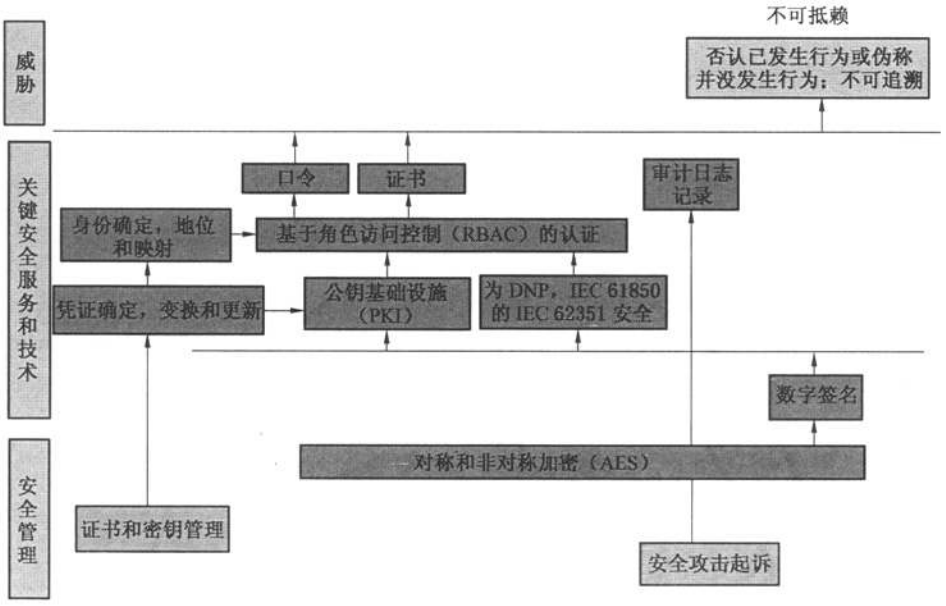

图 6　不可抵赖安全应对措施

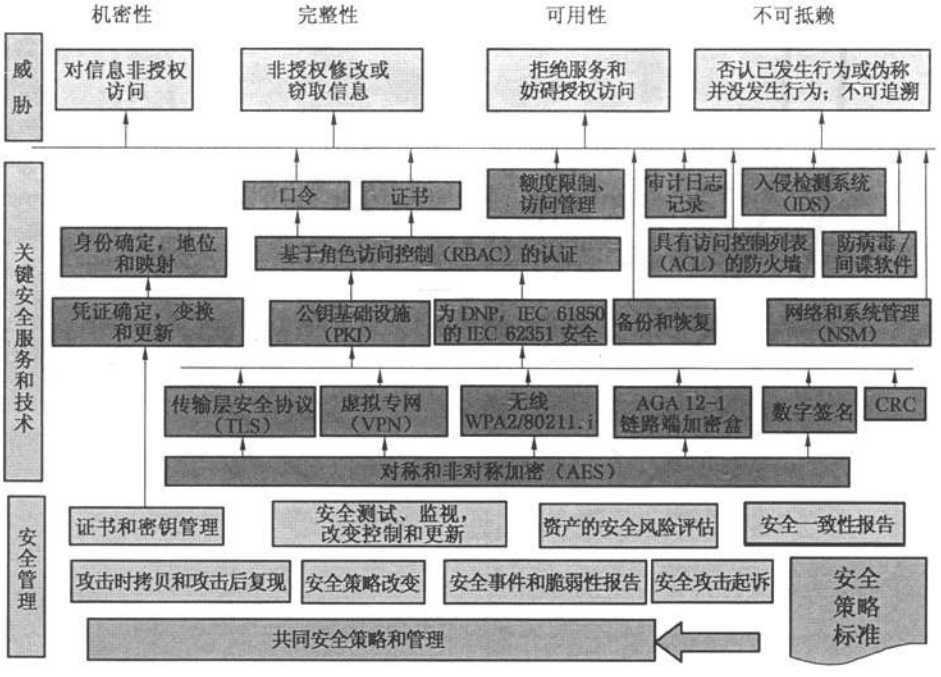

图 7　总安全：安全需求，威胁，应对措施和管理

5.3.7　分解安全问题空间

安全包括一套极其复杂且多维的问题。不存在任何标准化的或清晰规定的机制去分解安全问题空间，因此以成本效益方法分析和部署既适度又完善的安全措施，常会感到这是无法实现的。