国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1032

(12/2010)

X系列：数据网、开放系统通信和安全性

信息和网络安全 – 网络安全

电信IP网络安全系统外部相互关系架构

ITU-T X.1032建议书

ITU-T

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1-X.199
开放系统互联互通	X.200-X.299
网间互通	X.300-X.399
报文处理系统	X.400-X.499
号码簿	X.500-X.599
OSI 组网和系统概貌	X.600-X.699
OSI 管理	X.700-X.799
安全	X.800-X.849
OSI 应用	X.850-X.899
开放分布式处理	X.900-X.999
信息网络安全	
一般性安全问题	X.1000-X.1029
网络安全	**X.1030-X.1049**
安全管理	X.1050-X.1069
远程生物测定	X.1080-X.1099
安全应用和业务	
多点传送安全	X.1100-X.1109
家庭网络安全	X.1110-X.1119
移动安全	X.1120-X.1139
网络安全	X.1140-X.1149
安全协议	X.1150-X.1159
点对点安全	X.1160-X.1169
网络身份安全	X.1170-X.1179
IP电视安全	X.1180-X.1199
网络空间安全	
网络安全	X.1200-X.1229
打击垃圾邮件	X.1230-X.1249
身份管理	X.1250-X.1279
安全应用和业务	
应急通信	X.1300-X.1309
无所不在的传感器网络安全	X.1310-X.1339
网络安全信息交流	
计算机信息交流	X.1500-X.1519
易受攻击性/国家交流	X.1520-X.1539
情况/事件 /启发性交流	X.1540-X.1549
政策交流	X.1550-X.1559
启发法和信息请求	X.1560-X.1569
识别和发现	X.1570-X.1579
可靠的交流	X.1580-X.1589

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1032建议书

电信IP网络安全系统外部相互关系架构

摘要

本ITU-T X.1032建议书提出了可用来审议电信IP网络安全系统（TNSS）与各类外部对象相互关系的四个模型。根据其主要功能及其对TNSS建设和运转原则可能产生的影响对每个对象进行了审议。本建议书为制定有关网络安全对外部对象影响的具体建议奠定了基础。

历史

版本	建议书	批准	研究组
1.0	ITU-T X.1032	2010-12-17	17

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准ITU-T建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

© 国际电联 2011

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1 范围 1
2 参考文献 2
3 定义 2
3.1 其它资料定义的术语 2
3.2 本建议书定义的术语 2
4 缩写词和首字母缩略语 3
5 惯例 3
6 概述 3
7 TNSS与信息系统和信息结构的安全系统的相互关系 3
7.1 相互关系模型 3
7.2 外部对象的功能及其对TNSS的影响 3
8 TNSS与电信系统对象的相互关系 5
8.1 相互关系模型 5
8.2 外部对象的功能及其对TNSS的影响 5
9 TNSS与外部组织的相互关系 6
9.1 相互关系模型 6
9.2 外部组织的功能及其对TNSS的影响 6
10 TNSS与安全威胁来源的相互关系 7
10.1 相互关系模型 7
10.2 外部对象的功能及其对TNSS的影响 7
附录一 电信IP网络技术设施的可能构成 9
参考资料 10

ITU-T X.1032建议书

电信IP网络安全系统外部相互关系架构

1 范围

1.1 对任何对象的研究不仅要考虑对象内不同组成部分之间的相互关联，还应考虑该对象的外部相互关系。通过外部关系，该对象在整体系统环境中行使功能。此外，这些相互关系可能形成影响该对象运行的不同威胁。

采用这种手段开展对象研究对于电信IP网络安全系统（TNSS）而言特别重要，TNSS主要需要保护电信IP网络免遭外部威胁（见图1）。

附录一显示了电信IP网络技术设施的可能构成情况。

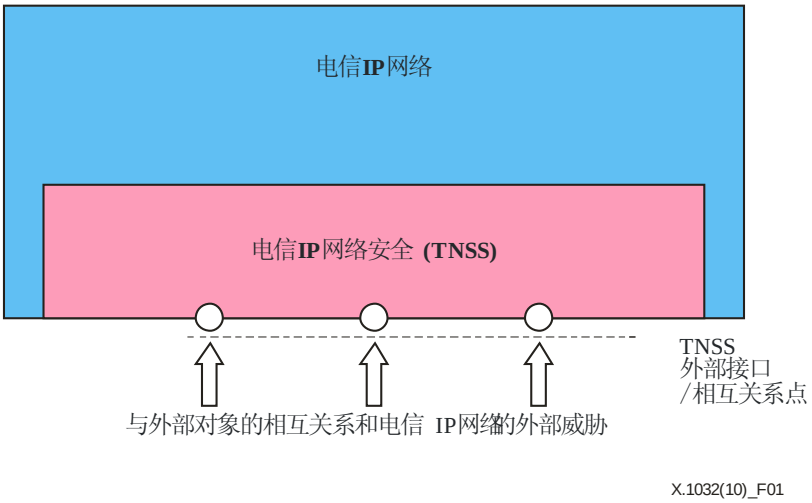

图1 – 电信IP网络安全系统和外部对象之间的相互关系

1.2 TNSS不是一个独立运行的系统，它与若干外部系统具有密切的互动。

这些系统首先包括保护TNSS的电信网本身。传输媒介和服务平台的建设原则直接决定对TNSS的要求和TNSS建设原则。

第二，这些外部系统包括电信IP网络用户。他们的要求必须通过包括TNSS在内的电信IP网络得到满足。

一些其它的外部组织亦能影响到TNSS建设原则。这些组织包括：

– 国家监管机构；
– 为安全系统提供服务的可信赖的第三方（基于“外包”原则）；
– 使用电信IP网络服务创建信息网络的组织。

总之，TNSS 的主要任务包括保护电信网和通过该网络传输的信息免受安全威胁。因此，TNSS 在运转中面临各种外部安全威胁。

上述清单表明，TNSS 与众多外部对象具有相互关系，这些对象可细分为若干组。

1.3 TNSS与外部对象的相互关系可直接或间接影响到对TNSS的要求和TNSS建设和运转原则。因此，TNSS的发展过程中应考虑到这些相互关系。ITU-T建议书已经将该问题的某些方面考虑在内，举例而言，[ITU-T X.842]和[ITU-T X.843]考虑了与可信赖的第三方之间的相互关系。但是，TNSS与外部对象相互关系的很多方面至今为止尚未得到考虑。

1.4 本建议书涉及TNSS与外部对象相互关系的总体架构。该架构适用于各种类型的电信IP网络以及各种电信安全系统。本建议书旨在提纲契领地介绍TNSS的所有外部相互关系，它为网络安全制定有关外部对象影响的具体建议奠定基础。

2 参考文献

下列 ITU-T 建议书和其它参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所标示的版本是有效的。所有的建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的 ITU-T 建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T X.800] ITU-T X.800 建议书（1991 年）：CCITT *应用开放系统互通的安全架构*

[ITU-T X.805] ITU-T X.805建议书（2003年）：*提供端到端通信的系统的安全架构*

[ITU-T X.842] ITU-T X.842建议书（2000年）：*信息技术 – 安全技术 – 可信赖的第三方业务使用和管理导则*

[ITU-T X.843] ITU-T X.843建议书（2000年）：*信息技术 – 安全技术 – 支持应用数字签名的第三方（TTP）业务技术规范*

3 定义

3.1 其它资料定义的术语

无。

3.2 本建议书定义的术语

本建议书定义的术语如下：

3.2.1 安全系统：相互关联的不同元素（提供安全的一些原则、组织和技术措施），它们最大程度地降低资产和资源的风险。

3.2.2 电信IP网络安全系统（TNSS）：电信IP网络中使用的安全系统。

4 缩写词和首字母缩略语

本建议书使用了以下缩写词和首字母缩略语：

ICT 信息通信技术

TNSS 电信IP网络安全系统

5 惯例

无。

6 概述

6.1 对TNSS与外部对象相互关系的考虑。由于这种对象数量之大以及五花八门的关系和接口而多种多样。因此，主要的问题是将相互关系进行分解（拆分）的可能性。本建议书建议将外部相互关系类型分为四种：

– TNSS与叠加于基础设施信息系统和信息结构之上的安全系统的相互关系；

– TNSS与电信系统对象的相互关系；

– TNSS与诸如外部组织等其它对象的相互关系；

– TNSS与上述命名对象或新对象等安全威胁的相互关系。

以下第 7、8、9 和 10 节分别探讨了这些相互关系类型。

6.2 此外，第7、8、9和10各节采用了分解原则。首先，用图形表定义了相互关系模型。该模型包含外部对象及其与TNSS之间的相互关系。之后，对各外部对象的功能进行阐述。最后，从这些功能就以下方面做出简要评价：

– 外部对象对TNSS可能造成的影响（如，对TNSS要求的影响、对TNSS建设和运转原则的影响）；

– 可能的相互关系类型（如，电器接口、组织要求、外部环境影响）。

7 TNSS与信息系统和信息结构的安全系统的相互关系

7.1 相互关系模型

图 2 显示了 TNSS 与叠加于基础设施信息系统之上的安全系统的相互关系，该系统转而又与信息结构安全系统拥有接口。

7.2 外部对象的功能及其对TNSS的影响

7.2.1 信息系统使用各种利用电信的信息技术。信息系统的功能包括信息的收集、存储和检索、数据库的组织和用户网址、编辑、转换和其它信息处理方面的技术支持。信息系统可执行远程信息传送和发布功能，使用电信服务（如，来自信息电信网络的服务）。互联网就是公众信息电信网络的一个例子。

传统的通信类型（如电话通信和传真通信）在使用和不使用信息电信网络的情况下均可受到影响。

信息系统的安全系统用来保护这些系统的技术流程和这些系统中存储和转发的信息。信息系统的安全系统可以下列方式影响TNSS，如：

– 在保护网络免受某种威胁（如信息披露）时相互补充；及

– 为在TNSS内使用的安全协议增加限制。

TNSS 与信息系统的安全系统的外部相互关系可以是：

– 硬件或软件接口；

– 契约性协议。

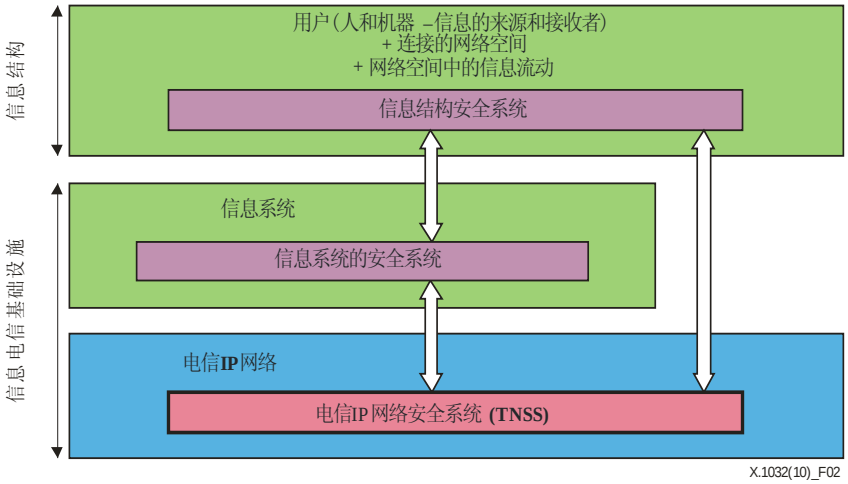

图 2 – TNSS与信息系统和信息结构安全系统的相互关系模型

7.2.2 信息结构确保信息被用于人类社会的各种活动。信息结构安全系统用来保护网络空间的用户（信息的作者、所有者、来源、接收者和购买者）免受中断用户工作的网络空间的入侵。网络空间用户包括人和机器（传感元素、驱动器、自动化装置等）。意外入侵的事例包括病毒、“蠕虫”、垃圾信息、和网络空间存在的各种恶意程序。意外入侵还可能包括在信息通信基础设施中拒绝服务。

信息结构安全系统可能直接或通过信息网络安全系统影响 TNSS。例如，它可对 TNSS 提出通过技术手段保护网络空间的要求，从而支持信息结构安全系统内法律、行政和组织措施的落实。这种技术手段包括打击病毒和垃圾信息的手段。

TNSS 与信息结构安全系统的外部相互关系可以通过契约性协议加以明确。

8 TNSS与电信系统对象的相互关系

8.1 相互关系模型

图 3 显示了 TNSS 与自身电信网络对象和其它电信系统对象的安全系统，即与用户终端设备和邻近电信网络的相互关系。

8.2 外部对象的功能及其对TNSS的影响

8.21 电信网络内部对象（传输层和服务层）决定了所提供的电信服务的专门术语以及这些服务的定量和定性特点。这些对象直接影响TNSS，尤其是，它们决定：

– 需要保护的服务清单；

– 实现安全机制的网络可能性。

TNSS 与传输层和服务层的外部相互关系可以是：

– 硬件或软件接口；或

– 契约性协议。

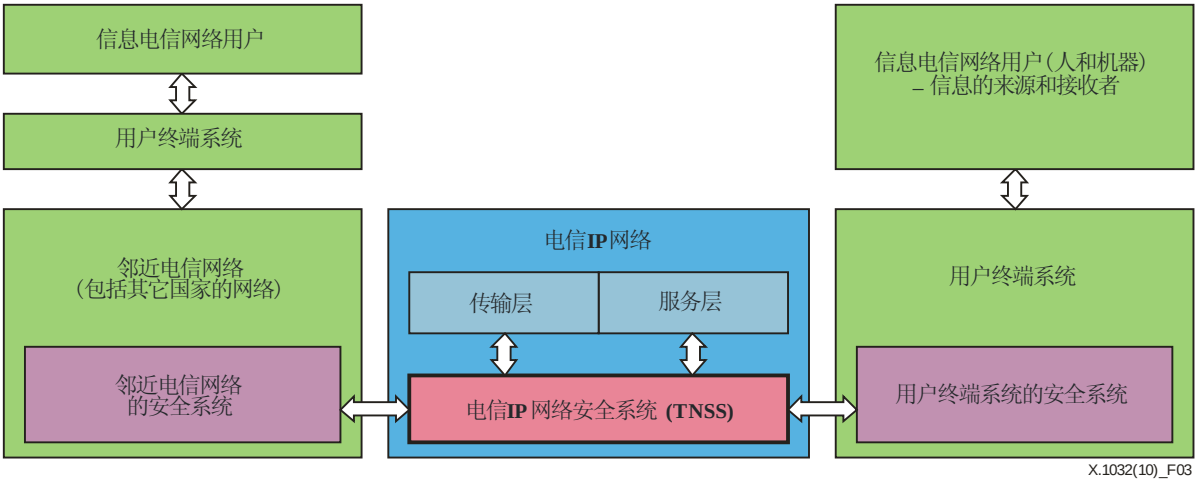

图 3 – TNSS与电信系统对象的相互关系模型

8.22 用户终端系统可能包括一些终端设备（电话设备、电视机、计算机和其它类型终端）以及相关的家庭/企业网络连接（详情见附录一）。用户终端系统的安全系统行使保护终端设备和家庭/企业网络免受安全威胁的功能。这些威胁既可来自连接的电信网，也可来自内部来源（如，用户的终端系统）。此外，用户终端系统的安全系统具有保护向电信网传送的用户信息的机制。

用户终端系统的安全系统可能影响 TNSS，具体说来：它们可

– 通过对所传数据加密，在保护用户信息免受某种威胁的过程中相互支持；

– 决定TNSS必须保证的预定安全级别要求。

TNSS 与用户终端系统安全系统的外部相互关系可能是：

– 电器接口；或

– 组织的要求和限制。

8.23 邻近电信网络（包括其它国家的网络）与所考虑的电信网络交换业务。邻近电信网络的安全系统行使保护这些网络和通过这些网络传送的信息免受安全威胁的功能。这些系统可能影响TNSS，具体说来， 它们可：

– 在保护用户信息免受破坏或修改的过程中相互支持；

– 为使用一些TNSS安全机制或使这些安全机制模式得到运行引入限制。

TNSS 与邻近电信网络安全系统的外部相互关系可为：

– 电器接口；或

– 达成的双边组织条款。

9 TNSS与外部组织的相互关系

9.1 相互关系模型

图 4 显示了 TNSS 与电信网络的各种外部组织的相互关系：

– 监管机构；

– 可信赖的第三方；

– 执法机构；及

– 技术工具（软件和硬件）提供商。

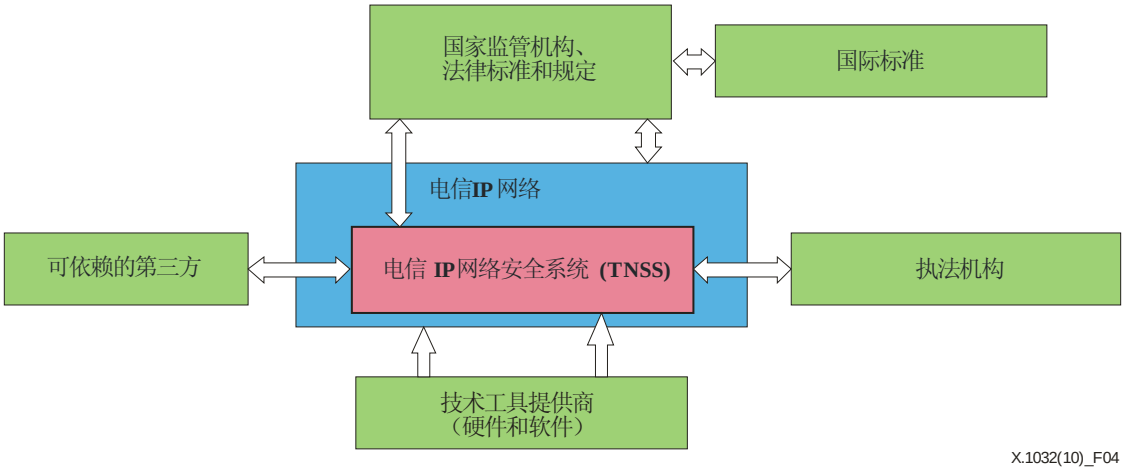

图 4 – TNSS与外部组织的相互关系模型

9.2 外部组织的功能及其对TNSS的影响

9.2.1 监管机构制定电信领域的一般性政策。特别是，它们支持制定和应用国际标准、法律和法规，同时支持制定国家标准。

9.2.2 按照与电信网络运营商达成的双边协议，第三方可行使一些功能，以确保TNSS的运行。

这些功能的清单和第三方与之间的互动原则是由基础设施运营商确定的，在基础设施中已包含了特定的 TNSS。

TNSS 与可信赖的第三方的外部相互关系可为：

– 硬件或软件接口；或

– 契约性协议。

9.23 执法机构应对信息电信网络领域内违反国家法律的行为予以打击（起诉犯罪分子）。特别是，它们应捕获这类违法行为的犯罪分子。执法机构的工作和TNSS的功能应互为补充，从而提高电信安全。

鉴于信息通信技术（ICT）在人类社会所有领域中的重要性，随着我们向信息社会迈进，法律的制定在目前和将来仍十分重要。这种趋势终将增强相关执法机构的作用。

为履行上述职能，执法机构应及时从电信网络运营商处获悉有关构成违法行为的安全事件的数据。TNSS 应对信息进行获取、保存和分析，这将有助于对相应信息进行汇总，并传送给执法机关。将有关安全事件的信息从电信组织传送给执法机构的可能性在[b-ITU-T E.409]、[b-ITU-T X.1051]和[b-ITU-T X.1056]中有所阐述。

TNSS 与执法机构的外部相互关系可为：

– 电器接口或其它电信服务或邮政服务；

– 达成的双边组织协议。

10 TNSS与安全威胁来源的相互关系

10.1 相互关系模型

图 5 显示了 TNSS 与各种安全威胁来源的相互关系模型，这些来源包括：

– 用户及其连接至所述电信网络的终端系统；

– 外来者（非用户）和外部媒体；

– 电信网络的对象和人员；

– 包括相关用户和用户终端系统的邻近电信网络；

– 连通的信息系统；

– 可信赖的第三方；

– 技术工具的提供方。

10.2 外部对象的功能及其对TNSS的影响

安全威胁来源可攻击电信网络。电信 IP 网络安全系统（TNSS）用于警告、检测和应对这些攻击。因此，如图 5 所示，可以说，安全威胁与 TNSS 直接相关。

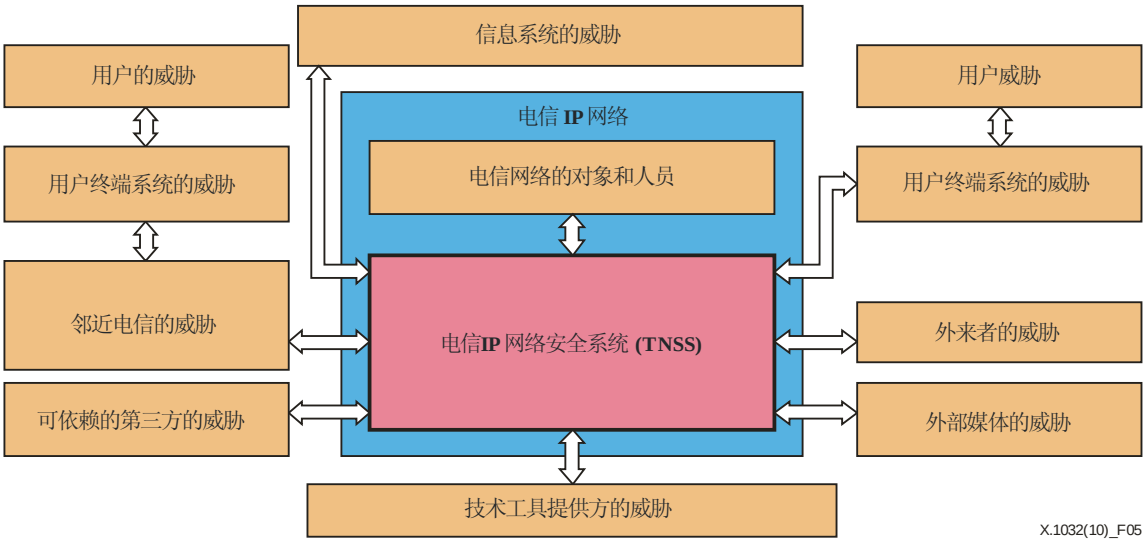

图 5 – TNSS 与安全威胁来源的相互关系模型

这些威胁按在[ITU-T X.800]和[ITU-T X.805]中分为以下五个类型：

– 对信息和其它资源的破坏；
– 对信息的损坏或修改；
– 信息和其它资源的盗用、消除或丢失；
– 信息披露；及
– 服务中断。

电信网络的安全政策可用来打击所有威胁，或打击某些威胁。由此，在 TNSS 的设计中选择了需要的安全尺度。这些安全威胁与安全尺度的对应关系见 [ITU-T X.805]表 1。

TNSS 与安全威胁来源的外部相互关系可为：

– 电器接口；
– 人员行动；
– 通过电信网络使用技术手段及使用外部技术手段进行的攻击；
– 外部环境影响；
– 应对攻击的技术措施；及
– 应对攻击的组织措施。

附录一

电信IP网络技术设施的可能构成

（本附录不构成本建议书不可分割的一部分）

I.1 本建议书使用术语“电信网络”涵盖以下电信运营商的设施：

– 基础设施提供商的设施（即网络节点、连接电路、接入网等）；

– 服务提供商的设施（即业务服务器等），服务提供商可通过基础设施提供商发挥作用，否则，服务提供商可在网络内独立运行；

– 应用提供商的设施（即应用服务器等），应用提供商可通过服务提供商发挥作用；否则，应用提供商可在网络内独立工作；

– 连接、与电信运营商的连接（即与基础设施/服务/应用提供商的连接）；

– 在基础设施/服务/应用提供商运行的设施内传送和存储的信息。

I.2 电信网络不包含“用户终端系统”。这类系统包括：

– 电信用户终端（及用来行使基础设施用户、服务用户和应用用户功能（其中包括执行某些本地功能（消息的拟定和编辑））的软件）；

– 应用服务器（如用户行使网络结构以外应用服务提供商的功能）；

– 企业/本地/家庭网络（如有的话）；

– 防火墙/网关（如有的话）；及

– 传送、接收和存储的用户信息。

参考资料

[b-ITU-T E.409] ITU-T E.409建议书（2004年）：事件组织和安全事件处理：电信组织导则

[b-ITU-T X.1051] ITU-T X.1051建议书（2008年）| ISO/IEC 27011:2008：信息技术 – 安全技术 – 基于ISO/IEC 27002的电信组织信息安全管理导则

[b-ITU-T X.1056] ITU-T X.1056建议书 (2009年)：电信组织安全事件管理导则

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	电信系统使用的语言和一般性软件情况

瑞士印制
2011年，日内瓦