YD

中华人民共和国通信行业标准

YD/T 1744-2008

传送网安全防护要求

Security Protection Requirements for Transport Network

2008-01-14 发布　　2008-01-14 实施

中华人民共和国信息产业部　发布

目　　次

前　言

本标准是“电信网和互联网安全防护体系”系列标准之一。该系列标准的结构及名称如下：

1. YD/T 1728-2008　电信网和互联网安全防护管理指南；
2. YD/T 1729-2008　电信网和互联网安全等级保护实施指南；
3. YD/T 1730-2008　电信网和互联网安全风险评估实施指南；
4. YD/T 1731-2008　电信网和互联网灾难备份及恢复实施指南；
5. YD/T 1732-2008　固定通信网安全防护要求；
6. YD/T 1733-2008　固定通信网安全防护检测要求；
7. YD/T 1734-2008　移动通信网安全防护要求；
8. YD/T 1735-2008　移动通信网安全防护检测要求；
9. YD/T 1736-2008　互联网安全防护要求；
10. YD/T 1737-2008　互联网安全防护检测要求；
11. YD/T 1738-2008　增值业务网——消息网安全防护要求；
12. YD/T 1739-2008　增值业务网——消息网安全防护检测要求；
13. YD/T 1740-2008　增值业务网——智能网安全防护要求；
14. YD/T 1741-2008　增值业务网——智能网安全防护检测要求；
15. YD/T 1742-2008　接入网安全防护要求；
16. YD/T 1743-2008　接入网安全防护检测要求；
17. YD/T 1744-2008　传送网安全防护要求；
18. YD/T 1745-2008　传送网安全防护检测要求；
19. YD/T 1746-2008　IP承载网安全防护要求；
20. YD/T 1747-2008　IP承载网安全防护检测要求；
21. YD/T 1748-2008　信令网安全防护要求；
22. YD/T 1749-2008　信令网安全防护检测要求；
23. YD/T 1750-2008　同步网安全防护要求；
24. YD/T 1751-2008　同步网安全防护检测要求；
25. YD/T 1752-2008　支撑网安全防护要求；
26. YD/T 1753-2008　支撑网安全防护检测要求；
27. YD/T 1754-2008　电信网和互联网物理环境安全等级保护要求；
28. YD/T 1755-2008　电信网和互联网物理环境安全等级保护检测要求；
29. YD/T 1756-2008　电信网和互联网管理安全等级保护要求；
30. YD/T 1757-2008　电信网和互联网管理安全等级保护检测要求；
31. YD/T 1758-2008　非核心生产单元安全防护要求；
32. YD/T 1759-2008　非核心生产单元安全防护检测要求。

本标准与YD/T 1745-2008《传送网安全防护检测要求》配套使用。

随着电信网和互联网的发展，将不断补充和完善电信网和互联网安全防护体系的相关标准。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院、中国电信集团公司、中国移动集团通信公司、中国网络通信集团公司、中国联合通信有限公司

本标准主要起草人：赵文玉、胡昌军、袁　琦、赵　阳、易　武、支春龙、陈忠民、肖延敏

传送网安全防护要求

1 范围

本标准规定了传送网(含光传送网、微波接力传送网和卫星传送网)在安全等级保护、安全风险评估、灾难备份及恢复等方面的安全防护要求。

本标准适用于公用电信传送网中的传送网。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。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标准。然而，鼓励根据本标准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标准。

GB 7611-2001	数字网系列比特率电接口特性
GB/T 16712-1996	同步数字体系（SDH）复用设备技术要求
GB/T 20185-2006	同步数字体系设备和系统的光接口技术要求
GB/T 13159-91	数字微波接力通信系统进网技术要求
GB/T 15841-1995	数字微波通信设备进网技术要求 2~8GHz 数字微波收发信机
YD/T 1728-2008	电信网和互联网安全防护管理指南
YD/T 1729-2008	电信网和互联网安全等级保护实施指南
YD/T 1730-2008	电信网和互联网安全风险评估实施指南
YD/T 1731-2008	电信网和互联网灾难备份及恢复实施指南
YD/T 1754-2008	电信网和互联网物理环境安全等级保护要求
YD/T 1756-2008	电信网和互联网管理安全等级保护要求
YD 5014-1995	数字复用设备安装工程施工及验收技术规范(PDH)部分
YD/T 1016-1999	接入网用 PDH 光端机技术条件
YD/T 1022-1999	同步数字体系(SDH)设备功能要求
YD/T 1017-1999	同步数字体系(SDH)网络节点接口
YD/T 1289.1-2003	同步数字体系（SDH）传送网网络管理技术要求 第一部分：基本原则
YD/T 1289.2-2003	同步数字体系（SDH）传送网网络管理技术要求 第二部分：网元管理系统（EMS）功能
YD/T 1289.3-2003	同步数字体系（SDH）传送网网络管理技术要求 第三部分：网络管理系统（NMS）功能
YD/T 1289.4-2006	同步数字体系（SDH）传送网网络管理技术要求 第 4 部分：网元管理系统（EMS）与网络管理系统（NMS）接口功能
YD/T 900-1997	SDH 设备技术要求——时钟
YD/T 974-1998	SDH 数字交叉连接设备（SDXC）技术要求和测试方法
YD/T 1167-2001	STM-64 分插复用（ADM）设备技术要求
YD/T 882-1996	STM-1，STM-4，STM-16 再生中继设备主要技术要求

YD/T 1420-2005	基于2048kbit/s系列的数字网抖动和漂移技术要求
YD/T 1238-2002	基于SDH的多业务传送节点技术要求
YD/T 1345-2005	基于SDH的多业务传送节点（MSTP）技术要求——内嵌弹性分组环（RPR）功能部分
YD/T 1474-2006	基于SDH的多业务传送节点（MSTP）技术要求——内嵌多协议标记交换（MPLS）功能部分
YD/T 1060-2000	光波分复用系统（WDM）技术要求——32×2.5Gbit/s 部分
YD/T 1143-2001	光波分复用（WDM）技术要求——16×10Gb/s、32×10Gb/s 部分
YD/T 1205-2002	城市光传送网波分复用（WDM)环网技术要求
YD/T 1273-2003	光波分复用（WDM）终端设备技术要求——16×10Gb/s、32×10Gb/s 部分
YD/T 1274-2003	光波分复用系统（WDM）技术要求——160×10Gb/s、80×10Gb/s 部分
YD/T 1326-2004	粗波分复用（CWDM）系统技术要求
YD/T 1383-2005	波分复用(WDM)网元管理系统技术要求
YD/T 1350.1-2005	波分复用（WDM）系统网络管理接口技术要求 第一部分：接口功能部分
YD/T 1350.2-2005	波分复用（WDM）系统网络管理接口技术要求 第二部分：通用信息模型部分
YD/T 1350.3-2005	波分复用(WDM)系统网络管理接口技术要求 第三部分:基于GDMO/CMIP的信息模型部分
YD/T 746-95	点对多点微波通信系统技术要求和测量方法
YD/T 5017-2005	国内卫星通信地球站设备安装工程验收规范
YD/T 5050-2005	国内卫星通信地球站工程设计规范
YDN 120-1999	光波分复用系统总体技术要求（暂行规定）

3 术语和定义

下列术语和定义适用于本标准。

3.1

传送网安全等级 Security Classification of Transport Network

传送网安全重要程度的表征。重要程度可从传送网受到破坏后，对国家安全、社会秩序、经济运行、公共利益、网络和业务运营商造成的损害来衡量。

3.2

传送网安全等级保护 Classified Security Protection of Transport Network

对传送网分等级实施安全保护。

3.3

组织 Organization

组织是由传送网中不同作用的个体为实施共同的业务目标而建立的结构，组织的特性在于为完成目标而分工、合作；一个单位是一个组织，某个业务部门也可以是一个组织。

3.4

传送网安全风险 Security Risk of Transport Network

人为或自然的威胁可能利用传送网中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

3.5

传送网安全风险评估 Security Risk Assessment of Transport Network

指运用科学的方法和手段，系统地分析传送网所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和安全措施，防范和化解传送网安全风险，将风险控制在可接受的水平，为最大限度地保障传送网的安全提供科学依据。

3.6

传送网资产 Asset of Transport Network

传送网中具有价值的资源，是安全防护保护的对象。传送网中的资产可能是以多种形式存在，无形的、有形的、硬件、软件，包括物理布局、通信设备、物理线路、数据、软件、文档、规程、业务、人员、管理等各种类型的资源，如传送网节点设备、传送网的光缆线路、传送网的网络布局等。

3.7

传送网资产价值 Asset Value of Transport Network

传送网中资产的重要程度或敏感程度。资产价值是资产的属性，也是进行资产识别的主要内容。

3.8

传送网威胁 Threat to Transport Network

可能导致对传送网产生危害的不希望事件潜在起因，它可能是人为的，也可能是非人为的；可能是无意失误，也可能是恶意攻击。常见的传送网络威胁有光纤/缆中断、设备节点失效、火灾、水灾等。

3.9

传送网脆弱性 Vulnerability of Transport Network

脆弱性是传送网中存在的弱点、缺陷与不足，不直接对资产造成危害，但可能被威胁所利用从而危及资产的安全。

3.10

传送网灾难 Disaster of Transport Network

各种原因造成的传送网故障或瘫痪，使传送网支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

3.11

传送网灾难备份 Backup for Disaster Recovery of Transport Network

为了传送网灾难恢复而对相关网络要素进行备份的过程。

3.12

传送网灾难恢复 Disaster Recovery of Transport Network

为了将传送网从灾难造成的故障或瘫痪状态恢复到正常运行状态或部分正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

4 缩略语

下列缩略语适用于本标准。

ADM	Add and Drop Multiplexer	分插复用器
ASON	Automatic Switched Optical Network	自动交换光网络

CPU	Central Processing Unit	中央处理单元
E-NNI	External Network-Network Interface	外部网络—网络接口
MCN	Management Communication Network	管理通信网
MSP	Multiplex Section Protection	复用段保护
MS-SPRING	Multiplex Section Shared Proteciton Ring	复用段共享保护环
MSTP	Multi-Service Transport Platform	多业务传送平台
OADM	Optical Add and Drop Multiplexer	光分插复用器
OIF	Optical Internetworking Forum	光互联论坛
OSC	Optical Supervisory Channel	光监控通路
OSNR	Optical Signal to Noise Ratio	光信噪比
OTM	Optical Terminal Multiplexer	光终端复用器
OTN	Optical Transport Network	光传送网
PDH	Plesiochronous Digital Hierarchy	准同步数字体系
PTN	Packet Transport Network	分组传送网
SCN	Signalling Communication Network	信令通信网
SDH	Synchronous Digital Hierarchy	同步数字体系
SDXC	SDH Digital Cross Connect	SDH数字交叉连接
SNCP	SubNetwork Connection Protection	子网连接保护
TM	Terminal Multiplexer	终端复用器
UNI	User-Network Interface	用户—网络接口
WDM	Wavelength Division Multiplexing	波分复用

5 传送网安全防护概述

5.1 传送网安全防护范围

传送网可根据传输介质、载波频段、网络结构和地理覆盖范围等多种因素划分类型。按传送网所采用的传输介质和载频频段的不同，可分为光传送网、微波接力传送网和卫星传送网。按传送网的网络结构组成和地理覆盖范围的不同，光传送网可分为本地传送网（含城域传送网，包括核心层、汇聚层和接入层）、省内骨干传送网、省际骨干传送网和国际传送网；微波接力传送网包括省内传送网和省际传送网；卫星传送网可分为国内卫星传送网和国际卫星传送网。

传送网安全防护的范围包括光传送网、微波接力传送网和卫星传送网，相应的网络技术包括 PDH 光网络、SDH 光网络、MSTP 光网络、WDM 光网络、ASON 光网络、OTN 光网络、PTN 光网络、微波接力传送网络和卫星传送网络等。

5.2 传送网安全防护内容

根据电信网和互联网安全防护体系的要求，将传送网安全防护内容分为安全风险分析、安全等级保护、灾难备份及恢复等三个部分。

a）传送网安全等级保护：主要包括定级对象和安全等级的确定、网络安全、设备安全、物理环境安全和管理安全等。

b）传送网安全风险分析：主要包括资产识别、脆弱性识别、威胁识别、已有安全措施的确认、风险分析、风险评估文件记录等。本标准仅对传送网进行资产分析、脆弱性分析、威胁分析，在传送网安全风险评估过程中确定各个资产、脆弱性、威胁的具体值。资产、脆弱性、威胁的赋值方法及资产价值、风险值的计算方法参见YD/T 1730-2008《电信网和互联网安全风险评估实施指南》。

c）传送网灾难备份及恢复：主要包括灾难备份及恢复等级确定、针对灾难备份及恢复各资源要素的具体实施等。

6 传送网定级对象和安全等级确定

对光传送网进行安全等级定级时，定级对象应为本地传送网（含城域传送网，包括核心层、汇聚层和接入层）、省内骨干传送网、省际骨干传送网和国际传送网。

对微波接力传送网进行安全定级时，定级对象应为省内传送网、省际传送网。

对卫星传送网进行定级时，定级对象应为国内卫星传送网、国际卫星传送网。

网络和业务运营商应根据YD/T 1729-2008《电信网和互联网安全等级保护实施指南》附录A中确定网络安全等级的方法对传送网进行定级，即对传送网应根据社会影响力、所提供服务的重要性、规模和服务范围的大小分别定级，而定级方法中的权重因子 α、β、γ 可根据传送网具体情况进行调节，例如，对于承载党政专线业务的传送网，社会影响力和所提供服务的重要性的权重因子 α 和 β 值需适当增大一些，而规模和服务范围的权重因子 γ 值需适当减小一些。

7 传送网资产、脆弱性、威胁分析

7.1 资产分析

传送网资产应包括设备硬件、设备软件、重要数据、提供的服务、文档、人员、网络拓扑等，具体如表1所示。

表1 资产列表

分类	示 例
设备硬件	包括设备节点，如PDH节点、SDH节点、MSTP节点、ASON节点、WDM节点、OTN节点、微波中继设备、地球站、静止卫星、维护管理系统硬件；传送网信号传送的介质资源，如光缆/管道、波长、微波/卫星频率等；设备运行所需的物理环境硬件，如机房、电力供应系统、电磁防护系统、防火、防水、防潮系统、防静电系统、防雷击系统、温湿度控制系统等
设备软件	包括传送网设备涉及的系统软件（操作系统、各种数据库软件等）、系统控制软件、协议软件和操作维护系统软件等
重要数据	包括传送网网络配置数据、管理员操作维护记录、用户数据等
服务/业务	包括传送网专线业务、虚拟专网（VPN）业务等
文档	纸质以及保存在存储介质中的各种文件，如设计文档、技术要求、管理规定（机构设置、管理制度、人员管理办法）、工作计划、技术或财务报告、用户手册等
人员	掌握重要技术的人员，如网络维护人员、设备维护人员、网络或业务的研发人员等
网络拓扑	包括传送网节点之间点到点连接、环型连接和网状连接等

7.2 脆弱性分析

传送网存在的脆弱性可分为技术脆弱性（含网络类脆弱性、设备类脆弱性、物理环境类脆弱性）和管理类脆弱性等。脆弱性的识别对象应以资产为中心。表2给出了部分脆弱性识别内容。

表 2 脆弱性分析表

类 型	对 象	存在的脆弱性
技术脆弱性	网络	包括光缆备用纤芯不足、绘制网络拓扑与现网不一致、光缆物理路由维度太少、光缆超过设计使用年限、数据通信网（DCN）无保护路由、不支持多点同时故障的保护等
	设备（含操作系统和数据库）	包括设备重要部件未配置主备用保护、业务板卡无备件、设备接口指标不满足规范要求、设备超过设计使用年限、网管服务器没有采用主备、网管系统没有与外部网络隔离、网管系统的杀毒工具版本未升级、重要数据未定时备份、登录用户未实现等级管理等
	物理环境	包括机房选址不合理、电缆/光缆敷设不符合规范、物理访问控制管理松懈、防盗窃和防破坏措施简单、防雷击不符合规范、防火/防水/防潮不符合规范、防静电不符合规范、温湿度控制不符合规范、电力供应不符合规范、电磁防护不符合规范等
管理脆弱性		• 安全管理机构方面：岗位设置不合理（如人员配置过少、职责不清）、授权和审批程序简化、沟通和合作未执行、审核和检查未执行等。 • 安全管理制度方面：管理制度不完善、制度评审和修订不及时等。 • 人员安全管理方面：人员录用不符合程序、人员离岗未办理安全手续、人员未进行安全培训、对于第三方人员未进行限制访问等。 • 建设管理方面：安全方案不完善、软件开发不符合程序、工程实施未进行安全验收或验收不严格等。 • 运维管理方面：物理环境管理措施简单、存储介质使用不受限、设备没有定期维护、厂家支持力度不够、关键性能指标没有定期监控、无恶意代码防范措施、无数据备份和恢复策略、访问控制不严格、操作管理不规范等，应急保障措施不到位，灾难恢复预案不完善

7.3 威胁分析

对于传送网可能存在的威胁，根据来源可分为技术威胁、环境威胁和人为威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。表 3 列举出部分威胁。

表 3 威胁来源列表

来 源		威胁描述
技术威胁		包括光缆/管道中断、板卡失效、微波或卫星设备故障、网管瘫痪、ASON 控制平面故障、网络节点失效、病毒入侵、微波或卫星设备频率干扰和攻击等
环境威胁	物理环境	包括断电、静电、灰尘、潮湿、温度、电磁干扰等，意外事故或通信线路方面的故障等
	自然灾害	包括雷击、地震、洪灾、滑坡、飓风、火灾、泥石流、山体滑坡、鼠蚁虫害等
人为威胁	恶意人员	• 不满的或有预谋的内部人员滥用权限进行恶意破坏； • 采用自主或内外勾结的方式盗窃或篡改机密信息； • 外部人员利用网络进行攻击、入侵、植入病毒； • 外部人员进行物理破坏、盗窃等
	无恶意人员	• 内部人员由于缺乏责任心或者无作为而应该执行却没有执行相应的操作、或无意地执行了错误的操作导致安全事件； • 内部人员没有遵循规章制度和操作流程而导致故障或信息损坏； • 内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致故障或攻击； • 安全管理制度不完善、落实不到位造成安全管理不规范或者管理混乱导致安全事件
其他威胁		如战争等

8 传送网安全等级保护要求

8.1 第1级要求

不作要求。

8.2 第2级要求

8.2.1 网络安全要求

8.2.1.1 PDH光网络

8.2.1.1.1 网络拓扑安全

a） 传送网络拓扑设计合理；

b） 光缆/管道使用年限一般不应超过设计要求，超过设计年限要求的光缆/管道应加强在线监测，定期记录光缆/管道使用状态；

c） 应绘制与当前运行情况相符合的网络拓扑图。

8.2.1.2 SDH光网络

8.2.1.2.1 网络拓扑安全

a） 传送网络拓扑设计合理，网络拓扑以环网为主；

b） 光缆/管道使用年限一般不应超过设计要求，超过设计年限要求的光缆/管道应加强在线监测，定期记录光缆/管道使用状态；

c） 应绘制与当前运行情况相符合的网络拓扑图。

8.2.1.2.2 网络保护与恢复能力

a） 应能根据业务需求提供相应的网络保护能力，如支持复用段共享保护环（MS-SPRING）、复用段保护（MSP）和子网连接保护（SNCP）等保护方式中的一种或几种；

b） 网络保护倒换时间应小于50ms（大于1200km的环网根据实际传输距离情况考虑）；

c） 网络保护倒换机制应满足插入告警、插入越限误码、拔纤和网管人工/强制倒换等要求；

d） 工作路径与保护路径的网络抖动、色散容限、光信噪比（OSNR）等均满足设计要求。

8.2.1.2.3 MCN安全

a） MCN应保证用户在未经许可的情况下无法获取网管和网元中的信息；

b） MCN应保证通信和存储的数据的私密性；

c） MCN应保证通信和存储的数据的完整性；

d） MCN应对安全相关的行为进行记录，对非法的动作提供告警；

e） MCN中的网元应该提供关闭组网中未用的通信通道的功能，以避免不安全的接入；

f） 当发生单个故障时，MCN仍然能保证重要管理消息的传送；

g） 当MCN发生网络拥塞时，MCN应保证用于纠正失效或网络故障的管理消息不会被阻塞或过度延迟。

8.2.1.3 MSTP光网络

与8.2.1.2的要求相同。

8.2.1.4 WDM光网络

8.2.1.4.1 网络拓扑安全

a） 传送网络拓扑设计合理，网络拓扑以线性和环网为主；

b） 光缆/管道使用年限一般不应超过设计要求，超过设计年限要求的光缆/管道应加强在线监测，定期记录光缆/管道使用状态；

c） 应绘制与当前运行情况相符合的网络拓扑图。

8.2.1.4.2 网络保护恢复能力

a） 应根据业务需求提供相应的网络保护能力，如支持光复用段共享保护、光复用段线性保护和光通道保护等保护方式；

b） 网络保护倒换时间应小于50ms；

c） 网络保护倒换机制应满足插入告警、插入越限误码、拔纤和网管人工/强制倒换等要求；

d） 工作路径与保护路径的网络抖动、色散容限、光信噪比（OSNR）等均满足设计要求。

8.2.1.4.3 MCN 安全

a） 光监控通路（OSC）不限制光放大器的泵浦波长；

b） OSC在线路光纤放大器失效时仍然可以使用；

c） OSC的传输应该是分段的并且具有3R功能和双向传输功能，在每个光纤放大器中继站上，信息能被正确地接收下来，而且还可附加上新的信息；

d） OSC应具有自我管理能力，光监控通路信号丢失时有告警指示，其完全独立于其他工作通道的状况。

8.2.1.5 ASON 光网络

8.2.1.5.1 网络拓扑安全

a） 传送网络拓扑设计合理，网络拓扑以环网和网状网为主；

b） 光缆/管道使用年限一般不应超过设计要求，超过设计年限要求的光缆/管道应加强在线监测，定期记录光缆/管道使用状态；

c） 应绘制与当前运行情况相符合的网络拓扑图。

8.2.1.5.2 网络保护与恢复能力

a） 应根据业务需求提供相应的网络保护能力，如支持基于传送平面的 MS-SPRING、MSP 和 SNCP 等保护方式，以及基于控制平面的 1＋1、*M*:*N* 等区段/路径保护方式；

b） 应根据业务需求提供相应的网络恢复以及保护与恢复结合能力，如恢复、基于传送平面的保护与恢复结合（如 MS-SPRING＋恢复、MSP＋恢复、SNCP＋恢复等）和基于控制平面的保护与恢复结合（如区段/路径 1＋1＋恢复、区段/路径 *M*:*N*＋恢复）等；

c） 网络保护倒换时间应小于 50ms（大于 1200km 的环网根据实际传输距离情况考虑），网络恢复时间具体指标值待定；

d） 网络保护倒换机制应满足插入告警、插入越限误码、拔纤和网管人工/强制倒换等要求；

e） 工作路径与保护路径的网络抖动、色散容限、光信噪比（OSNR）等均满足设计要求。

8.2.1.5.3 MCN 安全

与8.2.1.2.3的要求相同。

8.2.1.5.4 SCN 安全

a） SCN 应保证恢复消息的可靠和快速传送；

b） SCN 应防止未经授权的用户接入；

c） 在管理域边界，只允许管理域之间满足要求的消息通过域间接口，不满足要求的消息禁止通过域间接口。

8.2.1.5.5 传送平面安全

a） 应避免传输链路的误连接以确保用户的数据不被传到错误的接收方；

b） 传送平面应能产生告警并向管理平面通告安全相关事件。

8.2.1.5.6 控制平面安全

a） 应支持 OIF 定义的“UNI 和 NNI 安全扩展”；

b） 应能够拒绝所有未认证的接入；

c） 敏感的网络信息不能经过外部接口（UNI 或 E-NNI），经过 E-NNI 的信息需要根据设置的策略受到控制和限制，只有在经过认证的实体间才可以进行信息交换；

d） 在 UNI 和 E-NNI 交互信令、路由和发现等消息时，应支持消息的认证、完整性、机密性等安全机制；

e） 允许用户选择其他方法进行保护，比如区域接入控制和防火墙，所选用的机制应不存在已知缺点或严重缺陷；

f） 应保证不同厂家安全机制之间的互通性；

g） 控制平面应保证 NNI 之间安全地交换路由信息。

8.2.1.5.7 管理平面安全

a） 能够划分不同权限的用户等级，禁止低权限用户使用高权限的管理操作功能；

b） 建立登录日志和操作日志并对其进行定期管理；

c） 网管系统应具备安全保护措施，防止外部侵入和病毒破坏；

d） 与传送平面/控制平面的通信中断时，系统应在一定时间内自动尝试重建连接，通信恢复后，应支持自动和手工方式实现网管数据的同步和更新；

e） 用户界面程序异常停止后，不应影响服务器端和其他用户界面的正常运行；

f） 管理平面故障不应影响控制平面和传送平面的正常工作。

8.2.1.6 OTN 光网络

待研究。

8.2.1.7 PTN 光网络

待研究。

8.2.1.8 微波接力传送网络

8.2.1.8.1 网络拓扑安全

微波接力传送网络拓扑设计合理，应绘制与当前运行情况相符合的网络拓扑图。

8.2.1.8.2 网络保护与恢复能力

a） 应提供工作波道的备用波道，支持备用波道的倒换机制；

b） 应支持公务波道的1+1备份。

8.2.1.8.3 MCN 安全

与8.2.1.2.3的要求相同。

8.2.1.9 卫星传送网络

8.2.1.9.1 网络拓扑安全

a） 卫星传送网络拓扑设计合理，星状网和网状网相结合。

b） 应绘制与当前运行情况相符合的网络拓扑图。

8.2.1.9.2 MCN 安全

与8.2.1.2.3的要求相同。

8.2.2 传送网设备安全要求

8.2.2.1 传送网设备分类

按照传送网技术构成，传送网设备可分为PDH、SDH、MSTP、WDM、ASON、OTN、PTN、微波接力设备和卫星通信设备等设备。

8.2.2.2 PDH 设备

PDH 设备应满足 YD 5014-1995、YD/T 1016-1999 和 GB 7611-2001 等规定的要求。

8.2.2.3 SDH 设备

SDH 设备应满足 YD/T 1022-1999、YD/T 1017-1999、YD/T 1289.1-2003、YD/T 1289.2-2003、YD/T 1289.3-2003、YD/T 1289.4-2006、YD/T 900-1997、YD/T 974-1998、YD/T 1167-2001、YD/T 882-1996、GB/T 16712-1996、GB/T 20185-2006、YD/T 1420-2005 和 GB 7611-2001 等规定的要求。

8.2.2.4 MSTP 设备

MSTP 设备应满足 YD/T 1238-2002、YD/T 1345-2005、YD/T 1474-2006 等规定的要求。

8.2.2.5 WDM 设备

WDM 设备应满足 YDN 120-1999、YD/T 1060-2000、YD/T 1143-2001、YD/T 1205-2002、YD/T 1273-2003、YD/T 1274-2003、YD/T 1326-2004、YD/T 1383-2005、YD/T 1350.1-2005、YD/T 1350.2-2005 和 YD/T 1350.3-2005 等规定的要求。

8.2.2.6 ASON 设备

ASON 设备应符合企业相关规范的要求。

8.2.2.7 OTN 设备

待研究。

8.2.2.8 PTN 设备

待研究。

8.2.2.9 微波接力设备

微波接力设备应满足 GB/T 13159-91、GB/T 15841-1995 和 YD/T 746-95 等规定的要求。

8.2.2.10 卫星通信设备

卫星地球站设备应满足YD/T 5017-2005和YD/T 5050-2005等规定的要求。

8.2.3 传送网物理环境安全要求

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中第2级的安全要求。

8.2.4 传送网管理安全要求

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第2级的安全要求。

8.3 第 3.1 级要求

8.3.1 网络安全要求

8.3.1.1 PDH 光网络

8.3.1.1.1 网络拓扑安全

除了满足8.2.1.1.1的要求之外，还应满足：光缆/管道使用合理，应预留备用纤芯/备用光缆。

8.3.1.2 SDH 光网络

8.3.1.2.1 网络拓扑安全

除了满足8.2.1.2.1的要求之外，还应满足：

a） 光缆/管道使用合理，应预留同物理路由和异物理路由备用纤芯/备用光缆；

b） 应预留一定比例的冗余通道和维护通道。

8.3.1.2.2 网络保护与恢复能力

除了满足8.2.1.2.2的要求之外，还应满足：工作路径与保护路径原则上应选择不同的路由。

8.3.1.2.3 MCN 安全

除了满足8.2.1.2.3的要求之外，还应满足：

a） MCN应该支持冗余路由；

b） MCN应提供紧急功能的网管系统和网元需要多条通道接入MCN。

8.3.1.3 MSTP 光网络

具体要求同8.3.1.2。

8.3.1.4 WDM 光网络

8.3.1.4.1 网络拓扑安全

除了满足8.2.1.4.1的要求之外，还应满足：

a） 光缆/管道使用合理，应预留同物理路由和异物理路由备用纤芯/备用光缆；

b） 应预留一定比例的冗余波道和维护波道。

8.3.1.4.2 网络保护恢复能力

除了满足8.2.1.4.2的要求之外，还应满足：工作路径与保护路径应选择不同的路由。

8.3.1.4.3 MCN 安全

与8.2.1.4.3的要求相同。

8.3.1.5 ASON 光网络

8.3.1.5.1 网络拓扑安全

除了满足8.2.1.5.1的要求之外，还应满足：

a） 网络节点之间应支持 2 条以上不同物理路由；

b） 光缆/管道使用合理，应预留同物理路由和异物理路由备用纤芯/备用光缆；

c） 应预留一定的冗余通道和维护通道。

8.3.1.5.2 网络保护与恢复能力

除了满足8.2.1.5.2的要求之外，还应满足：工作路径与保护路径应选择不同的路由。

8.3.1.5.3 MCN 安全

与8.2.1.5.3的要求相同。

8.3.1.5.4 SCN 安全

除了满足8.2.1.5.4的要求之外，还应满足：

a） SCN 应该冗余路由；

b） SCN 自身应能提供保护和恢复机制，如 1＋1 保护和重路由方式等。

8.3.1.5.5 传送平面安全

与 8.2.1.5.5 的要求相同。

8.3.1.5.6 控制平面安全

除了满足8.2.1.5.6要求之外，还应满足：

a） 控制平面应能够产生告警并向管理平面通告安全相关事件，并在管理平面上建立安全日志。管理平面应能够分析和使用日志中的数据以判断是否威胁到控制平面的安全；

b） 控制平面应能够从侵入攻击中恢复。

8.3.1.5.7 管理平面安全

除了满足8.2.1.5.7的要求之外，还应满足：

a） 网管系统应支持（1+1）热备用（Hot-Standby）或温备用（Warm-Standby）配置。在热备用方式下，主用到备用的切换应为实时切换；在温备用方式下，主用到备用的平均切换时间应小于20min。

b） 应支持对网管数据的备份，包括人工备份和自动定期备份。

8.3.1.6 OTN 光网络

待研究。

8.3.1.7 PTN 光网络

待研究。

8.3.1.8 微波接力传送网络

与8.2.1.8的要求相同。

8.3.1.9 卫星传送网络

8.3.1.9.1 网络拓扑安全

除了满足8.2.1.9.1的要求之外，还应满足支持地球站之间互为备用。

8.3.1.9.2 MCN 安全

与8.2.1.9.2的要求相同。

8.3.2 传送网设备安全要求

8.3.2.1 PDH 设备

与 8.2.2.2 的要求相同。

8.3.2.2 SDH 设备

与 8.2.2.3 的要求相同。

8.3.2.3 MSTP 设备

与 8.2.2.4 的要求相同。

8.3.2.4 WDM 设备

与 8.2.2.5 的要求相同。

8.3.2.5 ASON 设备

与 8.2.2.6 的要求相同。

8.3.2.6 OTN 设备

待研究。

8.3.2.7 PTN 设备

待研究。

8.3.2.8 微波接力设备

与 8.2.2.9 的要求相同。

8.3.2.9 卫星通信设备

与 8.2.2.10 的要求相同。

8.3.3 传送网物理环境安全要求

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中第3.1级的安全要求。

8.3.4 传送网管理安全要求

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第3.1级的安全要求。

8.4 第 3.2 级要求

8.4.1 网络安全要求

8.4.1.1 PDH 光网络

与8.3.1.1的要求相同。

8.4.1.2 SDH 光网络

8.4.1.2.1 网络拓扑安全

除了满足8.3.1.2.1的要求之外，还应满足：

a） 传送网络拓扑设计合理，不同传输节点机楼之间光缆/管道应支持多方向物理路由；

b） 传送网应支持双传送平面以实现业务负荷分担，提高安全性；

c） 不同传送网层面之间的互连采用双节点分离设备互联。

8.4.1.2.2 网络保护与恢复能力

除了满足8.3.1.2.2的要求之外，还应满足：工作路径与保护路径应选择不同的物理路由。

8.4.1.2.3 MCN 安全

与8.3.1.2.3的要求相同。

8.4.1.3 MSTP 光网络

与8.3.1.3的要求相同。

8.4.1.4 WDM 光网络

8.4.1.4.1 网络拓扑安全

除了满足8.3.1.4.1的要求之外，还应满足：

a） 传送网络拓扑设计合理，不同传输节点机楼之间光缆/管道应支持多方向物理路由；

b） 传送网应支持双传送平面以实现业务负荷分担，提高安全性。

8.4.1.4.2 网络保护与恢复能力

与 8.3.1.4.2 的要求相同。

8.4.1.4.3 MCN 安全

与 8.3.1.4.3 的要求相同。

8.4.1.5 ASON 光网络

8.4.1.5.1 网络拓扑安全

与8.3.1.5.1的要求相同。

8.4.1.5.2 网络保护与恢复能力

除了满足8.3.1.5.2的要求之外，还应满足：工作路径与保护恢复路径应选择不同的物理路由。

8.4.1.5.3 MCN 安全

与8.3.1.5.3的要求相同。

8.4.1.5.4 SCN 安全

与8.3.1.5.4的要求相同。

8.4.1.5.5 传送平面安全

与8.3.1.5.5的要求相同。

8.4.1.5.6 控制平面安全

与8.3.1.5.6的要求相同。

8.4.1.5.7 管理平面安全。

8.4.1.6 OTN 光网络

待研究。

8.4.1.7 PTN 光网络

待研究。

8.4.1.8 微波接力传送网络

与8.3.1.8的要求相同。

8.4.1.9 卫星传送网络

与8.3.1.9的要求相同。

8.4.2 传送网设备安全要求

与8.3.2的要求相同。

8.4.3 传送网物理环境安全要求

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中第3.2级的安全要求

8.4.4 传送网管理安全要求

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第3.2级的安全要求。

8.5 第 4 级要求

8.5.1 网络安全要求

8.5.1.1 PDH 光网络

与8.4.1.1的要求相同。

8.5.1.2 SDH 光网络

与8.4.1.2的要求相同。

8.5.1.3 MSTP 光网络

与8.4.1.3的要求相同。

8.5.1.4 WDM 光网络

与8.4.1.4的要求相同。

8.5.1.5 ASON 光网络

与8.4.1.5的要求相同。

8.5.1.6 OTN 光网络

待研究。

8.5.1.7 PTN 光网络

待研究。

8.5.2 传送网设备安全要求

与8.4.2的要求相同。

8.5.3 传送网物理环境安全要求

除了满足8.4.3的要求之外，还应满足：

a） 应对重要区域配置第二道电子门禁系统，控制、鉴别和记录进入的人员身份并监控其活动；

b） 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警；

c） 应采用静电消除器等装置，减少静电的产生；

d） 对机房实施电磁屏蔽。

8.5.4 传送网管理安全要求

除了满足8.4.4的要求之外，还应满足：

a） 对关键区域不允许第三方人员访问；

b） 应对机房和办公环境实行统一策略的安全管理，出入人员应经过相应级别授权，对进入重要安全区域的活动行为应实时监视和记录；

c） 应根据信息分类与标识的原则和方法，在信息的存储、传输等过程中对信息进行标识；

d） 应严格控制网络管理用户的授权，授权程序中要求必须有两人在场，并经双重认可后方可操作，操作过程应当有不可更改的审计日志；

e） 应定期检查变更控制的申报和审批程序的执行情况，评估系统现有状况与文档记录的一致性；

f） 对需要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场并登记备案；

g） 可能涉及国家秘密的重大失、泄密事件应按照有关规定向公安、安全、保密等部门汇报；

h） 严格控制参与涉密事件处理和恢复的人员，重要操作要求至少两名工作人员在场并登记备案。

8.6 第 5 级要求

待补充。

9 传送网灾难备份及恢复要求

9.1 灾难备份及恢复等级

根据 YD/T 1731-2008《电信网和互联网灾难备份及恢复实施指南》5.1 节，灾难备份及恢复定级应与安全等级保护确定的安全等级一致。

9.2 第 1 级要求

不作要求。

9.3 第 2 级要求

9.3.1 冗余系统、冗余设备及冗余链路要求

a） 单节点的灾难不应导致其他节点的业务提供发生异常，单一地区范围的灾难不应导致其他地区的业务提供发生异常；

b） 网络灾难恢复的恢复时间应满足行业管理、网络和业务运营商应急预案的相关要求。

9.3.2 冗余路由要求

传送网应支持带宽负荷传送分担设计。

9.3.3 备份数据要求

a） 关键数据（如传送网网络配置数据、性能数据、告警数据和安全访问数据等）应有本地数据备份；

b） 数据备份范围和时间间隔、采取的备份方式、数据恢复能力应符合相关要求。

9.3.4 人员和技术支持能力要求

a） 应有负责机房运行管理人员；

b） 应有负责数据备份技术支持人员；

c） 应有负责操作系统、数据库、网管系统和设备软件技术支持人员；

d） 应有负责传送设备硬件技术和网络技术支持人员等；

e） 相关技术支持人员应有定期的关于灾难备份及恢复的技术培训。

9.3.5 运行维护管理能力要求

a） 传送网应有机房运行管理制度；

b） 传送网应有介质存取、验证和转储管理制度，确保备份数据授权访问；

c） 传送网应按介质特性对备份数据进行定期的有效性验证；

d） 传送网应有传送网设备和网络运行管理制度；

e） 传送网应有数据异地实时容灾备份管理制度；

f） 传送网应有与外部组织保持良好的联络和协作能力。

9.3.6 灾难恢复预案要求

a） 应有完整的灾难恢复预案；

b） 应有灾难恢复预案的教育和培训，相关人员应了解灾难恢复预案并具有对灾难恢复预案进行实际操作的能力；

c） 应有灾难恢复预案的演练，并根据演练结果对灾难恢复预案进行修正。

9.4 第3.1级要求

9.4.1 冗余系统、冗余设备及冗余链路要求

除了满足9.3.1的要求之外，还应满足：传送网应支持采用异地/同地的冗余链路、冗余管理系统和冗余节点来提供保护等。

9.4.2 冗余路由要求

与9.3.2的要求相同。

9.4.3 备份数据要求

与9.3.3的要求相同。

9.4.4 人员和技术支持能力要求

与9.3.4的要求相同。

9.4.5 运行维护管理能力要求

与 9.3.5 的要求相同。

9.4.6 灾难恢复预案要求

与 9.3.6 的要求相同。

9.5 第 3.2 级要求

9.5.1 冗余系统、冗余设备及冗余链路要求

除了满足9.4.1的要求之外，还应满足：不同的传送网（光传送网、微波接力传送网、卫星传送网）可互为冗余网络。

9.5.2 冗余路由要求

除了满足9.4.2的要求之外，还应满足：物理光缆路由应支持冗余方式。

9.5.3 备份数据要求

除了满足9.4.3的要求之外，还应满足：关键数据（如传送网网络配置数据、性能数据、告警数据和安全访问数据等）应有异地数据备份；

9.5.4 人员和技术支持能力要求

与9.4.4的要求相同。

9.5.5 运行维护管理能力要求

除了满足9.4.5的要求之外，还应满足：传送网应有操作系统、数据库、网管系统和设备软件运行管理制度。

9.5.6 灾难恢复预案要求

除了满足9.4.6的要求之外，还应满足：应有完善的灾难恢复预案管理制度。

9.6 第 4 级要求

9.6.1 冗余系统、冗余设备及冗余链路要求

除了满足9.5.1的要求之外，还应满足：光传送网可尽量采用多个不同光缆物理路由（如陆缆和海缆等）的网络互为冗余。

9.6.2 冗余路由要求

与9.5.2的要求相同。

9.6.3 备份数据要求

与9.5.3的要求相同。

9.6.4 人员和技术支持能力要求

与9.5.4的要求相同。

9.6.5 运行维护管理能力要求

与9.5.5的要求相同

9.6.6 灾难恢复预案要求

与9.5.6的要求相同

9.7 第 5 级要求

待补充。