YD

中华人民共和国通信行业标准

YD/T 1745-2008

传送网安全防护检测要求

Security Protection Testing 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……II
1　范围……1
2　规范性引用文件……1
3　术语和定义……1
4　缩略语……3
5　传送网安全防护检测概述……3
5.1　安全防护检测范围……3
5.2　安全防护检测对象……4
5.3　安全防护检测内容……4
5.4　安全防护检测结果判定……4
6　传送网安全等级保护检测要求……5
6.1　第1级要求……5
6.2　第2级要求……5
6.3　第3.1级要求……11
6.4　第3.2级要求……15
6.5　第4级要求……17
6.6　第5级要求……19
7　传送网安全风险评估检测要求……19
7.1　安全风险评估范围……19
7.2　安全风险评估内容……19
7.3　安全风险评估要素……20
7.4　安全风险评估赋值原则……21
7.5　安全风险评估计算方法……21
7.6　安全风险评估文件类型……21
7.7　安全风险评估文件记录……22
8　传送网灾难备份及恢复检测要求……23
8.1　第1级要求……23
8.2　第2级要求……23
8.3　第3.1级要求……25
8.4　第3.2级要求……25
8.5　第4级要求……27
8.6　第5级要求……27

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 1744-2008《传送网安全防护要求》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

传送网安全防护检测要求

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检测要求。

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。

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/T1731-2008 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检测要求

YD/T 1756-2008 电信网和互联网管理安全等级保护检测要求

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。

3.13

访谈 Interview

检测人员通过与传送网有关人员（个人/群体）进行交流、讨论等活动，检查传送网安全等级保护、传送网安全风险评估和传送网灾难备份及恢复相关措施的落实情况以及相关工作的开展情况的一种方法。

3.14

检查 Examination

检测人员通过对检测对象进行观察、查验和分析等活动，检查传送网安全等级保护、传送网安全风险评估和传送网灾难备份及恢复相关措施的落实情况以及相关工作的开展情况的一种方法。

3.15

测试 Testing

检测人员通过对检测对象按照预定的方法/工具使其产生特定行为的活动，查看、分析输出结果，检查传送网安全等级保护、传送网安全风险评估和传送网灾难备份及恢复相关措施的落实情况以及相关工作的开展情况的一种方法。

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
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 传送网安全防护检测概述

5.1 安全防护检测范围

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。其中光传送网包括本地传送网（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；卫星传送网包括国内卫星传送网、国际卫星传送网。相

应的传送网组网技术包括 PDH、SDH、MSTP、WDM、ASON、OTN、PTN、微波接力和卫星传送等。

5.2 安全防护检测对象

对光传送网进行安全防护检测时，检测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防护检测时，检测对象应为省内传送网、省际传送网。

对卫星传送网进行安全防护检测时，检测对象应为国内卫星传送网、国际卫星传送网。

安全等级保护的检测对象确定后，安全风险评估的检测对象、灾难备份及恢复的检测对象应与安全等级保护的检测对象相一致。

5.3 安全防护检测内容

按照传送网安全防护检测的需要，将传送网安全防护检测分为传送网安全等级保护检测、传送网安全风险评估检测和传送网灾难备份及恢复检测三个部分。

传送网安全防护检测要求包括以下内容。

a）传送网安全等级保护检测：主要包括网络安全检测、设备安全检测、物理环境安全检测、管理安全检测等。

b）传送网安全风险评估检测：主要包括安全风险评估范围检测、安全风险评估内容检测、安全风险评估要素检测、安全风险评估赋值原则检测、安全风险评估计算方法检测、安全风险评估文件类型检测和安全风险评估文件记录检测等。

c）传送网灾难备份及恢复检测：主要包括冗余系统、冗余设备及冗余链路检测、冗余路由检测、备份数据检测、人员和技术支持能力检测、运行维护管理能力检测和灾难恢复预案检测等。

5.4 安全防护检测结果判定

传送网安全防护检测包括对传送网的安全等级保护、安全风险评估、灾难备份及恢复三个部分的检测，应对三个部分的检测结果分别进行判定，并根据检测结果分别出具检测报告，检测报告中应具体说明安全防护工作的优势和不足。

对每一个部分中的每一个评测项，应根据具体实施情况进行等级化评价（分5级：很好、较好、一般、较差、很差）。参照表1将各评测项的评价等级换算成评分，各评测项的分数经过一定的算法（例如加权平均）分别得到安全等级保护、安全风险评估、灾难备份及恢复三个部分的总分数，根据总分数分别对安全等级保护、安全风险评估、灾难备份及恢复三个部分的评测结果进行等级化评定，总分数和评定等级的关系如表2所示。在计算总分数过程中，应充分考虑到各评测项在安全防护检测要求中所占的比重，例如，表3给出了安全等级保护子类所占的比重。固定通信网安全防护检测的结果还应充分考虑到支持固定通信网运行的各相关系统的检测结果。

表1 评测项评分方法

评价结果	评 分
实施很好	5
实施较好	4
实施一般	3
实施较差	2
实施很差	1

表2 总分数和评定等级的关系

总分数 x	评定等级
$4.5 \leqslant x \leqslant 5$	很好
$3.5 \leqslant x < 4.5$	较好
$2.5 \leqslant x < 3.5$	一般
$1.5 \leqslant x < 2.5$	较差
$x < 1.5$	很差

表3 安全等级保护子类所占的比重

比重（%）	安全等级保护子类
30	网络安全
20	设备安全
10	物理环境安全
40	管理安全

6 传送网安全等级保护检测要求

6.1 第1级要求

不作要求。

6.2 第2级要求

6.2.1 传送网网络安全

6.2.1.1 PDH光网络安全

6.2.1.1.1 网络拓扑安全

6.2.1.1.1.1 检测方式

访谈，检查。

6.2.1.1.1.2 检测对象

传送网络管理员，网络拓扑图，入网检测报告，故障记录，网络设计/验收文档。

6.2.1.1.1.3 检测实施

a）应访谈传送网管理人员，了解目前传送网的网络组织情况；

b）应检查网络拓扑图，查看其与当前运行情况是否一致；

c）应检查光缆/管道的使用年限，查看其是否超过设计使用年限，对于超过设计年限要求的光缆/管道应检查是否具有在线监测措施，是否定期记录光缆/管道使用状态。

6.2.1.2 SDH光网络安全

6.2.1.2.1 网络拓扑安全

6.2.1.2.1.1 检测方式

访谈，检查。

6.2.1.2.1.2 检测对象

传送网络管理员，网络拓扑，网络拓扑图，网络设计/验收文档。

6.2.1.2.1.3 检测实施

a）应访谈传送网管理人员，了解目前传送网的网络组织情况；

b）应检查网络拓扑图，查看其与当前运行情况是否一致，是否以环型为主；

c）应检查光缆/管道的使用年限，查看其是否超过设计使用年限，对于超过设计年限要求的光缆/管道应检查是否具有在线监测措施，是否定期记录光缆/管道使用状态。

6.2.1.2.2 网络保护与恢复能力

6.2.1.2.2.1 检测方式

访谈，检查。

6.2.1.2.2.2 检测对象

传送网网络管理员，网络设计/验收文档，历史记录，网络管理系统。

6.2.1.2.2.3 检测实施

a）应访谈网络管理员，并检查传送网设计文件，了解目前传送网的网络保护与恢复情况；

b）应检查网络设计文件和验收文件、演练记录、历史记录和基本处理预案，查看传送网是否根据业务需求提供相应的网络保护能力，如提供复用段共享保护环（MS-SPRING）、复用段保护（MSP）和子网连接保护（SNCP）等保护方式；

c）应检查传送网验收文件和历史记录，查看保护倒换时间是否满足小于50ms（大于1200km的环根据实际传输距离考虑）要求，同时查看业务的恢复时间范围；

d）应检查网络设计文件和验收文件、历史记录中的工作路径与保护路径的网络抖动、色散容限、光信噪比（OSNR）等参数，查看其是否设计要求。

6.2.1.2.3 MCN安全

6.2.1.2.3.1 检测方式

访谈，检查。

6.2.1.2.3.2 检测对象

网络管理员，网络设计/验收文档、历史记录。

6.2.1.2.3.3 检测实施

a）应检查网络设计/验收文档和历史记录，MCN是否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）应检查网络设计/验收文档和历史记录，MCN是否保证通信和存储的数据的私密性；

c）应检查网络设计/验收文档和历史记录，MCN是否保证通信和存储的数据的完整性；

d）应检查网络设计/验收文档和历史记录，MCN是否对安全相关的行为进行记录，对非法的动作提供告警；

e）应检查网络设计/验收文档和历史记录，MCN的网元是否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）应检查网络设计/验收文档和历史记录，查看当发生单个故障时，MCN的设计是否仍然能保证重要管理消息的传送；

g）应检查网络设计/验收文档和历史记录，当MCN发生网络拥塞时，MCN的设计是否能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。

6.2.1.3 MSTP光网络安全

6.2.1.3.1 网络拓扑安全

具体要求同6.3.1.2.1。

6.2.1.3.2 网络保护与恢复能力

具体要求同6.3.1.2.2。

6.2.1.3.3 MCN 安全

具体要求同6.3.1.2.3。

6.2.1.4 WDM 光网络安全

6.2.1.4.1 网络拓扑安全

6.2.1.4.1.1 检测方式

访谈，检查。

6.2.1.4.1.2 检测对象

传送网络管理员，网络拓扑，网络拓扑图，网络设计/验收文档。

6.2.1.4.1.3 检测实施

a）应访谈传送网管理人员，了解目前传送网的网络组织情况；

b）应检查网络拓扑图，查看其与当前运行情况是否一致，是否以线型和环型为主；

c）应检查光缆/管道的使用年限，查看其是否超过设计使用年限，对于超过设计年限要求的光缆/管道应检查是否具有在线监测措施，是否定期记录光缆/管道使用状态。

6.2.1.4.2 网络保护与恢复能力

6.2.1.4.2.1 检测方式

访谈，检查。

6.2.1.4.2.2 检测对象

传送网网络管理员，网络设计/验收文档，历史记录，网络管理系统。

6.2.1.4.2.3 检测实施

a）应访谈网络管理员，并检查传送网设计文件，了解目前传送网的网络保护与恢复情况；

b）应检查网络设计文件和验收文件、演练记录、历史记录和基本处理预案，查看传送网是否根据业务需求提供相应的网络保护能力，如提供光复用段共享保护、光复用段线性保护和光通道保护等保护方式；

c）应检查传送网验收文件和历史记录，查看保护倒换时间是否满足小于 50ms；

d）应检查网络设计文件和验收文件、历史记录中的工作路径与保护路径的网络抖动、色散容限、光信噪比（OSNR）等参数，查看其是否设计要求。

6.2.1.4.3 MCN 安全

6.2.1.4.3.1 检测方式

访谈，检查。

6.2.1.4.3.2 检测对象

传送网网络管理员，网络设计/验收文档，历史记录，网络管理系统。

6.2.1.4.3.3 检测实施

a）应访谈网络管理员，并检查传送网设计文件，了解目前传送网的 OSC 配置情况；

b）应检查网络设计文件和验收文件，查看 OSC 是否限制了光放大器的泵浦波长；

c）应检查网络设计文件/验收文件和历史记录，查看 OSC 在线路光纤放大器失效时仍然可以使用；

d）应检查网络设计文件/验收文件、历史记录和网管系统，查看 OSC 的传输是否分段，并且具有 3R 功能和双向传输功能；

e）应检查网络设计文件/验收文件、历史记录和网管系统，检查 OSC 是否具有自我管理能力，光监控通路信号丢失时是否有告警指示，是否完全独立于其他工作通道。

6.2.1.5 ASON 光网络安全

6.2.1.5.1 网络拓扑安全

6.2.1.5.1.1 检测方式

访谈，检查。

6.2.1.5.1.2 检测对象

传送网络管理员，网络拓扑，网络拓扑图，网络设计/验收文档。

6.2.1.5.1.3 检测实施

a）应访谈传送网管理人员，了解目前传送网的网络组织情况；

b）应检查网络拓扑图，查看其与当前运行情况是否一致，是否以环型和网状网为主；

c）应检查光缆/管道的使用年限，查看其是否超过设计使用年限，对于超过设计年限要求的光缆/管道应检查是否具有在线监测措施，是否定期记录光缆/管道使用状态。

6.2.1.5.2 网络保护与恢复能力

6.2.1.5.2.1 检测方式

访谈，检查。

6.2.1.5.2.2 检测对象

传送网网络管理员，网络设计/验收文档，历史记录，网络管理系统。

6.2.1.5.2.3 检测实施

a）应访谈网络管理员，并检查传送网设计文件，了解目前传送网的网络保护与恢复情况；

b）应检查网络设计文件和验收文件、演练记录、历史记录和基本处理预案，查看传送网是否根据业务需求提供相应的网络保护能力，如提供基于传送平面的 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/路径保护方式等保护方式；

c）应检查网络设计文件和验收文件、演练记录、历史记录和基本处理预案，查看传送网根据业务需求提供是否支持恢复以及一种或多种保护与恢复结合方式；

d）应检查传送网验收文件和历史记录，查看保护倒换时间是否满足小于 50ms（大于 1200km 的环网根据实际传输距离考虑）要求，同时查看业务的恢复时间范围；

e）应检查网络设计文件和验收文件、历史记录中的工作路径与保护路径的网络抖动、色散容限、光信噪比（OSNR）等参数，查看其是否设计要求。

6.2.1.5.3 MCN 安全

具体要求同6.3.1.2.3。

6.2.1.5.4 SCN 安全

6.2.1.5.4.1 检测方式

访谈，检查。

6.2.1.5.4.2 检测对象

ASON设备，网络管理员，网络设计/验收文档，历史记录。

6.2.1.5.4.3 检测实施

a）应检查网络设计/验收文档和历史记录，查看传送网 SCN 是否保证恢复消息的可靠和快速传送；

b）应检查网络设计/验收文档和历史记录，查看在管理域边界，是否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；

c）应检查历史记录，查看 SCN 是否可以防止未经授权的用户非法接入。

6.2.1.5.5 传送平面安全

6.2.1.5.5.1 检测方式

访谈，检查。

6.2.1.5.5.2 检测对象

ASON设备，网络管理员，网络设计/验收文档，历史记录。

6.2.1.5.5.3 检测实施

a）应访谈网络管理员，询问 ASON 在传输链路层面是否出现过误连接情况，最后是如何解决该类问题；

b）应检查历史记录文档，查看 ASON 在传送平面功能否正常，曾经是否出现过错连问题，最后是如何解决该类问题；

c）应检查网络设计/验收文档，查看 ASON 的传送平面是否满足设计要求。

6.2.1.5.6 控制平面安全

6.2.1.5.6.1 检测方式

访谈，检查。

6.2.1.5.6.2 检测对象

ASON设备，网络管理员，网络设计/验收文档，历史记录。

6.2.1.5.6.3 检测实施

a）应访谈网络管理员，询问 ASON 在控制平面是否工作正常，曾经是否出现过控制故障，最后是如何解决该类问题；

b）应检查历史记录文档，查看 ASON 在控制平面方面是否正常，曾经是否出现过控制平面故障，最后是如何解决该类问题；

c）应检查网络设计/验收文档，查看 ASON 的控制平面是否满足设计要求；

d）应检查网络设计/验收文档，查看控制平面是否支持 OIF 定义的“UNI 和 NNI 安全扩展”；

e）应检查历史记录文档，查看控制平面是否能够拒绝所有未认证的接入；

f）应检查历史记录文档，查看敏感的网络信息是否不能经过外部接口（UNI 或 E-NNI），经过 E-NNI 的信息是否需要根据设置的策略受到控制和限制等；

g）应检查网络设计/验收文档，查看在 UNI 和 E-NNI 交换发现、信令和路由消息时，是否支持认证、完整性和机密性等安全机制；

h）应检查网络设计/验收文档，查看控制平面是否选择其它方法进行保护，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；

i）应检查网络设计/验收文档，查看不同厂家安全机制之间是否实现了互通；

j）应检查网络设计/验收文档，查看控制平面是否能保证 NNI 之间安全地交换路由信息；

k）应检查网络设计/验收文档，查看 E-NNI 是否支持理由信息的鉴权、完整性和私密性。

6.2.1.5.7 管理平面安全

6.2.1.5.7.1 检测方式

访谈，检查，测试。

6.2.1.5.7.2 检测对象

ASON设备，网络管理员，网络设计/验收文档，历史记录，网管系统。

6.2.1.5.7.3 检测实施

a）应访谈网络管理员，询问ASON网管出现过哪些安全问题以及如何解决这些安全问题；

b）应测试网管系统的不同权限的用户等级，查看是否禁止低权限用户使用高权限的管理操作功能；

c）应检查网管系统的日志，查看其是否建立登录日志和操作日志并对其进行管理；

d）应检查网管系统是否具备安全保护措施，以防止外部侵入和病毒破坏；

e）应检查历史记录文档，查看当与传送平面/控制平面的通信中断时，系统是否在一定时间内自动尝试重建连接，通信恢复后，网管是否支持自动和手工方式实现网管数据的同步和更新；

f）应检查历史记录文档，查看用户界面程序异常停止后，是否影响服务器端和其他用户界面的正常运行；

g）应检查网络设计/验收文档，查看管理平面故障是否影响控制平面和传送平面的正常工作。

6.2.1.6 微波接力传送网络

6.2.1.6.1 网络拓扑安全

6.2.1.6.1.1 检测方式

访谈，检查。

6.2.1.6.1.2 检测对象

微波接力传送网络管理员，网络拓扑，网络拓扑图，网络设计/验收文档。

6.2.1.6.1.3 检测实施

a）应访谈微波传送网管理人员，了解目前微波传送网的网络组织情况；

b）应检查网络拓扑图，查看其与当前运行情况是否一致。

6.2.1.6.2 网络保护与恢复能力

6.2.1.6.2.1 检测方式

访谈，检查。

6.2.1.6.2.2 检测对象

传送网网络管理员，网络设计/验收文档，历史记录，网络管理系统。

6.2.1.6.2.3 检测实施

a）应访谈网络管理员，并检查微波传送网设计文件，了解目前微波接力传送网的工作波道的备用波道情况；

b）应访谈网络管理员，并检查微波传送网设计文件，了解目前微波接力传送网的公务波道是否支持 1+1 备份；

c）应检查网络设计文件和验收文件、演练记录、历史记录和基本处理预案，查看微波接力传送网是

否根据业务需求提供备用波道的倒换机制。

6.2.1.6.3 MCN 安全

具体要求同6.3.1.2.3。

6.2.1.7 卫星传送网络

6.2.1.7.1 网络拓扑安全

6.2.1.7.1.1 检测方式

访谈，检查。

6.2.1.7.1.2 检测对象

卫星传送网络管理员，网络拓扑，网络拓扑图，网络设计/验收文档。

6.2.1.7.1.3 检测实施

a）应访谈卫星传送网管理人员，了解目前卫星传送网的网络组织情况，是否为星状网和网状网相结合；

b）应检查网络拓扑图，查看其与当前运行情况是否一致。

6.2.1.7.2 MCN 安全

具体要求同6.3.1.2.3。

6.2.1.8 OTN 光网络安全

待研究。

6.2.1.9 PTN 光网络安全

待研究。

6.2.2 传送网设备安全

6.2.2.1 检测方式

访谈，检查。

6.2.2.2 检测对象

设备入网检测报告，设备入网证，设备安全检测报告。

6.2.2.3 检测实施

应访谈相关技术支持人员和管理人员，检查设备（包括PDH、SDH、MSTP、WDM、ASON 、OTN、PTN、微波接力设备和卫星通信设备等设备）是否有入网检测报告、入网证、安全检测报告。

6.2.3 物理环境安全

应满足《电信网和互联网物理环境安全等级保护检测要求》中第2级的检测要求。

6.2.4 管理安全

应满足《电信网和互联网管理安全等级保护检测要求》中第2级的检测要求。

6.3 第 3.1 级要求

6.3.1 传送网网络安全

6.3.1.1 PDH 光网络安全

6.3.1.1.1 网络拓扑安全

6.3.1.1.1.1 检测方式

访谈，检查。

6.3.1.1.1.2 检测对象

传送网络管理员，网络拓扑图，入网检测报告，故障记录，网络设计/验收文档。

6.3.1.1.1.3 检测实施

除按照6.2.1.1.1的要求进行检测之外，还应按照本节内容进行检测：应检查光缆纤芯/管道光缆使用预留情况，查看光纤/缆是否有一定的预留。

6.3.1.2 SDH 光网络安全

6.3.1.2.1 网络拓扑安全

6.3.1.2.1.1 检测方式

访谈，检查。

6.3.1.2.1.2 检测对象

传送网络管理员，网络拓扑，网络拓扑图，网络设计/验收文档。

6.3.1.2.1.3 检测实施

除按照6.2.1.2.1的要求进行检测之外，还应按照本节内容进行检测：

a）应检查光缆纤芯/管道光缆使用预留情况，查看节点之间的同物理路由和异物理路由光纤/缆是否有一定比例的预留；

b）应检查网络是否预留了一定比例的冗余通道和维护通道。

6.3.1.2.2 网络保护与恢复能力

6.3.1.2.2.1 检测方式

访谈，检查。

6.3.1.2.2.2 检测对象

传送网网络管理员，网络设计/验收文档，历史记录，网络管理系统。

6.3.1.2.2.3 检测实施

除按照6.2.1.2.2的要求进行检测之外，还应按照本节内容进行检测：应检查传送网验收文件和历史记录，查看保护路径与工作路径是否为不同路由。

6.3.1.2.3 MCN 安全

6.3.1.2.3.1 检测方式

访谈，检查。

6.3.1.2.3.2 检测对象

网络管理员，网络设计/验收文档、历史记录。

6.3.1.2.3.3 检测实施

除按照6.2.1.2.3的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈网络管理员，询问传送网 MCN 的配置情况，MCN 是否有冗余路由；

b）应检查网络设计/验收文档和历史记录，MCN 是否支持冗余设计，即是否提供紧急功能的网管系统和网元需要多条通道接入 MCN。

6.3.1.3 MSTP 光网络安全

6.3.1.3.1 网络拓扑安全

具体检测要求同6.3.1.2.1。

6.3.1.3.2 网络保护与恢复能力

具体检测要求同6.3.1.2.2。

6.3.1.3.3 MCN 安全

具体检测要求同6.3.1.2.3。

6.3.1.4 WDM 光网络安全

6.3.1.4.1 网络拓扑安全

6.3.1.4.1.1 检测方式

访谈，检查。

6.3.1.4.1.2 检测对象

传送网络管理员，网络拓扑，网络拓扑图，网络设计/验收文档。

6.3.1.4.1.3 检测实施

除按照6.2.1.4.1的要求进行检测之外，还应按照本节内容进行检测：

a） 应检查光缆纤芯/管道光缆使用预留情况，查看节点之间的同物理路由和异物理路由光纤/缆是否有一定比例的预留；

b） 应检查网络是否预留了一定比例的冗余波道和维护波道。

6.3.1.4.2 网络保护与恢复能力

6.3.1.4.2.1 检测方式

访谈，检查。

6.3.1.4.2.2 检测对象

传送网网络管理员，网络设计/验收文档，历史记录，网络管理系统。

6.3.1.4.2.3 检测实施

除按照6.2.1.4.2的要求进行检测之外，还应按照本节内容进行检测：检查保护路径与工作路径为不同物理路由还是相同物理路由。

6.3.1.4.3 MCN 安全

具体检测要求同 6.2.1.4.3。

6.3.1.5 ASON 光网络安全

6.3.1.5.1 网络拓扑安全

6.3.1.5.1.1 检测方式

访谈，检查。

6.3.1.5.1.2 检测对象

传送网络管理员，网络拓扑，网络拓扑图，网络设计/验收文档。

6.3.1.5.1.3 检测实施

除按照6.2.1.5.1的要求进行检测之外，还应按照本节内容进行检测：

a）应检查节点之间是否支持 2 条以上的物理路由；

b）应检查光缆纤芯/管道光缆使用预留情况，查看节点之间的同物理路由和异物理路由光纤/缆是否有一定比例的预留；

c）应检查网络是否预留了一定比例的冗余通道和维护通道。

6.3.1.5.2 网络保护与恢复能力

6.3.1.5.2.1 检测方式

访谈，检查。

6.3.1.5.2.2 检测对象

传送网网络管理员，网络设计/验收文档，历史记录，网络管理系统。

6.3.1.5.2.3 检测实施

除按照6.2.1.5.2的要求进行检测之外，还应按照本节内容进行检测：检查保护路径与工作路径是否为不同路由。

6.3.1.5.3 MCN 安全

具体检测要求同6.3.1.2.3。

6.3.1.5.4 SCN 安全

6.3.1.5.4.1 检测方式

访谈，检查。

6.3.1.5.4.2 检测对象

ASON设备，网络管理员，网络设计/验收文档，历史记录。

6.3.1.5.4.3 检测实施

除按照6.2.1.5.4的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈网络管理员，询问传送网 SCN 的配置情况，SCN 是否有冗余路由；

b）应检查网络设计/验收文档和历史记录，查看 SCN 自身是否能提供保护和恢复机制，如 1+1 保护和重路由方式等。

6.3.1.5.5 传送平面安全

检测要求同 6.2.1.5.5。

6.3.1.5.6 控制平面安全

6.3.1.5.6.1 检测方式

访谈，检查。

6.3.1.5.6.2 检测对象

ASON设备，网络管理员，网络设计/验收文档，历史记录。

6.3.1.5.6.3 检测实施

除按照6.2.1.5.6的要求进行检测之外，还应按照本节内容进行检测：

a）应检查历史记录文档，查看控制平面是否能够产生告警并向管理平面通告安全相关事件，且在管理平面上建立安全日志，管理平面是否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）应检查历史记录文档，查看控制平面是否能够从侵入攻击中恢复。

6.3.1.5.7 管理平面安全

6.3.1.5.7.1 检测方式

访谈，检查，测试。

6.3.1.5.7.2 检测对象

ASON设备，网络管理员，网络设计/验收文档，历史记录，网管系统。

6.3.1.5.7.3 检测实施

除按照6.3.1.5.7的要求进行检测之外，还应按照本节内容进行检测：

a）应检查网络设计/验收文档，查看网管系统是否支持（1+1）热备用（Hot-Standby）或温备用（Warm-Standby）配置。在热备用的方式下，主用到备用的切换应为实时切换；在温备用的方式下，主用到备用的平均切换时间应小于20min。

b）应检查网络设计/验收文档，查看网管是否支持对网管数据的备份，包括人工备份和自动定期备份。

6.3.1.6 微波接力传送网络

具体检测要求同6.2.1.6。

6.3.1.7 卫星传送网络

6.3.1.7.1 网络拓扑安全

6.3.1.7.1.1 检测方式

访谈，检查。

6.3.1.7.1.2 检测对象

卫星传送网络管理员，网络拓扑，网络拓扑图，网络设计/验收文档。

6.3.1.7.1.3 检测实施

除按照6.2.1.7.1的要求进行检测之外，还应按照本节内容进行检测：检查重要链路是否支持地球站之间的互为备用。

6.3.1.7.2 MCN 安全

具体检测要求同6.3.1.2.3。

6.3.1.8 OTN 光网络安全

待研究。

6.3.1.9 PTN 光网络安全

待研究。

6.3.2 传送网设备安全

具体检测要求同6.2.2。

6.3.3 物理环境安全

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

6.3.4 管理安全

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

6.4 第 3.2 级要求

6.4.1 传送网网络安全

6.4.1.1 PDH 网络

具体检测要求同6.3.1.1。

6.4.1.2 SDH 光网络安全

6.4.1.2.1 网络拓扑安全

6.4.1.2.1.1 检测方式

访谈，检查。

6.4.1.2.1.2 检测对象

传送网络管理员，网络拓扑，网络拓扑图，网络设计/验收文档。

6.4.1.2.1.3 检测实施

除按照6.3.1.2.1的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈传送网管理人员，了解目前传送网的网络组织情况；

b）应检查网络拓扑图，查看其与当前运行情况是否一致，是否以环型为主；

c）应检查网络是否采用双平面结构；

d）应检查网络层间互联是否采用设备分离双节点结构。

6.4.1.2.2 网络保护与恢复能力

6.4.1.2.2.1 检测方式

访谈，检查。

6.4.1.2.2.2 检测对象

传送网络管理员，网络设计/验收文档，历史记录，网络管理系统。

6.4.1.2.2.3 检测实施

除按照6.3.1.2.2的要求进行检测之外，还应按照本节内容进行检测：应检查传送网验收文件和历史记录，查看保护路径与工作路径是否物理分离。

6.4.1.2.3 MCN 安全

具体检测要求同6.3.1.2.3。

6.4.1.3 MSTP.光网络安全

具体检测要求同6.3.1.3。

6.4.1.4 WDM 光网络安全

6.4.1.4.1 网络拓扑安全

6.4.1.4.1.1 检测方式

访谈，检查。

6.4.1.4.1.2 检测对象

传送网络管理员，网络拓扑，网络拓扑图，网络设计/验收文档。

6.4.1.4.1.3 检测实施

除按照第6.3.1.4.1的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈传送网管理人员，了解目前传送网的网络组织情况；

b）应检查网络设计/验收文档，查看不同机楼（节点）之间光缆/管道是否存在多条物理路由；

c）应检查网络是否采用双平面结构。

6.4.1.4.2 网络保护与恢复能力

6.4.1.4.2.1 检测方式

访谈，检查。

6.4.1.4.2.2 检测对象

传送网络管理员，网络设计/验收文档，历史记录，网络管理系统。

6.4.1.4.2.3 检测实施

除按照6.3.1.4.2的要求进行检测之外，还应按照本节内容进行检测：应检查传送网验收文件和历史记录，查看保护路径与工作路径是否物理分离。

6.4.1.4.3 MCN 安全

具体检测要求同6.3.1.4.3。

6.4.1.5 ASON 安全

6.4.1.5.1 网络拓扑安全

具体检测要求同6.3.1.5.1。

6.4.1.5.2 网络保护与恢复能力

6.4.1.5.2.1 检测方式

访谈，检查。

6.4.1.5.2.2 检测对象

传送网络管理员，网络设计/验收文档，历史记录，网络管理系统。

6.4.1.5.2.3 检测实施

除按照6.3.1.5.2的要求进行检测之外，还应按照本节内容进行检测：应检查传送网验收文件和历史记录，查看保护恢复路径与工作路径是否物理分离。

6.4.1.5.3 MCN 安全

具体检测要求同6.3.1.5.3。

6.4.1.5.4 SCN 安全

具体检测要求同6.3.1.5.4。

6.4.1.5.5 传送平面安全

具体检测要求同6.3.1.5.5。

6.4.1.5.6 控制平面安全

具体检测要求同6.3.1.5.6。

6.4.1.5.7 管理平面安全

具体检测要求同6.3.1.5.7。

6.4.1.6 OTN 光网络

待研究。

6.4.1.7 PTN 光网络

待研究。

6.4.2 传送网设备安全

具体检测要求同6.3.2。

6.4.3 物理环境安全

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护检测要求》中第3.2级的检测要求。

6.4.4 管理安全

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

6.5 第 4 级要求

6.5.1 网络安全要求

6.5.1.1 PDH 光网络

具体检测要求同6.4.1.1。

6.5.1.2 SDH 光网络

具体检测要求同6.4.1.2。

6.5.1.3 MSTP 光网络

具体检测要求同6.4.1.3。

6.5.1.4 WDM 光网络

具体检测要求同6.4.1.4。

6.5.1.5 ASON 光网络

具体检测要求同6.4.1.5。

6.5.1.6 OTN 光网络

待研究。

6.5.1.7 PTN 光网络

待研究。

6.5.2 传送网设备安全

具体检测要求同6.4.2。

6.5.3 物理环境安全

除了按照6.4.3的要求进行检测之外，还应按照本节下列内容进行检测。

6.5.3.1 检测方式

访谈，检查。

6.5.3.2 检测对象

传送网机房。

6.5.3.3 检测实施

a）应访谈机房管理员，了解传送网机房对于人员出入控制、机房防水、防静电和防电磁辐射等方面所采取的措施和方法；

b）应检查机房对于重要区域是否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；

c）应检查机房是否安装对水敏感的检测仪表或元件，以便对机房进行防水检测和报警；

d）应检查机房是否安装静电消除器等装置，以减少静电产生；

e）应检查机房是否实施电磁屏蔽。

6.5.4 管理安全

除了按照6.4.4的要求进行检测之外，还应按照本节下列内容进行检测。

6.5.4.1 检测方式

访谈，检查。

6.5.4.2 检测对象

关键区域管理制度，关键区域访问记录，网络管理用户授权记录，变更控制记录，秘密数据备份记录。

6.5.4.3 检测实施

a）应访谈安全主管，了解传送网关于区域管理制度、秘密数据备份管理制度，重大失、泄密事件管理制度等方面的主要内容；

b）应检查关键区域访问记录，对于关键区域是否允许第三方人员访问；

c）应检查关键区域一般管理制度，对于机房和办公环境等关键区域是否实行统一策略的安全管理，出入人员是否经过相应级别授权，对进入重要安全区域的活动行为是否实时监视和记录；

d）应检查关键区域一般管理制度，所有信息是否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；

e）应检查网络管理用户授权记录，是否严格控制网络管理用户的授权，在授权程序中是否有两人在场，并经双重认可后方可操作，操作过程是否有不可更改的审计日志；

f）应检查变更控制记录，是否相关负责人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；

g）在有授权的情况下，应检查秘密数据备份记录，对需要采取加密或数据隐藏处理的备份数据，是否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；

h）在有授权的情况下，应检查关键区域管理制度及相关记录，对于可能涉及国家秘密的重大失、泄密事件，是否按照有关规定向公安、安全、保密等部门汇报；

i）在有授权的情况下，应检查关键区域管理制度及相关记录，是否严格控制参与涉密事件处理和恢复的人员，重要操作是否要求至少两名工作人员在场并登记备案。

6.6 第5级要求

待补充。

7 传送网安全风险评估检测要求

7.1 安全风险评估范围

7.1.1 检测方式

访谈，检查。

7.1.2 检测对象

风险评估报告。

7.1.3 检测实施

应访谈风险评估负责人，询问进行传送网风险评估时，选择的风险评估范围是什么，应检查风险评估报告，查看其风险评估范围是否与要求相一致。

7.2 安全风险评估内容

7.2.1 检测方式

访谈，检查。

7.2.2 检测对象

风险评估报告。

7.2.3 检测实施

a）应访谈传送网风险评估负责人，查看传送网风险评估报告，检查风险评估报告是否覆盖了技术安全和管理安全；

b）应访谈传送网风险评估负责人，查看传送网风险评估报告，检查风险评估报告中技术安全是否覆盖了网络安全、设备安全和物理安全等方面；

c）应访谈传送网风险评估负责人，查看传送网风险评估报告，检查风险评估报告中管理安全是否覆盖了安全管理机构、安全管理制度、人员安全管理、安全建设管理、安全运维管理等方面。

7.3 安全风险评估要素

7.3.1 检测方式

访谈，检查。

7.3.2 检测对象

风险评估报告，历史记录。

7.3.3 检测实施

a）应访谈风险评估负责人，询问进行传送网风险评估时采用了哪些风险评估的要素，查看风险评估报告，检查风险评估时是否包含了资产、脆弱性、威胁、安全措施、风险和残余风险等要素。

b）应访谈风险评估负责人，询问进行传送网风险评估时考虑了哪些风险评估要素的相关属性；查看风险评估报告，检查传送网风险评估报告是否包含了与评估要素密切相关的业务战略、资产价值、安全需求和安全事件等属性。

c）应访谈风险评估负责人，询问进行传送网风险评估时评估了哪些资产；查看风险评估报告，检查风险评估报告中资产是否包含了设备硬件（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、防水和防潮系统，防静电系统，防雷击系统，温湿度控制系统等），各种设备的系统软件、系统控制软件、协议软件、操作维护系统软件，支撑传送网运行的各种重要数据，网络提供的各类业务，设备维护人员、各种管理规定和设备文档、网络拓扑源等。

d）应访谈风险评估负责人，询问计算传送网各资产的资产价值时考虑了哪些因素；查看风险评估报告，检查风险评估报告中资产价值的计算是否主要考虑了社会影响力、资产价值和可用性等因素，同时采用了合理的计算方法。

e）应访谈风险评估负责人，询问识别传送网各资产的脆弱性时考虑了哪些方面的脆弱，查看风险评估报告，检查风险评估报告中脆弱性识别是否包含了技术脆弱性和管理脆弱性等方面。

f）应访谈风险评估负责人，询问识别传送网各资产的脆弱性时考虑了哪些方面的脆弱性；查看风险评估报告中技术脆弱性是否包含了网络脆弱性、设备脆弱性和物理环境脆弱性，管理脆弱性是否包含安全管理机构方面的脆弱性、人员管理方面脆弱性、建设管理方面的脆弱性、运维管理方面的脆弱性。

g）应访谈风险评估负责人，询问传送网存在哪些威胁；查看风险评估报告，检查风险评估报告中威胁是否包含了网络设备自身的威胁、环境威胁、人员威胁。

h）应访谈风险评估负责人，询问威胁识别依据了哪些历史数据；查看风险评估报告，检查风险评估报告中威胁识别是否依据已有的安全事件报告数据、检测工具检测数据和国内外同行业报告数据等多个方面综合考虑。

i）应访谈风险评估负责人，询问风险值的计算采用了哪种计算方法；查看风险评估报告，检查传送网风险评估中风险值的计算是否主要考虑了资产、威胁和脆弱性等因素，是否采用了合理的计算方法。

j）应访谈风险评估负责人，询问如何确定的风险阈值；查看风险评估报告，检查传送网风险评估中确定的风险阈值是否合理，是否与资产所在网络或系统的安全等级相结合。

k）应访谈风险评估负责人，询问对于不可接收的风险，是否制定了相应的风险处理计划；查看风险评估报告，检查传送网风险评估中对于不可接收的风险，是否制定了相应的风险处理计划，采用风险处理计划以后，风险值是否满足阈值要求。

7.4 安全风险评估赋值原则

7.4.1 检测方式

访谈，检查。

7.4.2 检测对象

风险评估报告。

7.4.3 检测实施

a）应访谈风险评估负责人，询问传送网风险评估时对资产的赋值遵循了什么样的原则，查看风险评估报告，检查传送网各资产的赋值是否从资产的社会影响力、资产价值和可用性三个方面和5个等级进行赋值；

b）应访谈风险评估负责人，询问传送网风险评估时对脆弱性的赋值遵循了什么样的原则；查看风险评估报告，检查传送网脆弱性的赋值是否考虑赋值对象对资产损害程度等因素，同时是否按照5个等级进行赋值；

c）应访谈风险评估负责人，询问传送网风险评估时对威胁的赋值遵循了什么样的原则；查看风险评估报告，检查传送网威胁的赋值是否依据威胁发生的频率，同时是否按照5个等级进行赋值。

7.5 安全风险评估计算方法

7.5.1 检测方式

访谈，检查。

7.5.2 检测对象

风险评估报告。

7.5.3 检测实施

a）应访谈风险评估负责人，询问传送网风险评估中采用了什么样的方法计算资产价值；查看风险评估报告，检查传送网资产价值的计算方法是否合理，是否有对所采用计算方法的理论分析。

b）应访谈风险评估负责人，询问传送网风险评估中采用了什么样的方法计算风险值；查看风险评估报告，检查传送网风险值的计算方法是否合理，是否有对所采用计算方法的理论分析。

7.6 安全风险评估文件类型

7.6.1 检测方式

访谈，检查。

7.6.2 检测对象

风险评估报告，风险评估文件。

7.6.3 检测实施

a）应访谈风险评估负责人，询问是否制定了风险评估方案；查看此文件，检查是否包括风险评估的目标、范围、人员、评估方法、评估结果的形式和实施进度等内容。

b）应访谈风险评估负责人，询问是否制定了风险评估程序；查看此文件，检查是否包括风险评估的目的、职责、过程、相关的文件要求，以及实施本次评估所需要的各种资产、威胁、脆弱性识别和判断依据等内容。

c）应访谈风险评估负责人，询问是否制定了资产识别清单；查看此文件，检查是否根据组织在风险评估程序文件中所确定的资产分类方法进行资产识别，形成资产识别清单，明确资产的责任人/部门等内容。

d）应访谈风险评估负责人，询问是否制定了重要资产清单；查看此文件，检查是否根据资产识别和赋值的结果，形成重要资产列表，包括重要资产名称、描述、类型、重要程度、责任人/部门等内容。

e）应访谈风险评估负责人，询问是否根据威胁识别和赋值的结果，制定了威胁列表；查看此文件，检查是否包括威胁名称、种类、来源、动机及出现的频率等内容。

f）应访谈风险评估负责人，询问是否根据脆弱性识别和赋值的结果，形成脆弱性列表；查看此文件，检查是否包括具体脆弱性的名称、描述、类型及严重程度等。

g）应访谈风险评估负责人，询问是否根据已采取的安全措施确认的结果，形成已有安全措施确认表；查看此文件，检查是否包括已有安全措施名称、类型、功能描述及实施效果等。

h）应访谈风险评估负责人，询问是否有风险评估报告；查看此文件，检查是否对整个风险评估过程和结果进行总结，详细说明被评估对象，风险评估方法，资产、威胁、脆弱性的识别结果，风险分析、风险统计和结论等内容。

i）应访谈风险评估负责人，询问是否有风险处理计划；查看此文件，检查是否对评估结果中不可接受的风险制定风险处理计划，选择适当的控制目标及安全措施，明确责任、进度、资源，并通过对残余风险的评价以确定所选择安全措施的有效性。

j）应访谈风险评估负责人，询问是否有风险评估记录；查看此文件，检查风险评估过程中的各种现场记录是否可复现评估过程，是否能够作为产生歧义后解决问题的依据。

7.7 安全风险评估文件记录

7.7.1 检测方式

访谈，检查。

7.7.2 检测对象

风险评估报告，风险评估文件。

7.7.3 检测实施

a）应访谈风险评估负责人，询问风险评估文件发布以前是否需要批准；应查看风险评估文件，检查文件发布以前是否得到批准。

b）应访谈风险评估负责人，询问风险评估文件的更改和现行修订状态是如何进行识别的；应查看风险评估文件，检查文件的更改和现行修订状态是否是可识别的。

c）应访谈风险评估负责人，询问风险评估文件的版本如何管理；应查看风险评估文件，检查是否有版本划分以及相应的版本使用说明。

d）应访谈风险评估负责人，询问作废文件是如何管理的；应查看风险评估文件，检查是否对作废文件作了标识。

e）应访谈风险评估负责人，询问如何对文件进行控制；应查看风险评估文件，检查是否规定其标识、储存、保护、检索、保存期限以及处置所需的控制。

8 传送网灾难备份及恢复检测要求

8.1 第1级要求

不作要求。

8.2 第2级要求

8.2.1 冗余系统、冗余设备及冗余链路

8.2.1.1 检测方式

访谈，检查。

8.2.1.2 检测对象

传送网的冗余系统、冗余设备和冗余链路，运行日志、故障记录，设计/验收文档，演练文档。

8.2.1.3 检测实施

a）应访谈安全管理人员，询问并现场检查传送网目前有哪些冗余系统、冗余设备、冗余链路的设计和部署，是否与设计/验收文档相符合；查看运行日志、故障记录，检查出现灾难以后采用冗余系统、冗余设备和冗余链路来进行灾难恢复的情况。

b）应访谈安全管理人员，询问并现场检查采取了哪些措施防止单节点的灾难导致其他节点的业务提供发生异常，查看运行日志、故障记录，检查是否发生过单一地区范围的灾难导致其他地区的业务提供发生异常的情况，安全措施是否与设计/验收文档相符合。

c） 应访谈安全管理人员，查看演练文档，检查传送网的网络灾难演练恢复时间是否能够满足行业管理、网络和业务运营商应急预案的相关要求。

8.2.2 冗余路由

8.2.2.1 检测方式

访谈，检查。

8.2.2.2 检测对象

传送网物理链路，设计/验收文档，演练记录，故障记录。

8.2.2.3 检测实施

a）应访谈安全管理人员，询问传送网络的物理链路是否采用了冗余路由以及冗余路由是否都可以传送业务；

b）应访谈安全管理人员，询问并查看演练记录、故障记录，检查传送网是否有带宽负荷分担的功能，是否与设计/验收文档相符合，是否发生过带宽负荷分担能力不足影响网络业务提供的情况。

8.2.3 备份数据

8.2.3.1 检测方式

访谈，检查。

8.2.3.2 检测对象

数据备份服务器，设计/验收文档，演练记录。

8.2.3.3 检测实施

a）应访谈传送网安全管理人员，询问是否支持关键数据（如传送网网络配置数据、性能数据、告警数据和安全数据）的本地定期备份；

b）应访谈传送网安全管理人员，询问并查看传送网是否支持关键数据的本地定期备份；

c）应访谈安全管理人员，询问并查看数据备份服务器、演练记录，检查传送网关键数据的备份范围和时间间隔、采取的备份方式、数据恢复能力的情况，是否与设计/验收文档一致。

8.2.4 人员和技术支持能力

8.2.4.1 检测方式

访谈，检查。

8.2.4.2 检测对象

机房管理人员，技术支持人员，历史值班记录，培训记录。

8.2.4.3 检测实施

a）应访谈安全管理相关人员，询问并查看历史值班记录，检查是否有负责灾难备份及恢复的机房管理人员、技术支持人员，检查相关人员对灾难备份及恢复的技术支持能力；

b）应访谈安全管理相关人员，询问并查看培训记录，检查负责灾难备份及恢复的人员定期进行灾难备份及恢复方面的技能培训的情况。

8.2.5 运行维护管理能力

8.2.5.1 检测方式

访谈，检查。

8.2.5.2 检测对象

机房运行管理制度，介质存取、验证和转储管理制度，设备和网络运行管理制度，数据异地实时容灾备份管理制度，联络和协作的记录，操作系统、数据库、网管系统和设备软件运行管理制度。

8.2.5.3 检测实施

a）应访谈安全管理人员，询问并查看机房运行管理制度，检查是否有完善的针对灾难备份及恢复的机房运行管理制度；

b）应访谈安全管理人员，询问并查看介质存取、验证和转储管理制度，检查是否有完善的针对灾难备份及恢复的介质存取、验证和转储管理制度，检查备份数据的授权访问情况；

c）应访谈安全管理人员，询问并检查按介质特性对灾难备份及恢复相关数据定期进行有效性验证的情况；

d）应访谈安全管理人员，询问并查看设备和网络运行管理制度，检查是否有完善的针对灾难备份及恢复的设备和网络运行管理制度；

e）应访谈安全管理人员，询问并查看数据异地实时容灾备份管理制度，检查是否有完善的针对灾难备份及恢复的数据异地实时容灾备份管理制度；

f）应访谈安全管理人员，询问并查看与其他组织进行联络和协作的记录，检查传送网内部是否具有与外部组织保持良好的联络和协作的能力；

g）应访谈安全管理人员，询问并查看操作系统、数据库、网管系统和设备软件运行管理制度，检查是否具有完善的针对灾难备份及恢复的操作系统、数据库、网管系统和设备软件运行管理制度（仅适用于重点监督保护级）。

8.2.6 灾难恢复预案

8.2.6.1 检测方式

访谈，检查。

8.2.6.2 检测对象

灾难恢复预案，设计/验收文档，灾难恢复预案的教育和培训记录、演练记录、调整记录、管理制度。

8.2.6.3 检测实施

a）应访谈安全管理人员，询问并查看灾难恢复预案，检查传送网是否具有完整的灾难恢复预案，是否与设计/验收文档一致。

b）应访谈安全管理人员，询问并查看灾难恢复预案的教育和培训记录，检查对灾难恢复预案进行教育和培训的情况，是否达到了教育和培训的预期目标，检查相关人员对灾难恢复预案的了解情况，检查相关人员是否具有对灾难恢复预案进行实际操作的能力。

c）应访谈安全管理人员，询问并查看灾难恢复预案演练记录，检查灾难恢复预案的演练情况，灾难恢复预案演练的效果是否达到设计要求；查看灾难恢复预案调整记录，检查根据演练结果对灾难恢复预案进行修正的情况。

d）应访谈安全管理人员，询问并查看传送网管理制度，检查是否有灾难恢复预案的管理制度（仅适用于重点监督保护级）。

8.3 第3.1级要求

8.3.1 冗余系统、冗余设备及冗余链路

8.3.1.1 检测方式

访谈，检查。

8.3.1.2 检测对象

传送网的冗余系统、冗余设备和冗余链路，运行日志、故障记录，设计/验收文档，演练文档。

8.3.1.3 检测实施

除按照8.2.1的要求进行检测之外，还应按照本节内容进行检测：应检查传送网的抗灾难以及灾难恢复能力设计/验收文档，查看是否采用异地/同地的链路、冗余系统和节点冗余来提供保护等。

8.3.2 冗余路由

具体检测要求同8.2.2。

8.3.3 备份数据

具体检测要求同8.2.3。

8.3.4 人员和技术支持能力

具体检测要求同8.2.4。

8.3.5 运行维护管理能力

具体检测要求同8.2.5。

8.3.6 灾难恢复预案

具体检测要求同8.2.6。

8.4 第3.2级要求

8.4.1 冗余系统、冗余设备及冗余链路

8.4.1.1 检测方式

访谈，检查。

8.4.1.2 检测对象

传送网的冗余系统、冗余设备和冗余链路，运行日志、故障记录，设计/验收文档，演练文档。

8.4.1.3 检测实施

除按照8.3.1的要求进行检测之外，还应按照本节内容进行检测：应检查传送网的抗灾难以及灾难恢复能力设计/验收文档，查看不同的传送网（光传送网、微波接力传送网、卫星传送网）是否可互为冗余网络。

8.4.2 冗余路由

8.4.2.1 检测方式

访谈，检查。

8.4.2.2 检测对象

传送网物理链路，设计/验收文档，演练记录，故障记录。

8.4.2.3 检测实施

除按照8.3.2的要求进行检测之外，还应按照本节内容进行检测：应检查设计/验收文档和历史记录，查看传送网络的物理链路是否采用了冗余路由。

8.4.3 数据备份

除按照8.3.3的要求进行检测之外，还应按照本节内容进行检测：应访谈传送网安全管理人员，询问并查看传送网是否支持关键数据的异地定期备份。

8.4.4 人员和技术支持能力

具体检测要求同8.3.4。

8.4.5 运行维护管理能力

8.4.5.1 检测方式

访谈，检查。

8.4.5.2 检测对象

机房运行管理制度，介质存取、验证和转储管理制度，设备和网络运行管理制度，数据异地实时容灾备份管理制度，联络和协作的记录，操作系统、数据库、网管系统和设备软件运行管理制度。

8.4.5.3 检测实施

除按照8.3.5的要求进行检测之外，还应按照本节内容进行检测：应访谈安全管理人员，询问并查看操作系统、数据库、网管系统和设备软件运行管理制度，检查是否具有完善的针对灾难备份及恢复的操作系统、数据库、网管系统和设备软件运行管理制度。

8.4.6 灾难恢复预案

8.4.6.1 检测方式

访谈，检查。

8.4.6.2 检测对象

灾难恢复预案，设计/验收文档，灾难恢复预案的教育和培训记录、演练记录、调整记录、管理制度。

8.4.6.3 检测实施

除按照8.3.6的要求进行检测之外，还应按照本节内容进行检测：应访谈安全管理人员，询问并查看传送网管理制度，检查是否有完善的灾难恢复预案管理制度。

8.5 第4级要求

8.5.1 冗余系统、冗余设备及冗余链路

8.5.1.1 检测方式

访谈，检查。

8.5.1.2 检测对象

传送网的冗余系统、冗余设备和冗余链路，运行日志、故障记录，设计/验收文档，演练文档。

8.5.1.3 检测实施

除按照8.4.1的要求进行检测之外，还应按照本节内容进行检测：应检查传送网的抗灾难以及灾难恢复能力设计/验收文档，查看是否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。

8.5.2 冗余路由

具体检测要求同8.4.2。

8.5.3 备份数据

具体检测要求同8.4.3。

8.5.4 人员和技术支持能力

具体检测要求同8.4.4。

8.5.5 运行维护管理能力

具体检测要求同8.4.5。

8.5.6 灾难恢复预案

具体检测要求同8.4.6。

8.6 第5级要求

待补充。