YD

中华人民共和国通信行业标准

YD/T 1748-2008

信令网安全防护要求

Security Protection Requirements for Signalling 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 1749-2008《信令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、中国网络通信集团公司、中国移动集团公司、中国联合通信有限公司

本标准主要起草人：邓东丰、薄明霞、尹粤容、魏　来、裴小燕

信令网安全防护要求

1 范围

本标准规定了信令网在安全等级保护、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No.7信令网。

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。

YDN 089-1998　No.7信令网技术体制(1998修订版)

YDN 113-1999　GSM No.7信令网技术体制

YD/T 1144-2001　国内No.7信令网信令转接点（STP）设备技术规范

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 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

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

信令网安全等级 Security Classification of Signalling Network

信令网安全重要程度的表征。重要程度可从信令网受到破坏后，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。

3.1.2

信令网安全等级保护 Classified Security Protection of Signalling Network

对信令网分等级实施安全保护。

3.1.3

组织 Organization

组织是由信令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。

3.1.4

信令网安全风险 Security Risk of Signalling Network

人为或自然的威胁可能利用信令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。

3.1.5

信令网安全风险评估 Security Risk Assessment of Signalling Network

指运用科学的方法和手段，系统地分析信令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，为进一步提出有针对性的抵御威胁的防护对策和安全措施，防范和化解信令网安全风险，将风险控制在可接受的水平，最大限度地保障信令网的安全提供科学依据。

3.1.6

信令网资产 Asset of Singalling Network

信令网中具有价值的资源，是安全防护保护的对象。信令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，如信令网节点设备、信令网的信令链路、信令网的网络布局等。

3.1.7

信令网资产价值 Asset Value of Singalling Network

信令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。

3.1.8

信令网威胁 Threat of Singalling Network

可能导致对信令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。常见的信令网络威胁有信令链路中断、信令设备节点失效、火灾、水灾等。

3.1.9

信令网脆弱性 Vulnerability of Singalling Network

脆弱性是信令网中存在的弱点、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。

3.1.10

信令网灾难 Disaster of Signalling Network

由于各种原因，造成信令网故障或瘫痪，使信令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。

3.1.11

信令网灾难备份 Backup for Disaster Recovery of Signalling Network

为了信令网灾难恢复而对相关网络要素进行备份的过程。

3.1.12

信令网灾难恢复 Disaster Recovery of Signalling Network

为了将信令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，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。

3.1.13

A链路、B链路、C链路以及D链路 Access Link，Bridge Link，Cross Link and Diagonal Link

A链路（接入链路）：连接SCP 或 SSP 到 STP 的信令数据链路；

B链路（桥接链路）：用于连接不同地区的STP的信令数据链路；

C链路（交叉链路）：一对冗余STP间的信令数据链路；

D链路（对角链路）：是指连接本地STP到其他No.7信令网络的链路。

3.2 缩略语

下列缩略语适用于本标准。

No.7	No.7 Signalling Network	七号信令网络
SP	Signalling Point	信令点
STP	Signalling Transfer Point	信令转接点
SG	Signalling Gateway	信令网关
MG	Media Gateway	媒体网关
OMAP	Operations Maintenance and Administrative Part	操作维护应用部分

4 信令网安全防护概述

4.1 信令网安全防护范围

本标准中的信令网即是七号信令网络，是一种国际性的标准化的通用公共信道信号系统。信令网是由信令点SP、信令转接点STP、信令链路以及信令网管理系统组成。信令网不但可以在电话网、电路交换的数据网和ISDN网中传送有关呼叫建立、释放的信令，还可以为交换局和各种特种服务中心（如业务控制点、网管中心等）间传送数据信息，并且也可以在七号信令系统与SG、MG的网络互通。

No.7为固定电话网/ISDN/智能网/移动网络等提供信令服务。

4.2 信令网安全防护内容

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

——信令网安全等级保护。主要包括定级对象和安全等级的确定、网络安全、路由安全、网络管理、设备安全、物理环境安全、管理安全等。

——信令网安全风险评估。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。本标准仅对信令网进行资产分析、脆弱性分析、威胁分析，在信令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》。

——信令网灾难备份及恢复。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。

5 信令网定级对象和安全等级确定

我国信令网按其地理覆盖范围大致分为省内信令网、省际信令网（含国际信令网）。网络和业务运营商应根据YD/T1729-2008《电信网和互联网安全等级保护实施指南》中确定网络安全等级的方法对信令网定级，即对省内信令网、省际信令网（含国际信令网）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，权重α、β、γ可根据具体网络情况进行调节。

6 信令网资产、脆弱性、威胁分析

6.1 信令网资产分析

信令网的资产包括设备硬件、设备软件、重要数据、管理文档以及人员等，见表 1。

表 1　资产列表

分　类	示　例
设备硬件	信令网包括 SP，具体有各种交换局、特种服务中心、移动业务交换中心、拜访位置寄存器、归属位置寄存器和鉴权中心的 SP，还包括 No.7 的网管硬件、STP、信令链路等； 物理环境设备包括机房、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
设备软件	设备的系统软件，如操作系统、No.7 信令系统等
重要数据	保存在设备上的各种重要数据，包括局数据、计费数据、网络配置数据、管理员操作维护记录等
管理文档	纸质以及保存在电脑中的各种文件，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、设备维护人员等

6.2　信令网脆弱性分析

信令网的脆弱性可以从技术脆弱性、管理脆弱性两个方面考虑，脆弱性识别对象应以资产为核心。表 2 给出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	信令网络拓扑设计不合理、信令路由配置不合理、信令网络内部的访问控制不够等
	设备（含操作系统）	用户名和口令保护不够，鉴权和访问控制机制不完善，重要部件未配置主备用保护，系统配置不合理，备份和恢复机制不健全，设备超过使用年限或核心部件老化，设备发生故障后未及时告警，单点 STP 设备失败造成信令网络失败。设备自身的软件、硬件故障，信令系统本身设计缺陷或软件 Bug
	数据	信令网络中日志或关键数据不全、丢失或篡改
	物理脆弱性	机房场地选择不合理，防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制不符合规范，通信线路、机房设备的保护不符合规范
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、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； 网络管理方面：信令网非正常工作时不能对故障检出、定位、隔离和恢复；不能有效控制信令网资源和它的组成单元；不能有效评估信令网资源的性能和通信活动；信令网管理中心不能对全网进行动态监视

6.3　信令网威胁性分析

信令网的根据来源可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其他物理威胁。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		系统无安全记录、软硬件故障、重要数据没有备份机制、设备单点故障、信令数据链路没有设置双路由策略、STP 设备没有设置双备份策略、信令设备的误操作以及重要数据的篡改；节假日或其他原因的高话务冲击等
环境威胁	物理环境	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
	自然灾害	鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、闪电
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而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

7　信令网安全等级保护要求

7.1　第 1 级要求

不作要求。

7.2　第 2 级要求

7.2.1　网络安全要求

7.2.1.1　网络拓扑安全

a）应绘制与当前运行情况相符合的信令网络拓扑图。

b）在两个SP或STP间配置两条或两条以上的信令链路作为备用。

c）每个低一级的STP通过信令链路至少要分别连接至互为备份的两个高一级STP，低一级STP连接到互为备份的两个高一级STP的信令链路之间应采用负荷分担方式工作。

d）每个SP至少应连至两个低一级的STP，在连至高一级STP时，应分别固定连至互为备份的高一级STP处，SP至两个低一级STP的信令链路组间采用负荷分担方式工作。

e）直联方式的信令链路组至少应包括两条信令链，准直联方式时，SP至STP的A链路组，连接本地STP到其他No.7的STP的D链路组可以只设置一条信令链，但一对冗余STP间的C链路组和连接不同地区的一对STP的B链路组应至少包括两条信令链。

f）为了保证信令网的安全可靠性，SP至STP的A链路，一对STP间的C链路应尽可能分配在完全分开的两条物理路由上，一对STP至另一对STP之间的B链路和D链路不管是何种连接方式，应尽可能分配在完全分开的3条物理路由上。

g）如果信令网络中同时存在64kbit/s和2Mbit/s信令链路，应在同一链路组中使用相同速率的链路，同时也应在采用负荷分担的链路组中使用速率相同的链路，以保证信令链路正确安全的实施。

h）对于直辖市、省会城市和地级市本地网拓扑应采用STP设备双备份的措施来保证本地信令网络的可靠安全性。

i）对于高速链路设计的业务负荷量不应过大（原则上建议目前每条高速信令链路的业务量最大不超过0.4ERL）。

j）信令网的不可用性指标应当满足ITU－T Q.706建议，即每年的不可用性指标不大于10min。

7.2.1.2 路由安全

通常在信令路由组中可以设置多个信令路由，包括直达信令路由、准直联信令路由以及采用负荷分担方式的信令路由,来保证两个具有信令关系的信令点之间传送信令的可靠性。

7.2.1.3 网络管理

7.2.1.3.1 信令网络管理通用要求

a）信令网管理活动应包括信令网非正常工作故障的检出、定位、隔离和恢复的故障管理；初始信令网业务和允许继续提供和停止信令业务的配置管理以及评估信令网络资源的性能和通信活动的有效性的性能管理。

b）能显示所辖范围内信令网的连接情况，能用数字和颜色指示出信令节点（STP、SP）链路组、链路的故障状态（如可用性），能用数字和颜色显示业务量。

c）STP设备可以通过信令网管理中心（NMC）进行监控、管理和维护，也可以通过操作工作台进行监控、管理和维护。

d）信令节点接口数据链路应支持数据链路优先权的设置和紧急消息的优先传递。

e）STP设备当中的路由表信息应该能够在信令网管理中心通过人机命令完成有关的建立、修改和删除的操作。

7.2.1.3.2 信令网络故障管理要求

a）具备对信令网的非正常工作时故障检出、定位、隔离以及修正，在某些情况下，故障的修正需要诊断功能。

b）具备对告警状态的处理功能，例如信令链路组的故障和信令点不可接入。

c）启动测量和测试。

d）能对网络单元性能数据统计分析。

7.2.1.3.3 信令网络结构管理要求

a）能够控制信令网和它的各个组成单元，并且采集和提供其数据，便于准备和信令业务的初始化，以及允许这种业务启动、继续和停止。

b）可以对No.7信令网静态结构设置。

c）能够更改已运行的No.7信令网的结构和提供状态改变信息。

d）在有关的信令点处根据主管部门确定的路由计划组建路由表。

e）对路由表进行校验，可以用读路由表的方法或按OMAP中规定的路由校验测试。

f）设置和启动信令链路组和信令链。

g）确认信令网中两信令点间命名的一致性，如一个信令链的SLC在两端的取值应相同，两端话音电路编码（CIC）的取值也应一致。

7.2.1.3.4 信令网络性能管理要求

a）能够进行数据统计，保存和读出网络和系统状态的历史记录和提供在正常和非正常条件下的网络性能。

b）能够对包括改变链路组的容量（如增加激活链路的数量）、改变路由的容量（如增加链路组的数量）以及调整定时器进行控制。

c）实时控制信令网中的消息和业务流量，包括实时控制路由表以及激活附加的信令链路或链路组。

7.2.2 设备安全要求

信令网主要包括SP、STP、信令链路以及信令网管理系统等。信令网设备的安全应满足设备技术规范、设备安全要求、设备入网管理相关要求。

信令网STP设备的安全应满足YD/T 1144-2001中相关的安全要求，信令链路的安全应满足YDN 089-1998、YDN 113-1999中相关的安全要求。

7.2.3 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。

7.2.4 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。

7.3 第3.1级要求

7.3.1 网络安全要求

7.3.1.1 网络拓扑安全

与7.2.1.1的要求相同。

7.3.1.2 路由安全

除满足7.2.1.2的要求之外，还应：

a）在组织信令网时一个信令点需配置的信令路由组应不大于1000，以保证电话网的正常服务。

b）在组织信令网时信令路由组的最大信令路由数量应不大于6，以保证信令传送的可靠安全性。

7.3.1.3 网络管理

7.3.1.3.1 信令网络管理通用要求

除满足7.2.1.3.1的要求之外，信令网管理中心接口数量不少于250个，支持数据链路优先权设置和紧急消息的优先传送，要求系统应具有冗余度的可靠性措施，当接口数据链路故障时不致造成系统不能工作。

7.3.1.3.2 信令网络故障管理要求

与7.2.1.3.2的要求相同。

7.3.1.3.3 信令网络结构管理要求

与7.2.1.3.3的要求相同。

7.3.1.3.4 信令网络性能管理要求

与7.2.1.3.4的要求相同。

7.3.2 设备安全要求

与7.2.2的要求相同。

7.3.3 物理环境安全要求

应满足YD/T 1755-2008《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。

7.3.4 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。

7.4 第3.2级要求

7.4.1 网络安全要求

7.4.1.1 网络拓扑安全

除满足7.3.1.1的要求之外，信令链路应优先采用地面电路，如果地面电路出现故障，在必要时选用卫星电路，以保证信令正常转接。

7.4.1.2 路由安全

与7.3.1.2的要求相同。

7.4.1.3 网络管理

7.4.1.3.1 信令网络管理通用要求

与7.3.1.3.1的要求相同。

7.4.1.3.2 信令网络故障管理要求

除满足7.3.1.3.2的要求之外，还应预防性采集和统计网络数据。

7.4.1.3.3 信令网络结构管理要求

与7.3.1.3.3的要求相同。

7.4.1.3.4 信令网络性能管理要求

除满足7.3.1.3.3的要求之外，还应能够采集测量数据，便于进行长期和短期的控制，包括告警监视、启动Q.752建议包括的某些测量以及从测量中提供网络信息，如路由利用率。

7.4.2 设备安全要求

与7.3.2的要求相同。

7.4.3 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。

7.4.4 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。

7.5 第4级要求

同第3.2级要求。

7.6 第5级要求

待补充。

8 信令网灾难备份及恢复要求

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要求

a）信令网单点故障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）信令网网络灾难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。

8.2.2 冗余路由要求

路由具备冗余能力，如SP信令点在接入到STP时应当考虑使用双路由。

8.2.3 备份数据要求

a）信令网应当对重要数据进行本地备份，包括网络配置数据（路由数据、GT数据、链路数据以及信令网管理数据等）等。

b）信令网数据备份范围、时间间隔、备份数据方式及数据恢复能力应满足相关要求。

8.2.4 人员和技术支持能力要求

有负责灾难备份及恢复的管理人员。

8.2.5 运行维护管理能力要求

a）有针对灾难备份及恢复的机房运行管理制度。

b）有针对灾难备份及恢复的介质存取、验证和转储管理制度，确保备份数据授权访问。

8.2.6 灾难恢复预案要求

应有完整的灾难恢复预案。

8.3 第3.1级要求

8.3.1 冗余系统、冗余设备及冗余链路要求

除满足8.2.1的要求之外，系统的容量和处理能力应能有一定的冗余，以便处理因灾难发生后的信令流量的变化。

8.3.2 冗余路由要求

除满足8.2.2的要求之外，还应对于重要地区的信令网路由应考虑支持负荷分担设计。

8.3.3 备份数据要求

与8.2.3的要求相同。

8.3.4 人员和技术支持能力要求

除满足8.2.4的要求之外，还应满足下列要求。

a）应有负责数据备份技术支持人员。

b）应对负责灾难备份及恢复的人员定期进行关于灾难备份及恢复的技术培训。

8.3.5 运行维护管理能力要求

除满足8.2.5的要求之外，还应满足下列要求。

a）应对灾难备份及恢复相关数据进行定期的有效性验证；

b）应有针对灾难备份及恢复的网络运行维护管理制度；

c）应有针对灾难备份及恢复的数据容灾备份管理制度；

d）应具有与外部组织保持良好的联络和协作的能力。

8.3.6 灾难恢复预案要求

除满足8.2.6的要求之外，还应满足下列要求。

a）信令网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；

b）信令网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。

8.4 第3.2级要求

8.4.1 冗余系统、冗余设备及冗余链路要求

除满足8.3.1的要求之外，还应满足：

信令网应具备一定的抗灾难以及灾难恢复能力，如具备卫星电路时，可以考虑采用卫星电路代替信令链路传送功能。

8.4.2 冗余路由要求

与8.3.2的要求相同。

8.4.3 备份数据要求

与8.3.3的要求相同。

8.4.4 人员和技术支持能力要求

与 8.3.4 的要求相同。

8.4.5 运行维护管理能力要求

与 8.3.5 的要求相同。

8.4.6 灾难恢复预案要求

与 8.3.6 的要求相同。

8.5 第 4 级要求

同第3.2级要求。

8.6 第 5 级要求

待补充。

参 考 文 献

1. GF 001-9001　中国国内电话网No.7信号方式技术规范
2. YDN 066-1997　国内No.7信令方式技术规范——运行、维护和管理部分（OMAP）（暂行规定）
3. YD/T 1125－2001　国内No.7信令方式技术规范——2Mbit/s高速信令链路
4. YD/T 1728-2008　电信网和互联网安全防护管理指南
5. YD/T 1731-2008　电信网和互联网灾难备份及恢复实施指南