YD

中华人民共和国通信行业标准

YD/T 1738-2008

增值业务网——消息网安全防护要求

Security Protection Requirements for
Value Added Service Network(Messaging 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、定义和缩略语……1
4　消息网安全防护概述……3
5　消息网定级对象和安全等级确定……5
6　消息网资产、脆弱性、威胁分析……5
7　短消息网及多媒体消息网安全等级保护要求……7
8　消息网相关信息服务单位（SP）系统安全等级保护要求……8
9　短消息网及多媒体消息网灾难备份及恢复要求……9
10　消息网相关信息服务单位（SP）系统灾难备份及恢复要求……10
参考文献……11

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 1739-2008《增值业务网——消息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、中国联合通信有限公司、中国移动通信集团公司、中国电信集团公司、中国网络通信集团公司

本标准主要起草人：盛　蕾、黄　颖、严斌峰、朱　凯、杨　恒、付　坚

增值业务网——消息网安全防护要求

1 范围

本标准规定了消息网在安全等级保护、安全风险评估、灾难备份及恢复等方面的安全防护要求。

本标准适用于公众电信网中的短消息网和多媒体消息网及与消息网相关的信息服务单位（SP）系统。

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 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 1732-2008	固定通信网安全防护要求
YD/T 1734-2008	移动通信网安全防护要求
YD/T 1752-2008	支撑网安全防护要求
YD/T 1758-2008	非核心生产单元安全防护要求
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/T 1598-2007	2GHz cdma2000数字蜂窝移动通信网多媒体邮件业务系统技术要求
YD/T 1533.1-2006	固定网多媒体消息业务技术要求 第1部分：多媒体消息中心（MMSC）设备
YD/T 1499-2006	数字蜂窝移动通信网多媒体消息业务（MMS）中心设备技术要求
YD/T1039.1-2005	900/1800MHz TDMA数字蜂窝移动通信网短消息中心设备规范 第一分册 点对点短消息业务
YD/T 1364-2005	点对点短消息网间互通设备技术要求
YD/T1248.3-2004	固定电话网短消息业务 第三部分：短消息中心技术要求
YD/T 1221.1-2002	800MHZ CDMA数字蜂窝移动通信网短消息中心设备技术要求 第一分册 点对点短消息业务

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

消息网安全等级 Security Classification of Messaging Network

消息网安全重要程度的表征。重要程度可从消息网受到破坏后，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

消息网安全等级保护 Classified Security Protection of Messaging Network

对消息网分等级实施安全保护。

3.1.3

组织 Organization

组织是由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

消息网安全风险 Security Risk of Messaging Network

人为或自然的威胁可能利用消息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

消息网安全风险评估 Security Risk Assessment of Messaging Network

指运用科学的方法和手段，系统地分析消息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，防范和化解消息网安全风险，将风险控制在可接受的水平，为最大限度地保障消息网的安全提供科学依据。

3.1.6

消息网资产 Asset of Messaging Network

消息网中具有价值的资源，是安全防护保护的对象。消息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，如消息网的消息中心设备、网关设备、网络布局等。

3.1.7

消息网资产价值 Asset Value of Messaging Network

消息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

消息网威胁 Threat of Messaging Network

可能导致对消息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。常见的消息网络威胁有光缆中断、设备节点失效、火灾、水灾等。

3.1.9

消息网脆弱性 Vulnerability of Messaging Network

脆弱性是消息网中存在的弱点、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

消息网灾难 Disaster of Messaging Network

由于各种原因，造成消息网故障或瘫痪，使消息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

消息网灾难备份 Backup for Disaster Recovery of Messaging Network

为了消息网灾难恢复而对相关网络要素进行备份的过程。

3.1.12

消息网灾难恢复 Disaster Recovery of Messaging Network

为了将消息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。

3.2 缩略语

下列缩略语适用于本标准。

CDMA	Code Division Multiple Access	码分多址
GPRS	General Packet Radio Service	通用无线分组业务
GSM	Global System of Mobile communication	全球移动通讯系统
MTBF	Mean Time Between Failures	平均故障间隔时间
PLMN	Public Land Mobile Network	公众陆地移动电话网
PSTN	Public Switched Telephone Network,	公用电话交换网
SP	Service Provider	业务提供商
TDMA	Time Division Multiple Access	时分多址
WAP	Wireless Application Protocol	无线应用协议

4 消息网安全防护概述

4.1 消息网安全防护范围

消息网按照消息类型分为短消息网和多媒体消息网。短消息网包括900/1800MHz TDMA数字蜂窝移动通信网短消息网、800MHz CDMA数字蜂窝移动通信网短消息网、固定电话网短消息网。多媒体消息网包括数字蜂窝移动通信网多媒体消息网、2GHz CDMA2000数字蜂窝移动通信网多媒体邮件业务消息网等。消息网所包括的业务为点对点短消息业务、点对点多媒体消息业务、与SP相关的点播订阅业务等。

消息网的安全防护范围包括短消息网和多媒体消息网及与消息网相关的信息服务单位（SP）系统。

短消息网的架构示意如图 1 和图 2 所示。多媒体消息网的架构示意如图 3 所示。

图 1 和图 2 为短消息网的网络架构示意图，短消息业务的完成主要涉及短消息中心和短消息网关设备。如果涉及不同运营商的点对点短消息互通时，还包括短消息互通网关。

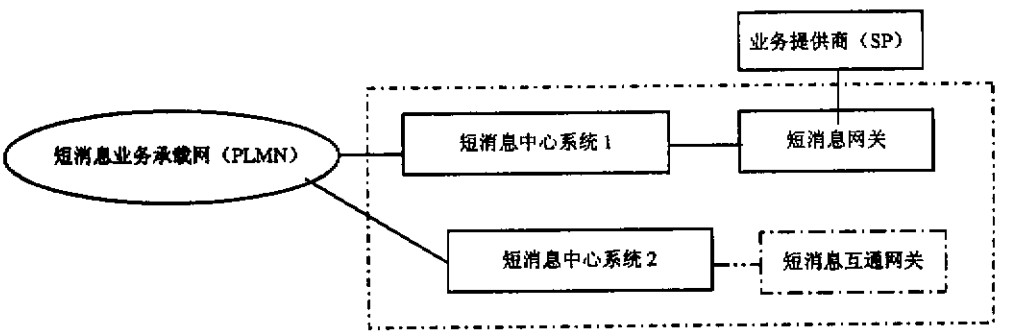

图 1 移动短消息网的网络架构示意

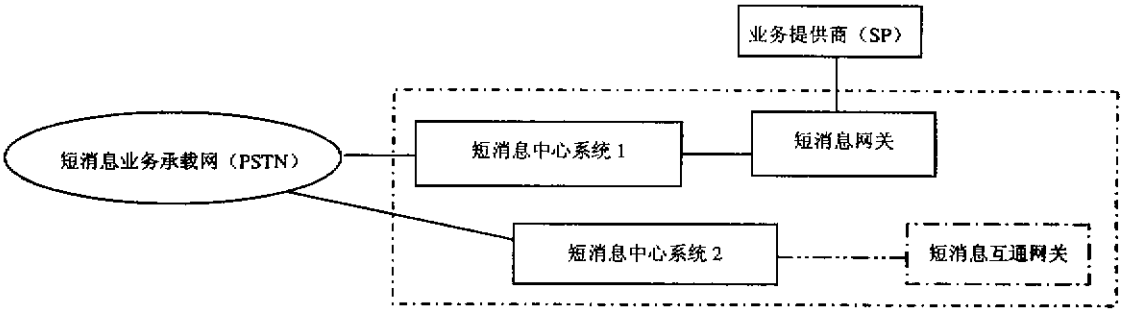

图 2　固定短消息网的网络架构示意

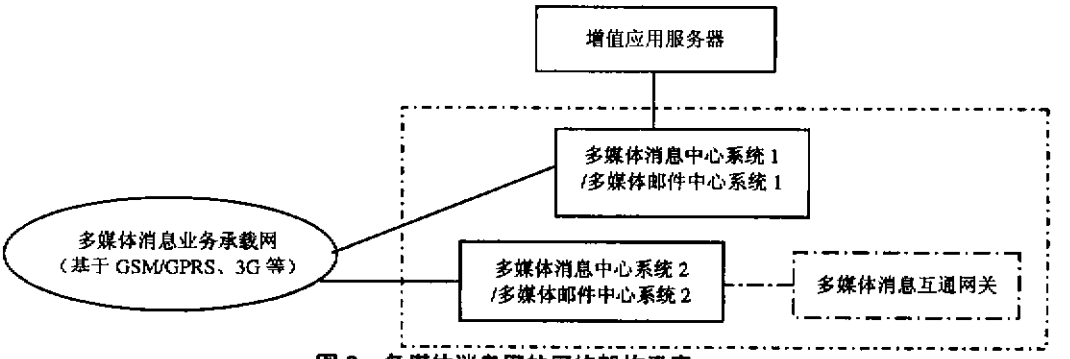

图 3　多媒体消息网的网络架构示意

短消息业务是电路域的数据业务。基于 PLMN 的短消息是以信令方式在网络中传送。基于 PSTN 的短消息是以话路为承载方式的，话路的建立与信令网相关。为配合短消息业务平台提供短消息服务，需要各种承载网设备的支持，还要和现网中的计费系统、网管系统等互联。核心网络的安全防护要求参见对应的 YD/T 1734-2008《移动通信网安全防护要求》及 YD/T 1732-2008《固定通信网安全防护要求》。计费和网管部分的安全防护要求参见 YD/T 1752-2008《支撑网安全防护要求》。

移动网内的消息中心之间是通过信令网连接的。固定网内的消息中心是通过两个或两个以上的网关之间的 IP 链路进行连接的。互通网关之间是以 IP 链路连接的。消息中心到消息网关都是 IP 链路。

图 3 为多媒体消息网的网络架构示意图。多媒体消息业务完成主要涉及多媒体消息中心系统/多媒体邮件中心系统，如果涉及不同运营商多媒体消息互通，还包括多媒体消息互通网关。多媒体消息中心系统之间通过 IP 链路连接。

多媒体消息业务是一种分组数据业务，为配合多媒体消息平台提供多媒体消息服务，需要各种承载网设备的支持，还要和现网中的计费系统、网管系统等互联。核心网络的安全防护要求参见对应的 YD/T 1734-2008 移动通信网安全防护要求及 YD/T 1732-2008《固定通信网安全防护要求》。计费和网管部分的安全防护要求参见 YD/T 1752-2008《支撑网安全防护要求》。

4.2　消息网安全防护内容

根据电信网和互联网安全防护体系的要求，将消息网安全防护内容分为安全风险评估、安全等级保护、灾难备份及恢复等3个部分：

——安全等级保护

主要包括定级对象和安全等级的确定、业务安全、网络安全、设备安全、物理环境安全、管理安全等。

——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。本标准仅对消息网进行资产分析、脆弱性分析、威胁分析，在消息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》。

——灾难备份及恢复

主要包括灾难备份及恢复等级确定、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等。

5 消息网定级对象和安全等级确定

短消息网及多媒体消息网定级对象应为以一个消息中心系统为最小划分单元的网络（一个消息中心的本地业务划分区域可能是一个省/市或多个省）。

消息网相关的信息服务单位（SP）系统定级对象应以一个服务系统为最小划分单元的网络。

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》中确定网络安全等级的方法（附录A）对消息网定级，即对短消息网、多媒体消息网、消息网相关的信息服务单位（SP）系统根据社会影响力、所提供服务的重要性、规模和服务范围分别定级，权重 α、β、γ 可根据具体情况进行调节。

6 消息网资产、脆弱性、威胁分析

6.1 资产分析

消息网安全风险评估的资产至少应包括设备硬件、设备软件、重要数据、提供的服务、文档、人员等，如表1所示。

表1 资产列表

分 类	示 例
设备硬件	短消息网的资产包括短消息中心、短消息网关、短消息互通网关等； 多媒体消息网的资产包括多媒体消息中心/多媒体邮件中心、多媒体消息互通网关等； 消息网相关的信息服务单位（SP）系统包括各种服务器等； 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：操作系统、各种数据库软件等
重要数据	保存在设备上的各种重要数据，包括计费数据、网络配置数据、管理员操作维护记录等
服务/业务	消息网提供的短消息业务和多媒体消息业务
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、网络或业务的研发人员等

6.2 脆弱性分析

消息网的脆弱性可以从技术脆弱性和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	业务/应用	网络和设备的处理能力不够而导致在突发业务量高时无法正常提供消息网业务，业务数据的保密性不够，重要数据未及时进行本地和异地备份
	网络	网络拓扑设计不合理，网络节点设备、路由配置不合理或不够，消息网设备之间的 IP 连接带来的不安全性，网络防病毒和防攻击能力不够，外部和内部的访问控制不够等
	设备（含操作系统和数据库）	账号和口令保护不够，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、设备补丁安装不及时、设备防病毒和防攻击能力不够，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
	物理环境	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、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

6.3 威胁分析

消息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		设备自身的软件、硬件故障，系统本身设计缺陷或软件 Bug，节假日或其他原因的高话务冲击等； 外部连接设备的恶意攻击； 无法管理的用户设备的接入以及来自终端和 SP 的内容管理等； 需要在网络中实施监管和监测的技术手段
环境威胁	物理环境	断电、静电、灰尘、潮湿、温度、电磁干扰等，意外事故或通讯线路方面的故障
	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； 外部人员利用恶意代码和病毒对网络或系统进行攻击； 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 短消息网及多媒体消息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 业务安全要求

a） 所提供的业务应尽可能不因系统引入其他新业务、业务升级或者系统升级而中断；

b） 应当具备对相关SP业务的业务要求，在SP接入前进行相应的业务验证；

c） 在办理SP接入服务业务之前，应对SP资格进行审查（例如：无短信息服务业务经营许可证单位擅自通过网站及接入合作方式为用户提供短信）。

7.2.2 网络安全要求

a） 网络拓扑设计中，应当充分考虑传输链路（IP链路）连接的冗余设置，故障时应能快速恢复；

b） 应有安全的管理，包括网内设备认证和鉴权机制管理、设备的登录有账号和密码管理、计费管理等；

c） 网内设备之间连接时、网内设备与网外设备之间连接时，应支持相互安全认证功能；

d） 在网络与互联网边界处应采取防火墙等安全措施。

7.2.3 设备安全要求

短消息网主要包括短消息中心设备、短消息网关设备、短消息互通网关设备。多媒体消息网设备包括多媒体消息中心设备/多媒体邮件中心设备、多媒体消息互联网关设备。以上提到的主要设备的安全应满足设备入网管理规定。

短消息网主要设备应满足：

a） 900/1800MHz TDMA数字蜂窝移动通信网短消息中心设备的安全，应满足YD/T 1039.1-2005中的安全相关要求；

b） 800MHz CDMA数字蜂窝移动通信网短消息中心设备的安全，应满足YD/T 1221.1-2002中的安全相关要求；

c） 固定网短消息中心的安全，应满足YD/T 1248.3-2004中的安全相关要求；

d） 点对点短消息网间互通设备的安全，应满足YD/T 1364-2005中的安全相关要求。

多媒体消息网主要设备应满足：

a） 数字蜂窝移动通信网多媒体消息中心设备的安全，应满足YD/T 1499-2006中的安全相关要求；

b） 2GHz CDMA2000数字蜂窝移动通信网多媒体邮件中心设备的安全，应满足YD/T 1598-2007中的安全相关要求；

c） 固定网多媒体消息中心的安全，应满足YD/T 1533.1-2006中安全相关要求。

7.2.4 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。

7.2.5 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 业务安全要求

除满足7.2.1的要求之外，还应满足：

a） 对SP应当提供统一的接入入口，对SP进行统一的接入管理；

b） 应有对SP服务的监督管理机制，对SP的业务提供情况能够进行监控，具备相应的技术手段能够及时对违规的SP行为进行制止；

c） 对SP应有业务过滤机制（例如：应对短信内容进行审核，防止散布不健康或虚假信息）。

7.3.2 网络安全要求

除满足7.2.2的要求之外，还应满足：

a） 设备之间的连接认证应采用带有加密算法的认证方式；

b） 网络应有对恶意消息群发的监视和防范措施，包括点对点及点对SP的消息；

c） 网络内部核心设备包括消息中心及各种网关应当采取适当的防病毒和攻击措施，例如：防火墙等；

d） 网络结构应能够避免不明设备接入，例如：采用专网或者虚拟专网方式；

e） 系统重要数据（如计费数据）应有可靠的备份功能；

f） 应有对业务数据和重要数据的访问进行权限限制；

g） 在与SP等业务提供设备连接时，网络应有对SP设备接入的安全措施（包括技术和管理），如应有对SP设备的接入认证等。

7.3.3 设备安全要求

同 7.2.3 的要求。

7.3.4 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。

7.3.5 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

同第 3.1 级要求。

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 消息网相关信息服务单位（SP）系统安全等级保护要求

8.1 第 1 级要求

不作要求。

8.2 第 2 级要求

应满足YD/T 1758-2008《非核心生产单元安全防护要求》中非核心生产单元网安全等级保护要求第2级的安全要求。

8.3 第 3.1 级要求

应满足YD/T 1758-2008《非核心生产单元安全防护要求》中非核心生产单元网安全等级保护要求第3.1级的安全要求。

8.4 第 3.2 级要求

同第 3.1 级要求。

8.5 第4级要求

同第3.2级要求。

8.6 第5级要求

待补充。

9 短消息网及多媒体消息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》，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） 网络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

应有网络路由设计的冗余性。

9.3.3 备份数据要求

a） 关键数据（如计费数据、用户数据、网络配置数据、管理员操作维护记录）应有本地数据备份；

b） 关键数据的备份范围和时间间隔、采取的备份方式、数据恢复能力应符合相关要求。

9.3.4 人员和技术支持能力要求

应有负责灾难备份及恢复的管理人员。

9.3.5 运行维护管理能力要求

a） 应有针对灾难备份及恢复的机房运行管理制度；

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

9.3.6 灾难恢复预案要求

应有完整的灾难恢复预案。

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

除满足9.3.1的要求之外，还应满足：

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业务流量的变化。

9.4.2 冗余路由要求

同9.3.2的要求。

9.4.3 备份数据要求

同9.3.3的要求。

9.4.4 人员和技术支持能力要求

除满足9.3.4的要求之外，还应满足：

a） 应有负责灾难备份及恢复的技术人员；

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。

9.4.5 运行维护管理能力要求

除满足9.3.5的要求之外，还应满足：

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设备和网络运行管理制度；

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。

9.4.6 灾难恢复预案要求

除满足9.3.6的要求之外，还应满足：

a） 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） 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。

9.5 第3.2级要求

同第3.1级要求。

9.6 第4级要求

同第3.2级要求。

9.7 第5级要求

待补充。

10 消息网相关信息服务单位（SP）系统灾难备份及恢复要求

10.1 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》，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。

10.2 第1级要求

不作要求。

10.3 第2级要求

应满足YD/T 1758-2008《非核心生产单元安全防护要求》中非核心生产单元灾难备份及恢复要求第2级的安全要求。

10.4 第3.1级要求

应满足YD/T 1758-2008《非核心生产单元安全防护要求》中非核心生产单元灾难备份及恢复要求第3.1级的安全要求。

10.5 第3.2级要求

同第3.1级要求。

10.6 第4级要求

同第3.2级要求。

10.7 第5级要求

待补充。

参 考 文 献

1. 国家标准　　信息安全技术信息系统安全等级保护基本要求
2. YD/T 1639-2007　　短消息中心设备和短消息网关设备的安全要求和测试方法