YD

中华人民共和国通信行业标准

YD/T 1734-2008

移动通信网安全防护要求

Security Protection Requirements for
Mobile Communication 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 1735-2008《移动通信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、中国移动通信集团公司、中国联合通信有限公司、中国电信集团公司

本标准主要起草人：袁　琦、王自亮、刘申建、杨　恒

移动通信网安全防护要求

1 范围

本标准规定了移动通信网中的GSM/GPRS/WCDMA/TD-SCDMA网和cdma 2000 1x/HRPD网在风险分析、安全等级保护、灾难备份及恢复等方面的安全防护要求，其中WCDMA/TD-SCDMA移动通信网主要对R99版本、R4版本规定了安全防护要求。

本标准适用于公众电信网中的移动通信网。

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 5098-2005 通信局（站）防雷与接地工程设计规范

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 1731-2008 电信网和互联网灾难备份及恢复实施指南

YD/T 1744-2008 传送网安全防护要求

YD/T 1746-2008 IP 承载网安全防护要求

YD/T 1748-2008 信令网安全防护要求

YD/T 1750-2008 同步网安全防护要求

YD/T 1752-2008 支撑网安全防护要求

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

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

移动通信网安全等级 Security Classification of MOBILE Communication Network

移动通信网安全重要程度的表征。重要程度可从移动通信网受到破坏后，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

移动通信网安全等级保护 Classified Security Protection of Mobile Communication Network

对移动通信网分等级实施安全保护。

3.1.3

组织 Organization

组织是由移动通信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

移动通信网安全风险 Security Risk of Mobile Communication Network

人为或自然的威胁可能利用移动通信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

移动通信网安全风险评估 Security Risk Assessment of Mobile Communication Network

指运用科学的方法和手段，系统地分析移动通信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，防范和化解移动通信网安全风险，将风险控制在可接受的水平，为最大限度地保障固定通信网的安全提供科学依据。

3.1.6

移动通信网资产 Asset of Mobile Communication Network

移动通信网中具有价值的资源是安全防护、保护的对象。移动通信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，包括频率和码号、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，如移动通信网节点设备、移动通信网的光缆线路、移动通信网的网络布局等。

3.1.7

移动通信网资产价值 Asset Value of Mobile Communication Network

移动通信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

移动通信网威胁 Threat of Mobile Communication Network

可能导致对移动通信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。常见的移动通信网络威胁有光缆中断、设备节点失效、火灾、水灾等。

3.1.9

移动通信网脆弱性 Vulnerability of Mobile Communication Network

脆弱性是移动通信网中存在的弱点、缺陷与不足，不直接对资产造成危害，但可能被威胁利用从而危及资产的安全。

3.1.10

移动通信网灾难 Disaster of Mobile Communication Network

由于各种原因造成移动通信网故障或瘫痪，使移动通信网支持的业务功能停顿或服务水平不可接受、达到特定时间的突发性事件。

3.1.11

移动通信网灾难备份 Backup for Disaster Recovery of Mobile Communication Network

为了移动通信网灾难恢复而对相关网络要素进行备份的过程。

3.1.12

移动通信网灾难恢复 Disaster Recovery of Mobile Communication Network

为了将移动通信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

移动通信网相关系统 Systems of Mobile Communication Network

组成移动通信网的相关系统，包括传送网、IP承载网、信令网、同步网、支撑网等。其中，传送网包括光缆、波分、SDH、微波、卫星等，支撑网则包括业务支撑和网管系统。

3.2 缩略语

下列缩略语适用于本标准。

AAA	Authentication, Authorization, and Accounting	认证、授权、计费
AC	AuthenticationCenter	鉴权中心
AUC	Authentication Center	鉴权中心
BG	Border Gateway	边界网关
BSS	BaseStation Subsystem	基站子系统
CG	Charging Gateway	计费网关
DNS	Domain Name Server	域名服务器
FA	Foreign Agent	拜访代理
GGSN	Gateway GPRS Support Node	网关 GPRS 支持节点
GSM	Global System for Mobile Communication	全球移动通信系统
GPRS	General Packet Radio Service	通用分组无线业务
HA	Home Agent	归属代理
HRPD	High Rate Packet Data	高速分组数据
IMSI	International Mobile Subscriber Identification	国际移动用户识别码
MSC	Mobile Switch Center	移动交换中心
MS	Mobile Station	移动台
MGW	Media Gateway	媒体网关
MSC server	Mobile Switching Center Server	移动交换中心服务器
PDSN	Packet Data Serving Node	分组数据业务节点
PCF	Packet Control Function	分组控制功能
RNC	Radio Network Controller	无线网络控制器
SGSN	Serving GPRS Support Node	服务 GPRS 支持节点
TD-SCDMA	Time Division Synchronous Code Division Multiple Access	时分同步码分多址
VLR	Visitor Location Register	拜访位置寄存器
WCDMA	Wideband Code Division Multiple Access	宽带码分多址

4 移动通信网安全防护概述

4.1 移动通信网安全防护范围

移动通信网是通过无线接入技术为公众用户提供移动通信业务的网络。移动通信网的安全防护范畴包括 GSM/GPRS/WCDMA/TD-SCDMA 网、cdma 2000 1x/HRPD 网以及与这些网络运行和业务提供相关的传送网、IP 承载网、信令网、同步网、支撑网等相关系统，如图 1 所示。

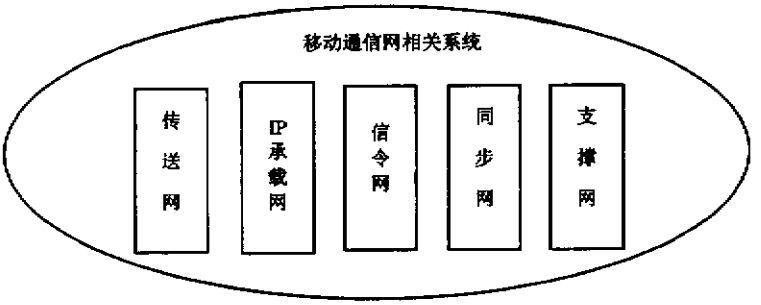

图 1 移动通信网安全防护涉及的相关系统

本标准仅对移动通信网中的 GSM/GPRS/WCDMA/TD-SCDMA 网和 cdma 2000 1x/HRPD 网提出安全防护要求，传送网安全防护的具体要求参见《传送网安全防护要求》，IP 承载网安全防护的具体要求参见《IP 承载网安全防护要求》，信令网安全防护的具体要求参见《信令网安全防护要求》，同步网安全防护的具体要求参见《同步网安全防护要求》，支撑网安全防护的具体要求参见《支撑网安全防护要求》。

4.2 移动通信网安全防护内容

根据电信网和互联网安全防护体系的要求，将移动通信网安全防护内容分为安全风险评估、安全等级保护、灾难备份及恢复等三个部分，本标准规定了移动通信网中网的安全防护内容。

— 移动通信网安全风险评估。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。本标准仅对移动通信网进行资产分析、脆弱性分析、威胁分析，在移动通信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《电信网和互联网安全风险评估实施指南》。

— 移动通信网安全等级保护。主要包括定级对象和安全等级确定、业务安全、网络安全、设备安全、物理环境安全、管理安全等。

— 移动通信网灾难备份及恢复。主要包括灾难备份及恢复等级确定和针对灾难备份及恢复各资源要素的具体实施等。

5 移动通信网安全定级对象和安全等级确定

对 GSM/GPRS/WCDMA/TD-SCDMA 网进行安全定级时，GSM 网的定级对象可为本地网、省内长途网、省际长途网（含国际长途网）。GPRS 网定级对象可为省网、国际部分。WCDMA/TD-SCDMA 网定级对象分为电路域和分组域。电路域定级对象可为本地网、省内长途网、省际长途网（含国际长途网）；分组域定级对象可为省网、国际部分。

对 cdma 2000 1x/HRPD 网进行安全定级时，cdma 2000 1x 定级对象可分为电路域和分组域。电路域可为本地网、省内长途网、省际长途网（含国际长途网），分组域可为省网、国际部分。cdma 2000 1x HRPD 网定级对象可为省网、国际部分。

网络和业务运营商应根据《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），对移动通信网进行定级，即对移动通信网划分的单元、电信智能卡根据社会影响力、所提供服务的重要性、服务用户数的大小分别定级，权重α、β、γ可根据具体网络情况进行调节。

6 移动通信网资产、脆弱性、威胁分析

6.1 资产分析

移动通信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，见表1。

表1 资产列表

分 类	示 例
频率和码号资源	频段、频点、码号
电信智能卡	SIM、USIM、UIM、RUIM
设备硬件	GSM网络设备：BTS、BSC、MSC、VLR、HLR、AUC等； GPRS网络设备：BTS、BSC、PCU、SGSN、GGSN、VLR、HLR、AUC、BG、CG等； 基于R99的WCDMA/TD-SCDMA网络设备：Node B、RNC、MSC、SGSN、GGSN、VLR、HLR、AUC、BG、CG等； 基于R4的WCDMA/TD-SCDMA网络设备：Node B、RNC、MGW、MSC Server、SGSN、GGSN、VLR、HLR、AUC、BG、CG等； cdma 2000 1x网络设备：BTS、BSC、PCF 、MSC、VLR、HLR、AC、PDSN、AAA、HA、FA等 HRPD网络设备：BTS、BSC、PCF、AN AAA、PDSN、AAA、HA、FA等； 物理环境设备：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； 链路； 操作维护系统
设备软件	设备的系统软件：操作系统、各种数据库软件等； 系统控制软件、协议软件； 操作维护系统软件
重要数据	支撑移动通信网运行的的各种重要数据，包括用户数据、计费数据（指话单数据）、网络配置数据、管理员操作维护记录等
服务/业务	移动通信网提供的各种业务：基本通话、各种补充业务等
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	网络节点和链路之间的连接

6.2 脆弱性分析

移动通信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导致在突发话务量高时业务提供不连续、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，通信安全保护不充分，网络存在安全漏洞，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

移动通信网的威胁根据来源可分为网络设备威胁、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
网络设备威胁		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
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 移动通信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）在业务开始时对用户进行认证，防止未授权用户获得业务接入。

b）在网络发生拥塞或设备发生单点故障时，应保证业务的连续性。

c）应能够记录维护人员对网络进行的发布、修改、删除等操作行为，并且可以按时间、操作方式、操作人员来查询。

7.2.2 网络安全要求

7.2.2.1 通用网络安全要求

7.2.2.1.1 网络拓扑结构

a）网络设备处理能力应具备冗余空间，满足流量高负荷时需求，不能由于设备配置不够而导致网络全部或者局部瘫痪。

b）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。

7.2.2.2 GSM网络安全要求

a）对接入的用户身份发起鉴权认证，验证用户身份的合法性，保证授权用户能够接入网络。

b）应提供用户身份的保密措施，在用户初次接入网络的时候IMSI才被发送，仅在无线信道上发送移动用户相应的TMSI。

c）应在MS和BTS之间提供数据的加密机制，保证数据在无线链路上的传输安全（在国家未对算法作出具体规定之前，对此功能不做要求）。

7.2.2.3 GPRS网络安全要求

a）对接入的用户身份发起鉴权认证，验证用户身份的合法性，保证授权用户能够接入网络。

b）应提供用户身份的保密措施。在用户初次接入网络的时候IMSI才被发送，仅在无线信道上发送移动用户相应的TMSI。

c） 应在MS和SGSN之间提供用户数据的加密机制，保证用户数据在链路上的传输安全（在国家未对算法作出具体规定之前，对此功能不做要求）。

7.2.2.4 WCDMA/TD-SCDMA网络安全要求

a）支持双向鉴权认证功能。对接入的用户身份发起鉴权认证，验证用户身份的合法性，保证授权用户能够接入网络；用户对接入的网络发起鉴权认证，验证网络的合法性，保证用户能够接入合法网络。

b）应提供用户身份的保密措施，在用户初次接入网络的时候IMSI才被发送，仅在无线信道上发送移动用户相应的TMSI。

c）应支持用户和网络之间的密钥协商机制。

d）应在MS和RNC之间提供数据的加密机制，保证数据在链路上的传输安全（在国家未对算法作出具体规定之前，对此功能不做要求）。

e）支持对层三RRC消息的完整性保护，用于维护信令的完整性。

7.2.2.5 cdma 2000 1x网络安全要求

a）对接入的用户身份发起鉴权认证，验证用户身份的合法性，保证授权用户能够接入网络。

b）在空中接口的层三提供鉴权和加密的服务。

c）应在MS和基站系统之间提供数据的加密机制，保证数据在无线链路上的传输安全（在国家未对算法作出具体规定之前，对此功能不做要求）。

7.2.2.6 cdma 2000 1x HRPD 网络安全要求

a）应支持AN AAA对移动台进行无线接入网的认证和授权。

b）对接入的用户身份发起鉴权认证，验证用户身份的合法性，保证授权用户能够接入网络。

c）应支持空中接口安全层的密钥交换、鉴权和加密服务，安全层使用密钥交换协议、鉴权协议、加密协议和安全协议提供的这些功能。

d）应在MS和基站系统之间提供数据的加密机制，保证数据在无线链路上的传输安全（在国家未对算法作出具体规定之前，对此功能不做要求）。

7.2.3 设备安全要求

7.2.3.1 GSM/GPRS/WCDMA/TD-SCDMA 网

GSM/GPRS/WCDMA/TD-SCDMA网设备安全应满足设备技术规范、设备入网管理相关要求。

7.2.3.2 cdma 2000 1x/HRPD 网

cdma 2000 1x/HRPD网设备安全应满足设备技术规范、设备入网管理相关要求。

7.2.4 物理环境安全要求

7.2.4.1 机房、办公场地物理环境安全

应满足《电信网和互联网物理环境安全等级保护要求》中第2级的安全要求。

7.2.4.2 室外无线接入设备场地物理环境

7.2.4.2.1 物理位置的选择

a）室外无线接入设备场地应选择在具有防震、防风和防雨等能力的建筑内。

b）室外无线接入设备场地的承重能力应满足位置选择要求。

7.2.4.2.2 防盗窃和防破坏

a）应将主要设备放置在物理受限的范围内。

b）应对设备或主要部件进行固定，并设置明显的不易除去的标记。

c）应将通信线缆铺设在隐蔽处，如铺设在地下或管道中等。

7.2.4.2.3 防雷击

a）室外无线接入设备建筑应设置避雷装置。

b）应设置交流电源地线。

c）应满足YD 5098-2005中 “3 通用规定”、“4 综合通信大楼的防雷与接地”、“5 有线通信局（站）的防雷与接地”的要求。

7.2.4.2.4 防火

应设置灭火设备，并保持灭火设备的良好状态。

7.2.4.2.5 防水和防潮

a）应采取措施防止雨水通过屋顶和墙壁渗透。

b）应采取措施防止室内水蒸气结露和地下积水的转移与渗透。

7.2.4.2.6 温湿度控制

应设置温、湿度自动调节设施，使室外无线接入设备场地温、湿度的变化在设备运行所允许的范围之内。

7.2.4.2.7 防尘

应采取必要的对室外无线接入设备场地的防尘措施，出入室外无线接入设备场地要求使用鞋套，有专人定期对室外无线接入设备场地进行除尘工作。

7.2.4.2.8 电力供应

a）设备供电应与其他供电分开。

b）应设置稳压器和过电压防护设备。

c）应提供短期的备用电力供应（如：UPS设备）。

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

应满足8.2.1的要求。

7.3.2 网络安全要求

7.3.2.1 通用网络安全要求

7.3.2.1.1 网络拓扑结构

除满足8.2.2.1.1要求外，还需满足如下要求。

a）在组网设计时，对重要设备要选择实行双归属配置、1＋1互为主备或N＋1冗余备份等方案；

b）核心网络重要的节点设备之间采用负荷分担方式选择路由，设置迂回路由或备用路由。

7.3.2.1.2 用户数据存储

a）应保证重要设备中用户数据和参数存储的安全性。在线接入应依操作者的等级，控制不同等级的接入。

b）重要设备存储的用户数据和参数应保证有可靠的备份功能。

7.3.2.1.3 计费信息安全

应保证计费信息的安全，支持提供可靠的话单备份、转储手段，以进行话单数据的可靠备份。

7.3.2.2 GSM网络安全要求

应满足8.2.2.2的要求。

7.3.2.3 GPRS网络安全要求

除满足8.2.2.3要求外，还需：

a）在GGSN与外部IP网络之间应设置防火墙进行隔离，禁止外部网络对内部网络的配置操作，并严格管理内部网络数据。

b）不同GPRS网之间互连时应在BG处设置必要的安全机制。

7.3.2.4 WCDMA/TD-SCDMA网络安全要求

除满足8.2.2.4要求外，还需：

a）在分组域与外部IP网络之间应设置防火墙进行隔离，禁止外部网络对内部网络的配置操作，并

严格管理内部网络数据。

b）不同分组域之间互连时应在 BG 处设置必要的安全机制。

7.3.2.5 cdma 2000 1x 网络安全要求

除满足8.2.2.5要求外，还需在PDSN与外部IP网络之间设置防火墙进行隔离，禁止外部网络对内部网络的配置操作，并严格管理内部网络数据。

7.3.2.6 cdma 2000 1x HRPD 网络安全要求

除满足8.2.2.6要求外，还需：

在PDSN与外部IP网络之间设置防火墙进行隔离，禁止外部网络对内部网络的配置操作，并严格管理内部网络数据。

7.3.3 设备安全要求

应满足8.2.3的要求。

7.3.4 物理环境安全要求

7.3.4.1 机房、办公场地物理环境安全

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

7.3.4.2 室外无线接入设备场地物理环境

7.3.4.2.1 物理位置的选择

除满足8.2.4.2.1要求外，还需：

a）室外无线接入设备场地应当避开强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区。

b）室外无线接入设备的接地方式、接地线布放、接地电阻应满足要求。

7.3.4.2.2 防盗窃和防破坏

除满足8.2.4.2.2要求外，还需：

a）应利用光、电等技术设置室外无线接入设备场地的防盗报警系统，以防进入室外无线接入设备场地的盗窃和破坏行为。

b）应对室外无线接入设备场地设置监控报警系统。

7.3.4.2.3 防雷击

应满足8.2.4.2.3的要求。

7.3.4.2.4 防火

应满足8.2.4.2.4的要求。

7.3.4.2.5 防水和防潮

应满足8.2.4.2.5的要求。

7.3.4.2.6 温湿度控制

应满足8.2.4.2.6的要求。

7.3.4.2.7 防尘

应满足8.2.4.2.7的要求。

7.3.4.2.8 电力供应

除满足8.2.4.2.8要求外，还需：

a）尽可能设置冗余或并行的电力电缆线路，或采用其他手段保证不间断供电。

b）应建立备用供电系统（如备用发电机），以备常用供电系统停电时启用。

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

7.4.1 业务安全要求

应满足8.3.1的要求。

7.4.2 网络安全要求

应满足8.3.2的要求。

7.4.3 设备安全要求

应满足8.3.3的要求。

7.4.4 物理环境安全要求

7.4.4.1 机房、办公场地物理环境安全

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

7.4.4.2 室外无线接入设备场地物理环境

应满足8.3.4.2的要求。

7.4.5 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3.2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 移动通信网灾难备份及恢复要求

8.1 概述

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。

移动通信网的灾难恢复应根据灾难的情况，首先保证应急通信、重要通信，然后恢复一般的通信。

8.2 第1级要求

不作要求。

8.3 第2级要求

8.3.1 冗余系统、冗余设备及冗余链路要求

a）系统、设备、链路的设计部署等方面应实施冗余备份。

b）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。

c）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。

8.3.2 冗余路由要求

路由应支持冗余方式。

8.3.3 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。

8.3.4 人员和技术支持能力要求

应有负责灾难备份及恢复的机房运行管理人员。

8.3.5 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、验证和转储管理制度，确保备份数据的授权访问。

8.3.6 灾难恢复预案要求

应有完整的灾难恢复预案。

8.4 第3.1级要求

8.4.1 冗余系统、冗余设备及冗余链路要求

应满足9.3.1的要求。

8.4.2 冗余路由要求

除满足9.3.2的要求外，流量应支持负荷分担方式。

8.4.3 备份数据要求

除满足9.3.3的要求外，还需对关键数据（如计费数据、网络配置数据）在不同的地理位置进行备份。

8.4.4 人员和技术支持能力要求

除满足9.3.4的要求外，还需：

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。

8.4.5 运行维护管理能力要求

除满足9.3.5的要求外，还需满足下列要求。

a）应按介质特性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修改容灾备份管理制度，适时区分。

d）应具有与外部组织保持良好的联络和协作的能力。

8.4.6 灾难恢复预案要求

除满足9.3.6的要求外，还需满足下列要求。

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。

8.5 第3.2级要求

8.5.1 冗余系统、冗余设备及冗余链路要求

应满足9.4.1的要求。

8.5.2 冗余路由要求

应满足9.4.2的要求。

8.5.3 备份数据要求

应满足9.4.3的要求。

8.5.4 人员和技术支持能力要求

应满足9.4.4的要求。

8.5.5 运行维护管理能力要求

应满足9.4.5的要求。

8.5.6 灾难恢复预案要求

除满足9.4.6的要求外，还需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。

8.6 第4级要求

同第3.2级要求。

8.7 第5级要求

待补充。

参 考 文 献

1. GF 015.1-1995 900MHz TDMA 数字蜂窝移动通信系统设备总技术规范 第一分册 交换子系统（SSS）设备技术规范 YDN 065-1997

2. GF 015.2-1995 900MHz TDMA 数字蜂窝通信系统设备总技术规范 第二分册 基站子系统（BSS）设备技术规范

3. YD/T 1057-2000 900/1800MHz TDMA 数字蜂窝移动通信网基站子系统设备测试规范

4. YD/T 1110-2001 900/1800MHz TDMA 数字蜂窝移动通信网通用分组无线业务（GPRS）设备技术规范：基站子系统

5. YD/T 1216-2002 900/1800MHz TDMA 数字蜂窝移动通信网通用分组无线业务（GPRS）设备测试方法：基站子系统

6. YD/T 1105-2001 900/1800MHz TDMA 数字蜂窝移动通信网通用分组无线业务（GPRS）设备技术规范：交换子系统

7. YD/T 1242-2002 900/1800MHz TDMA 数字蜂窝移动通信网通用分组无线业务（GPRS）设备测试方法：交换子系统

8. YD/T 1365-2006 2GHz TD-SCDMA 数字蜂窝移动通信网 无线接入网络设备技术要求

9. YD/T 1366-2006 2GHz TD-SCDMA 数字蜂窝移动通信网 无线接入网络设备测试方法

10. YD/T 1410-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网核心网设备技术要求（第一阶段）

11. YD/T 1411-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网核心网设备测试方法（第一阶段）

12. YD/T 1505-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网媒体网关设备技术要求（第二阶段）

13. YD/T 1506-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网媒体网关设备测试方法（第二阶段）

14. YD/T 1507-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网移动软交换服务器设备技术要求（第二阶段）

15. YD/T 1508-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网移动软交换服务器设备测试方法（第二阶段）

16. YD/T 1552-2007 2GHz WCDMA 数字蜂窝移动通信网无线接入网络设备技术要求（第一阶段）

17. YD/T 1553-2007 2GHz WCDMA 数字蜂窝移动通信网无线接入网络设备测试方法（第一阶段）

18. YDC 014-2003 800MHz CDMA 1X 数字蜂窝移动通信网设备技术要求：基站子系统

19. YDC 022-2003 800MHz CDMA 1X 数字蜂窝移动通信网设备测试方法：基站子系统

20. YDC 016-2003 800MHz CDMA 1X 数字蜂窝移动通信网设备技术要求：分组设备

21. YDC 025-2003 800MHz CDMA 1X 数字蜂窝移动通信网设备测试方法：分组设备

22. YD/T 1048-2000 800MHz CDMA 数字蜂窝移动通信网设备总技术规范：交换子系统部分

23. YD/T 1049-2000 800MHz CDMA 数字蜂窝移动通信网设备总测试规范：交换子系统部分

24. YD/T 1556-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：基站子系统

25. YD/T 1573-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：基站子系统

26. YD/T 1568-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：交换子系统

27. YD/T 1569-2007 2GHz cdma2000 数字蜂窝移动通信网测试方法：交换子系统

28. YD/T 1557-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：分组设备

29. YD/T 1574-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：分组设备

30. YD/T 1561-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：高速分组数据（HRPD）（第一阶段）接入网（AN）

31. YD/T 1566-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：高速分组数据 HRPD）（第一阶段）接入网（AN）

32. YD/T 1579-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：高速分组数据（HRPD）（第一阶段）AN-AAA 设备

33. YD/T 1564-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：高速分组数据（HRPD）（第一阶段）AN-AAA 设备

34. YD/T 1677-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：高速分组数据（HRPD）（第二阶段）接入网（AN）

35. YD/T 1678-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：高速分组数据（HRPD）（第二阶段）接入网（AN）

36. YD/T 1557-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：分组设备

37. YD/T 1574-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：分组设备

38. YD/T 1729-2008 电信网和互联网安全等级保护实施指南

39. YD/T 1730-2008 电信网和互联网安全风险评估实施指南

40. YD/T 1731-2008 电信网和互联网灾难备份及恢复实施指南