YD

中华人民共和国通信行业标准

YD/T 1749-2008

信令网安全防护检测要求

Security Protection Testing 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 1748-2008《信令网安全防护要求》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

信令网安全防护检测要求

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检测要求。

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 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）

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 1755-2008 电信网和互联网物理环境安全等级保护检测要求

YD/T 1757-2008 电信网和互联网管理安全等级保护检测要求

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 Signaling Network

对信令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

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，为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 Signalling 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 Signalling 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 Signalling 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 Signalling 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害资产的安全。

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

访谈 Interview

检测人员通过与信令网有关人员（个人/群体）进行交流、讨论等活动，检查信令网安全等级保护、信令网安全风险评估和信令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。

3.1.14

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，检查信令网安全等级保护、信令网安全风险评估和信令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。

3.1.15

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，检查信令网安全等级保护、信令网安全风险评估和信令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。

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

4 信令网安全防护检测概述

4.1 信令网安全防护检测范围

信令网安全防护检测的范围包括省内信令网、省际信令网（包含国际信令网）。根据YD/T1748-2008《信令网安全防护要求》，本标准主要对信令网的安全等级保护、安全风险评估、灾难备份及恢复等提出检测要求。

4.2 信令网安全检测防护对象

信令网安全防护检测对象是省内信令网、省际信令网（含国际信令网）。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。

4.3 信令网安全防护检测内容

按照信令网安全防护检测的需要，将信令网安全防护检测分为信令网安全等级保护、信令网安全风险评估和信令网灾难备份及恢复等三个部分。

——信令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。

——信令网安全风险评估检测。主要包括安全风险评估范围、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。

——信令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。

4.4 信令网安全防护检测结果判定

信令网安全防护检测包括对信令网的安全等级保护、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，表3给出了安全等级保护子类所占的比重。

表1 测试项评分方法

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
$x \geq 4.5$	很好
$3.5 \leq x < 4.5$	较好
$2.5 \leq x < 3.5$	一般
$1.5 \leq x < 2.5$	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

5 信令网安全等级防护检测要求

5.1 第1级要求

不作要求。

5.2 第2级要求

5.2.1 网络安全

5.2.1.1 网络拓扑及路由安全

5.2.1.1.1 检测方式

访谈，检查。

5.2.1.1.2 检测对象

网络设计/验收文档，网络拓扑结构。

5.2.1.1.3 检测实施

a） 应访谈信令网管理人员，查看网络设计/验收文档，了解目前信令网的实际部署情况。

b） 应检查与信令网当前运行情况相符合的网络拓扑结构的设计是否合理。

c） 应访谈信令网管理人员，信令链路的设计、容量、配置、冗余备份是否满足要求。

d） 应访谈信令网管理人员，在组织设计信令网的过程中，当信令点达到一定数量时，是否引入信

令转接点组成分级的信令网。

e） 应检查信令网支持负荷分担的能力，包括同一链路组内链路间的负荷分担和不同链路组之间链路间的负荷分担。

f） 应访谈信令网管理人员，并查看网络设计/验收文档，检查各节点设备处理能力是否有一定的冗余度、各节点间链路路由设计是否合理，是否符合 YDN 089-1998、YDN 113-1999 技术体制中的要求。

5.2.1.2 信令网网络管理安全

5.2.1.2.1 检测方式

访谈，检查，测试。

5.2.1.2.2 检测对象

网络设计/验收文档、历史记录、信令网设备。

5.2.1.2.3 检测实施

a）应访谈网络管理员，查看网络设计/验收文档、历史记录，了解目前信令网的网络管理情况。

b）应检查信令设备是否接到了网络管理中心。

c）应检查信令网网络状态显示功能是否满足 YDN 066-1997 的 7.1 节要求。

d）应检查信令网性能管理功能、故障管理功能、运行和维护与管理当中的告警管理功能、配置管理功能、系统自身管理功能、网络结构与远程终端服务功能是否满足 YDN 066-1997 的 7.1 节要求。

5.2.2 设备安全

5.2.2.1 检测方式

访谈，检查。

5.2.2.2 检测对象

设备入网检测报告、设备入网证、安全检测报告。

5.2.2.3 检测实施

访谈相关技术支持人员和管理人员，查看相关设备的入网检测报告、设备入网证、安全检测报告、网络和业务运营商提供的其他文档，检查信令网络的 SP、STP 信令链路设备及信令网管设备是否有有效的入网检测报告、设备入网证、安全检测报告等。

5.2.3 物理环境安全

应满足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》中第2级的检测要求。

5.2.4 管理安全

应满足YD/T 1757-2008《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。

5.3 第 3.1 级要求

5.3.1 网络安全

5.3.1.1 网络拓扑及路由安全

除按照5.2.1.1的要求进行检测之外，还应按照本节内容进行检测。

5.3.1.1.1 检测方式

访谈，检查。

5.3.1.1.2 检测对象

网络设计/验收文档、网络拓扑结构。

5.3.1.1.3 检测实施

访谈信令网管理人员，查看网络设计/验收文档，检查设计的信令路由是否合理，是否符合YDN 089-1998、YDN 113-1999技术体制中的要求。

5.3.1.2 信令网网络管理安全

除按照5.2.1.2的要求进行检测之外，还应按照本节内容进行检测。

5.3.1.2.1 检测方式

访谈，检查，测试。

5.3.1.2.2 检测对象

设备入网检测报告、设备入网证、安全检测报告。

5.3.1.2.3 检测实施

a）检查信令网网管中心相关的接口配置是否满足YDN 066-1997的要求。

b）是否支持链路及数据优先级的设置，系统是否考虑了冗余度的设计。

5.3.2 设备安全

要求同5.2.2节。

5.3.3 物理环境安全

应满足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》中第3.1级的检测要求。

5.3.4 管理安全

应满足YD/T 1757-2008《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。

5.4 第3.2级要求

5.4.1 网络安全

5.4.1.1 路由拓扑及路由安全

除按照5.3.1.1的要求进行检测之外，还应按照本节内容进行检测。

5.4.1.1.1 检测方式

访谈，检查。

5.4.1.1.2 检测对象

网络设计/验收文档、网络拓扑结构。

5.4.1.1.3 检测实施

应访谈信令网管理人员，并查看网络设计/验收文档，检查是否具备冗余的卫星链路。

5.4.1.2 信令网网络管理安全

除按照5.3.1.2的要求进行检测之外，还应按照本节内容进行检测。

5.4.1.2.1 检测方式

访谈，检查，测试。

5.4.1.2.2 检测对象

设备入网检测报告、设备入网证、安全检测报告。

5.4.1.2.3 检测实施

检查信令网运行、维护与管理中的性能管理功能、故障管理功能是否满足YDN 066－1997的7.1节要求。

5.4.2 设备安全

要求同5.3.2节。

5.4.3 物理环境安全

应满足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》中第3.2级的检测要求。

5.4.4 管理安全

应满足YD/T 1757-2008《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。

5.5 第4级要求

同第3.2级要求。

5.6 第5级要求

待补充。

6 信令网安全风险评估检测要求

6.1 安全风险评估范围

6.1.1 检测方式

访谈，检查。

6.1.2 检测对象

风险评估报告。

6.1.3 检测实施

访谈风险评估负责人，询问进行信令网风险评估时，选择的风险评估范围是什么，以及风险评估范围中各个组成部分的评估权重因子如何分配。

6.2 安全风险评估内容

6.2.1 检测方式

访谈，检查。

6.2.2 检测对象

风险评估报告。

6.2.3 检测实施

a）应访谈信令网风险评估负责人、查看风险评估报告，检查信令网风险评估是否覆盖了技术安全和管理安全。

b）应访谈信令网风险评估负责人、查看风险评估报告，检查信令网风险评估中技术安全是否覆盖了业务安全、网络安全、设备安全和物理环境安全等方面。

c）应访谈信令网风险评估负责人、查看风险评估报告，检查信令网风险评估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。

6.3 安全风险评估要素

6.3.1 检测方式

访谈，检查。

6.3.2 检测对象

风险评估报告、历史记录。

6.3.3 检测实施

a）应访谈风险评估负责人，询问进行信令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，检查信令网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，询问进行信令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，检查信令网风险评估报告时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）应检查风险评估报告，查看风险评估报告中资产是否包含了网络设备（信令网包括SP、STP、信令链路以及信令网管系统，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），各种设备的系统软件，设备中的重要数据，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等。

d）应访谈风险评估负责人，询问计算信令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，检查信令网风险评估中，计算各资产的资产价值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，询问识别信令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，检查信令网风险评估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，询问识别信令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，检查信令网风险评估中技术脆弱性是否包含了业务/应用脆弱性、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、人员安全管理方面脆弱性、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，询问对信令网存在哪些威胁；查看风险评估报告，检查信令网风险评估时威胁识别是否包含了环境威胁、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，检查信令网风险评估中威胁识别是否依据了已有安全事件报告数据、检测工具检测数据和国内外同行业报告数据等多个方面。

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，检查信令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，检查信令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。

g）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，检查信令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。

6.4 安全风险评估赋值原则

6.4.1 检测方式

访谈，检查。

6.4.2 检测对象

风险评估报告。

6.4.3 检测实施

a）应访谈风险评估负责人，询问信令网风险评估时对资产的赋值遵循的原则；查看风险评估报告，检查信令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，询问信令网风险评估时对脆弱性的赋值遵循的原则；查看风险评估报告，检查信令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，询问信令网风险评估时对威胁的赋值遵循的原则；查看风险评估报告，检查信令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。

6.5 安全风险评估计算方法

6.5.1 检测方式

访谈，检查。

6.5.2 检测对象

风险评估报告。

6.5.3 检测实施

a）应访谈风险评估负责人，询问信令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，检查信令网资产价值的计算方法是否合理，是否有对于所采用计算方法的理论分析。

b）应访谈风险评估负责人，询问信令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，检查信令网风险值的计算方法是否合理，是否对于所采用计算方法的理论分析。

6.6 安全风险评估文件类型

6.6.1 检测方式

访谈，检查。

6.6.2 检测对象

风险评估方案、风险评估程序、资产识别清单、重要资产清单、脆弱性列表、威胁列表、已有安全措施确认表、风险评估报告、风险评估记录、风险处理计划。

6.6.3 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。

6.7 安全风险评估文件记录

6.7.1 检测方式

访谈，检查。

6.7.2 检测对象

风险评估方案、风险评估程序、资产识别清单、重要资产清单、脆弱性列表、威胁列表、已有安全措施确认表、风险评估报告、风险评估记录、风险处理计划等风险评估文件

6.7.3 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；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；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；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；查看风险评估文件，检查是否对于作废文件作了标识。

e）应访谈风险评估负责人，询问如何对文件进行控制；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。

7 信令网灾难备份及恢复检测要求

7.1 第1级要求

不作要求。

7.2 第2级要求

7.2.1 冗余系统、冗余设备及冗余链路

7.2.1.1 检测方式

访谈，检查。

7.2.1.2 检测对象

信令网的冗余系统、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。

7.2.1.3 检测实施

a）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，安全措施是否与设计/验收文档相符合；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。

b）应访谈安全管理人员，查看演练文档，检查信令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。

7.2.2 冗余路由

7.2.2.1 检测方式

访谈，检查。

7.2.2.2 检测对象

信令网的路由配置、设计/验收文档、演练记录、故障记录。

7.2.2.3 检测实施

应访谈安全管理人员，询问并查看信令网的路由配置，检查信令网的路由是否支持冗余方式，冗余路由是否都可以传送业务；是否与设计/验收文档相符合；检查信令网数据链路是否配备了双路由。

7.2.3 备份数据

7.2.3.1 检测方式

访谈，检查。

7.2.3.2 检测对象

信令网的数据备份介质、设计/验收文档、演练记录。

7.2.3.3 检测实施

a）应访谈安全管理人员，询问并查看数据备份介质，检查信令网中关键数据（如网络配置数据）是否有本地备份。

b）应访谈安全管理人员，询问并查看数据备份介质、演练记录，检查信令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，是否与设计/验收文档一致。

7.2.4 人员和技术支持能力

7.2.4.1 检测方式

访谈，检查。

7.2.4.2 检测对象

管理人员、历史值班记录。

7.2.4.3 检测实施

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管理人员，检查相关人员对灾难备份及恢复的技术支持能力。

7.2.5 运行维护管理能力

7.2.5.1 检测方式

访谈，检查。

7.2.5.2 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。

7.2.5.3 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。

7.2.6 灾难恢复预案

7.2.6.1 检测方式

访谈，检查。

7.2.6.2 检测对象

灾难恢复预案、设计/验收文档以及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。

7.2.6.3 检测实施

访谈安全管理人员，询问并查看灾难恢复预案，检查信令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。

7.3 第3.1级要求

7.3.1 冗余系统、冗余设备及冗余链路

除按照7.2.1的要求进行检测之外，还应按照本节内容进行检测。

7.3.1.1 检测方式

访谈，检查。

7.3.1.2 检测对象

信令网络、设计/验收文档。

7.3.1.3 检测实施

访谈安全管理人员，询问并现场检查信令网冗余系统或链路设置情况，检查是否与设计/验收文档相符合。

7.3.2 冗余路由

除按照7.2.2的要求进行检测之外，还应按照本节内容进行检测。

7.3.2.1 检测方式

访谈，检查。

7.3.2.2 检测对象

设计/验收文档、演练记录、历史记录、传送链路。

7.3.2.3 检测实施

访谈安全管理人员，询问并查看演练记录、故障记录，检查信令网是否有流量负荷分担的路由功能，是否与设计/验收文档相符合，是否发生过负荷分担能力不足影响网络业务提供的情况。

7.3.3 备份数据

应满足7.2.3的检测要求。

7.3.4 人员和技术支持能力

除按照7.2.4的要求进行检测之外，还应按照本节内容进行检测。

7.3.4.1 检测方式

访谈，检查。

7.3.4.2 检测对象

技术支持人员、历史值班记录、培训记录。

7.3.4.3 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，检查对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。

7.3.5 运行维护管理能力

除按照7.2.5的要求进行检测之外，还应按照本节内容进行检测。

7.3.5.1 检测方式

访谈，检查。

7.3.5.2 检测对象

设备和网络运行管理制度，联络和协作的记录，重要数据容灾备份管理制度。

7.3.5.3 检测实施

a）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。

b）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。

c）应访谈安全管理人员，询问并查看重要数据容灾备份管理制度，检查是否有完善的针对灾难备份及恢复的重要数据容灾备份管理制度。

d）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，检查信令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。

7.3.6 灾难恢复预案

除按照7.2.6的要求进行检测之外，还应按照本节内容进行检测。

7.3.6.1 检测方式

访谈，检查。

7.3.6.2 检测对象

灾难恢复预案、设计/验收文档以及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。

7.3.6.3 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预期目标，检查相关人员对灾难恢复预案的了解情况以及对灾难恢复预案进行实际操作的能力。

b）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。

7.4 第3.2级要求

7.4.1 冗余系统、冗余设备及冗余链路

除按照7.3.1的要求进行检测之外，还应按照本节内容进行检测。

7.4.1.1 检测方式

访谈，检查。

7.4.1.2 检测对象

信令网设计/验收文档。

7.4.1.3 检测实施

访谈安全管理人员，询问并现场检查省际信令网是否具备备份的卫星链路，保证信令网具有一定的抗灾难能力，是否与设计/验收文档相符合。

7.4.2 冗余路由

应满足7.3.2的检测要求。

7.4.3 备份数据

应满足7.3.3的检测要求。

7.4.4 人员和技术支持能力

应满足7.3.4的检测要求。

7.4.5 运行维护管理能力

应满足7.3.5的检测要求。

7.4.6 灾难恢复预案

应满足7.3.6的检测要求。

7.5 第4级要求

同第3.2级要求。

7.6 第5级要求

待补充。

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. YD/T 1125-2001　　国内No.7信令方式技术规范——2Mbit/s高速信令链路
3. YD/T 1144-2001　　国内No.7信令网信令转接点（STP）设备技术规范