YD

中华人民共和国通信行业标准

YD/T 1751-2008

同步网安全防护检测要求

Security Protection Testing Requirements for Synchronization 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 1750-2008《同步网安全防护要求》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、中国移动通信集团公司、中国网络通信集团公司

本标准主要起草人：胡昌军、李俊杰、易　武、王　路、汪建华、徐一军

同步网安全防护检测要求

1 范围

本标准规定了同步网在安全等级保护、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。

本标准适用于公众电信网中的频率同步网和时间同步网。

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 1267-2005	基于SDH传送网的同步网技术要求
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 缩略语

下列缩略语适用于本标准。

GPS	Global Positioning System	全球定位系统
LPR	Local Primary Referance	区域基准时钟
PRC	Primary Referance Clock	全国基准时钟
SDH	Synchronous Digital Heirarchy	同步数字体系
SEC	SDH Element Clock	SDH 网元时钟
SSU	Synchronization Supply Unit	同步供给单元

4 术语和定义

下列术语和定义适用于本标准。

4.1

同步网安全等级 Security Classification of Synchronization Network

同步网安全重要程度的表征。重要程度可从同步网受到破坏后，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。

4.2

同步网安全等级保护 Classified Security Protection of Synchronization Network

对同步网分等级实施安全保护。

4.3

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。

4.4

同步网安全风险 Security Risk of Synchronization Network

人为或自然的威胁可能利用同步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。

4.5

同步网安全风险评估 Security Risk Assessment of Synchronization Network

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

4.6

同步网资产 Asset of Synchronization Network

同步网中具有价值的资源，是安全防护保护的对象。同步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，如同步网的定时链路、同步节点设备等。

4.7

同步网资产价值 Asset Value of Synchronization Network

同步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。

4.8

同步网威胁 Threat of Synchronization Network

可能导致对同步网产生危害的不希望事故潜在起因，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。常见的同步网络威胁有定时链路中断、设备节点失效、火灾、水灾等等。

4.9

同步网脆弱性 Vulnerability of Synchronization Network

脆弱性是同步网中存在的弱点、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。

4.10

同步网灾难 Disaster of Synchronization Network

由于各种原因，造成同步网故障或瘫痪，使同步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。

4.11

同步网灾难备份 Backup for Disaster Recovery of Synchronization Network

为了同步网灾难恢复而对相关网络要素进行备份的过程。

4.12

同步网灾难恢复 Disaster Recovery of Synchronization Network

为了将同步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。

4.13

访谈 Interview

检测人员通过与同步网有关人员（个人/群体）进行交流、讨论等活动，检查同步网安全等级保护、同步网安全风险评估和同步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。

4.14

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，检查同步网安全等级保护、同步网安全风险评估和同步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。

4.16

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，检查同步网安全等级保护、同步网安全风险评估和同步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。

5 同步网安全防护检测概述

5.1 同步网安全防护检测范围

同步网的安全防护范畴包括构成同步网的各类同步设备以及定时链路。

安全等级保护的检测范围确定以后，风险评估的检测范围、灾难备份及恢复的检测范围应与安全等级保护的检测范围相一致。

5.2 同步网安全防护检测对象

同步网安全防护检测对象是省际骨干同步网和省内同步网。安全等级保护的检测对象确定以后，风险评估的检测范围、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 同步网安全防护检测内容

按照同步网安全防护检测的需要，将同步网安全防护检测分为同步网安全等级保护、同步网安全风险评估和同步网灾难备份及恢复等3个部分。

——同步网安全等级保护检测

主要包括应用安全检测、网络安全检测、设备安全检测、物理安全检测、管理安全检测等。

——同步网安全风险评估检测

主要包括风险评估范围、风险评估内容检测、风险评估要素检测、风险评估赋值原则检测、风险评估计算方法检测、风险评估文件类型检测和风险评估文件记录检测等。

——同步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 同步网安全防护检测结果判定

同步网安全防护检测包括对同步网的安全等级保护、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测试项，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将各测试项的评价等级换算成评分，各测试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3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3个部分的检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，应充分考虑到各测试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 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
$4.5 \leqslant x \leqslant 5$	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
20	应用安全
20	网络安全
10	设备安全
10	物理环境安全
40	管理安全

6 同步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 同步网网络安全

6.2.1.1 网络拓扑安全

6.2.1.1.1 检测方式

访谈、检查。

6.2.1.1.2 检测对象

网络设计/验收文档，网络管理文档，设备管理配置记录，运营商提供的其他文档，网络运行历史记录。

6.2.1.1.3 检测实施

a）应访谈同步网管理人员，检查网络设计/验收文档和网络管理文档，了解目前同步网的网络组织情况，确认同步网是否采取主从同步方法进行同步。

b）应访谈同步网管理人员，并检查网络设计/验收文档、网络设备管理配置记录，检查同步网的网络结构是否符合三级等级结构，检查不同等级的定时信号传送是否严格遵循从高级向较低等级或同等级间进行传送的原则。

c）应访谈同步网管理人员，并检查网络设计/验收文档、网络管理文档以及运营商提供的其他文档，检查同步网定时流向，检查同步网络中是否出现定时环和定时倒挂的现象。

d）应访谈同步网管理人员，并检查网络设计/验收文档、网络管理文档以及运营商提供的其他文档，检查时间同步设备是否按时间服务精度的不同分级设置，是否设置在频率同步网的节点时钟设备所在局。

e）应访谈同步网管理人员，并检查网络设计/验收文档、网络管理文档以及运营商提供的其他文档，检查同步网是否按一定的规律对同步区进行划分，每个同步区是否设置有两个 1 级基准时钟作为同步区的主备用定时。

f）应访谈同步网及传送网管理人员，并检查网络设计/验收文档、网络管理文档以及运营商提供的其他文档如网络运行历史记录，检查网络拓扑图与当前运行情况是否一致。

6.2.1.2 定时链路安全

6.2.1.2.1 检测方式

访谈、检查。

6.2.1.2.2 检测对象

网络设计/验收文档，网络运行历史记录。

6.2.1.2.3 检测实施

a）应访谈同步网管理人员，并检查网络运行历史记录，确定同步定时链路运行的可靠性和稳定性。

b）应访谈同步网管理人员，并检查同步网设计文件，确认同步网的主备用定时链路是否选择了不同的物理路由，保证在任何单点故障情况下主备用定时链路不会同时失效。

c）应访谈同步网管理人员，并检查同步网设计文件，检查由基于 SDH 传送网构成的定时链路是否满足 YD/T 1267-2003《基于 SDH 传送网的同步网技术要求》中第 6 节的规定。

d）应访谈同步网管理人员，并检查同步网设计文件和网络运行历史记录，检查极长定时链路的漂动累积是否满足 YD/T 1267-2003《基于 SDH 传送网的同步网技术要求》第 7.3 节的要求。

6.2.1.3 同步网定时源头的安全

6.2.1.3.1 检测方式

访谈、检查。

6.2.1.3.2 检测对象

同步网络设计/验收文档，网络管理文档，设备管理配置记录，设备运行历史记录，故障告警记录，日志文件资料。

6.2.1.3.3 检测实施

a）应访谈同步网管理人员，查看同步网设计文件，了解目前同步网中同步区的设置情况以及每个同步区中定时源头分布情况，检查每个同步区是否设置有两个不同的定时源头。

b）应访谈同步网管理人员，查看同步网设计文件和设备管理配置记录，了解目前 1 级基准时钟 LPR

的定时设置情况，是否具有4路以上的定时输入信号（包括来自卫星定位系统的信号）。

c）应访谈同步网管理人员，对于一个同步区只设置单个基准时钟LPR的情况，检查LPR是否能同时从多种卫星定位系统（如GPS，GLONASS和北斗系统）接收信号。

d）应访谈同步网管理人员，并检查LPR运行历史记录、故障告警记录和日志文件资料，检查LPR运行状态，是否出现过降质、定时倒换等异常现象。

6.2.2 同步网应用安全

6.2.2.1 局内定时分配安全

6.2.2.1.1 检测方式

访谈、检查。

6.2.2.1.2 检测对象

网络设计/验收文档，网络管理文档，网络和业务运营商提供的其他文档（包括从同步网接入定时信号的各种业务网的设计/验收文档），网络及相关设备，网络运行历史记录。

6.2.2.1.3 检测实施

a）访谈网络管理人员，并检查网络设计/验收文件、网络管理文档以及网络和业务运营商提供的其他文档（包括从同步网接入定时信号的各种业务网的设计/验收文档），对于设置有同步设备的机房，检查局内定时分配是否采用并行分配方法。

b）访谈网络管理人员，检查网络设计/验收文档、网络运行历史记录，检查各业务网元是否能够正常接收并锁定输入的定时信号。

6.2.2.2 各业务网同步安全

6.2.2.2.1 检测方式

访谈、检查。

6.2.2.2.2 检测对象

网络设计/验收文档，网络管理文档，业务网的相关文档，网络及相关设备，网络及设备运行历史记录。

6.2.2.2.3 检测实施

a）访谈同步网及业务网管理人员，并检查业务网同步设计/验收文件，确认各业务网网元设备是否具有2个以上外定时接口；

b）访谈同步网及业务网管理人员，并检查业务网同步设计/验收文件，确认各业务网网元设备是否优先选用外定时方式获取同步；

c）访谈同步网及业务网管理人员，并检查业务网同步设计/验收文件，确认各业务网网元设备是否接受来自SSU不同机框上的两路定时基准信号同步；

d）访谈同步网及业务网管理人员，并检查业务网同步设计/验收文件，确认同步设备定时输出接口的阻抗与业务网元设备外定时接口的阻抗是否一致；

e）访谈网络管理人员，检查网络运行历史记录，检查各业务网元是否设置有多路定时参考，主、备用定时是否可以自动或人工进行倒换，各业务网元在运行过程中是否出现时钟倒换或失锁的状态。

6.2.3 同步网设备安全

6.2.3.1 检测方式

访谈、检查。

6.2.3.2 检测对象

设备入网检测报告，设备入网证，安全检测报告。

6.2.3.3 检测实施

应访谈相关技术支持人员和管理人员，检查在用的同步设备（包括LPR设备、二级节点时钟设备、三级节点时钟设备、小型局站同步时钟设备、再定时设备、时间服务器等）是否有入网检测报告、设备入网证、安全检测报告等。

6.2.4 同步网物理环境安全

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。

6.2.5 同步网管理安全

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。

6.3 第3.1级要求

6.3.1 同步网网络安全

6.3.1.1 网络拓扑安全

与6.2.1.1 节检测要求相同。

6.3.1.2 定时链路安全

与6.2.1.2 节检测要求相同。

6.3.1.3 同步网定时源头的安全

与6.2.1.3 节检测要求相同。

6.3.2 同步网应用安全

与6.2.2 节检测要求相同。

6.3.3 同步网设备安全

6.3.3.1 检测方式

访谈、检查。

6.3.3.2 检测对象

设备入网检测报告，设备入网证，安全检测报告。

6.3.3.3 检测实施

应访谈相关技术支持人员和管理人员，检查在用的同步设备（LPR设备、二级节点时钟设备、三级节点时钟设备、时间服务器等）是否有入网检测报告、设备入网证、安全检测报告等。

6.3.4 同步网物理环境安全

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。

6.3.5 同步网管理安全

应满足YD/T1757-2008《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 同步网网络安全

6.4.1.1 网络拓扑安全

与6.3.1.1 节的检测要求相同。

6.4.1.2 定时链路安全

除按照6.3.1.2节的要求进行检测之外，还应按照本节内容进行检测。

6.4.1.2.1 检测方式

访谈、检查。

6.4.1.2.2 检测对象

网络设计/验收文档，网络运行历史记录。

6.4.1.2.3 检测实施

应访谈同步网及传送网管理人员，并检查同步网设计文件及网络运行历史记录，检查同步网管及传输网管把同步网定时链路作为重要的维护内容。

6.4.1.3 同步网定时源头的安全

除按照6.3.1.3节的要求进行检测之外，还应按照本节内容进行检测。

6.4.1.3.1 检测方式

访谈、检查。

6.4.1.3.2 检测对象

同步网络设计/验收文档，网络管理文档，设备管理配置记录，设备运行历史记录，故障告警记录，日志文件资料。

6.4.1.3.3 检测实施

a）应访谈同步网管理人员，检查同步网络设计/验收文档，确认组建同步网时是否将 PRC 信号作为整个同步网定时信号来源的根本保证；

b）应访谈同步网管理人员，检查同步网络设计/验收文档，确认每个同步区是否设置有两个不同的定时源头（PRC 或 LPR）；

c）应访谈同步网管理人员，检查 PRC 的配置文件，是否设置了至少三路来自铯钟或卫星定位系统的信号（至少一路铯钟信号）作为其定时输入信号；

d）应访谈同步网管理人员，并检查 PRC/LPR 运行历史记录、故障告警记录和日志文件资料，检查 PRC/LPR 运行状态，是否出现过降质、定时倒换等异常现象。

6.4.2 同步网应用安全

与6.3.2节检测要求相同。

6.4.3 同步网设备安全

6.4.3.1 检测方式

访谈、检查。

6.4.3.2 检测对象

设备入网检测报告，设备入网证，安全检测报告。

6.4.3.3 检测实施

应访谈相关技术支持人员和管理人员，检查在用的同步设备（包括PRC设备、LPR设备、二级节点时钟设备、三级节点时钟设备、时间服务器等）是否有入网检测报告、设备入网证、安全检测报告等。

6.4.4 同步网物理环境安全

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。

6.4.5 同步网管理安全

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。

6.5 第4级要求

同第3.2级要求。

6.6 第5级要求

待补充。

7 同步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，询问进行同步网风险评估时，选择的风险评估范围是什么；检查风险评估报告，查看同步网风险评估范围是否与要求一致。

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）应访谈同步网风险评估负责人、查看风险评估报告，检查同步网风险评估是否覆盖了技术安全和管理安全；

b）应访谈同步网风险评估负责人、查看风险评估报告，检查同步网风险评估中技术安全是否覆盖了应用安全、网络安全、设备安全和物理环境安全等方面；

c）应访谈同步网风险评估负责人、查看风险评估报告，检查同步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。

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。

7.3.3 检测实施

a）应访谈风险评估负责人，询问进行同步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，检查同步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，询问进行同步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，检查同步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）应访谈风险评估负责人，询问进行同步网风险评估时评估了哪些资产；查看风险评估报告，检查同步网风险评估时的资产是否包含了网络设备（包括一级基准时钟设备、二级节点时钟设备、三级节点时钟设备、小型局站同步时钟设备、再定时设备和时间服务器）,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、系统控制软件、协议软件、操作维护系统软件，支撑同步网运行的各种重要数据，网络提供的各类业务，网络拓扑、设备维护人员、各种管理规定和设备文档、码号资源等。

d）应访谈风险评估负责人，询问计算同步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，检查同步网风险评估中，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，询问识别了同步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，检查同步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，询问识别了同步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，检查同步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，询问对同步网存在哪些威胁；查看风险评估报告，检查同步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，检查同步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，检查同步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，检查同步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，检查同步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，询问同步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，检查看同步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，询问同步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，检查看同步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，询问同步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，检查看同步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，询问同步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，检查同步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，询问同步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，检查同步网风险值的计算方法是否合理，是否具有对于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。

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。

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；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 同步网灾难备份及恢复检测要求

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。

8.2 第1级要求

不作要求。

8.3 第2级要求

8.3.1 同步网冗余系统、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

同步网络，设计/验收文档。

8.3.1.3 检测实施

a）应检查同步网的冗余设备系统、设备及链路，参看其是否与设计一致。

b）应检查同步网的抗灾难以及灾难恢复能力设计/验收文档，查看同步网的抗灾难以及灾难恢复能力，如出现灾难以后采用来自不同物理路由的主备用定时链路提供路由保护，以及采用来自不同卫星定位系统的定时信号提供定时源头的保护等。

c）应检查演练文档，查看同步网网络灾难演练恢复时间是否满足演练的相关要求。

8.3.2 同步网冗余路由

8.3.2.1 检测方式

访谈、检查。

8.3.2.2 检测对象

设计/验收文档，演练记录，历史记录，传送链路。

8.3.2.3 检测实施

a）应访谈安全管理人员，检查设计/验收文档和网络运行历史记录，检查一级基准时钟 LPR 到 2 级和 3 级节点时钟的定时链路是否采用了冗余路由，并检查其与设计是否一致。

b）应访谈安全管理人员，检查网络运行历史记录，确认同步网在进行冗余保护时，定时信号输出的短时相位跳变是否满足相关标准要求。

8.3.3 同步网备份数据

8.3.3.1 检测方式

访谈、检查。

8.3.3.2 检测对象

数据备份服务器，设计/验收文档，演练历史记录。

8.3.3.3 检测实施

a）应访谈同步网安全管理人员，检查设计/验收文档，询问是否支持关键数据（如定时配置、定时性能监视数据等）在本地进行定期备份。

b）应检查同步网数据备份服务器，查看其与设计文档是否一致。

c）应检查演练历史记录，查看同步网数据备份范围和时间间隔、数据恢复能力是否满足相关演练要求。

8.3.4 同步网人员和技术支持能力

8.3.4.1 检测方式

访谈、检查。

8.3.4.2 检测对象

机房管理人员，数据备份技术支持人员，设备软件（操作系统、数据库、应用软件等）技术支持人员，设备硬件技术支持人员，网络技术支持人员，历史值班记录，培训记录。

8.3.4.3 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机房管理人员、数据备份技术支持人员、设备软件（操作系统、数据库、应用软件等）技术支持人员、设备硬件技术支持人员和网络技术支持人员，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。

8.3.5 同步网运行维护管理能力

8.3.5.1 检测方式

访谈、检查。

8.3.5.2 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。

8.3.5.3 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，询问并查看与其他组织进行联络和协作的记录，检查同步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。

8.3.6 同步网灾难恢复预案

8.3.6.1 检测方式

访谈、检查。

8.3.6.2 检测对象

灾难恢复预案，设计/验收文档，演练记录，管理制度。

8.3.6.3 检测实施

a）应访谈安全管理人员，询问同步网是否具有灾难恢复预案，是否演练过灾难恢复，是否具有灾难恢复的管理制度。

b）应检查同步网灾难恢复预案设计/验收文档，查看其是否具备完整的同步网灾难恢复预案。

c）应检查同步网灾难恢复预案，查看其与设计是否一致。

d） 应检查同步网灾难恢复预案演练记录，查看其是否已经过灾难恢复预案演练以及灾难恢复预案演练的效果是否达到设计要求。

8.4 第3.1级要求

8.4.1 同步网冗余系统、冗余设备及冗余链路

与8.3.1的检测要求相同。

8.4.2 同步网冗余路由

与8.3.2的检测要求相同。

8.4.3 同步网备份数据

与8.3.3的检测要求相同。

8.4.4 同步网人员和技术支持能力

与8.3.4的检测要求相同。

8.4.5 同步网运行维护管理能力

与8.3.5的检测要求相同。

8.4.6 同步网灾难恢复预案

与8.3.6的检测要求相同。

8.5 第3.2级要求

8.5.1 同步网冗余系统、冗余设备及冗余链路

除按照8.4.1节的要求进行检测之外，还应按照本节内容进行检测。

8.5.1.1 检测方式

访谈、检查。

8.5.1.2 检测对象

同步网络，设计/验收文档。

8.5.1.3 检测实施

应检查同步网的抗灾难以及灾难恢复能力设计/验收文档，查看同步网的抗灾难以及灾难恢复能力，如出现灾难以后采用来自不同物理路由的主备用定时链路提供路由保护，以及采用来自地面（如铯原子钟）/天上（如GPS卫星定位系统）的定时信号提供定时源头的保护等。

8.5.2 同步网冗余路由

除按照8.4.2节的要求进行检测之外，还应按照本节内容进行检测。

8.5.2.1 检测方式

访谈、检查。

8.5.2.2 检测对象

设计/验收文档，演练记录，历史记录，传送链路。

8.5.2.3 检测实施

应访谈安全管理人员，检查设计/验收文档和网络运行历史记录，检查一级基准时钟LPR/PRC到2级节点时钟的定时链路是否采用了冗余路由，以及PRC到LPR的定时链路是否采用了冗余路由，并检查其与设计是否一致。

8.5.3 同步网备份数据

除按照8.4.3节的要求进行检测之外，还应按照本节内容进行检测。

8.5.3.1 检测方式

访谈、检查。

8.5.3.2 检测对象

数据备份服务器，设计/验收文档，演练历史记录。

8.5.3.3 检测实施

应访谈同步网安全管理人员，检查设计/验收文档，询问是否支持关键数据（如定时配置、PRC定时性能监视数据等）在不同的物理位置的定期备份。

8.5.4 同步网人员和技术支持能力

除按照8.4.4节的要求进行检测之外，还应按照本节内容进行检测。

8.5.4.1 检测方式

访谈、检查。

8.5.4.2 检测对象

机房管理人员，数据备份技术支持人员，设备软件（操作系统、数据库、应用软件等）技术支持人员，设备硬件技术支持人员，网络技术支持人员，历史值班记录，培训记录。

8.5.4.3 检测实施

应访谈数据备份技术支持人员、设备软件技术支持人员、设备硬件技术支持人员和网络技术支持人员，检查相关技术是否熟悉整个同步网的运行现状、各个业务网对定时信号的引接情况等。

8.5.5 同步网运行维护管理能力

除按照8.4.5节的要求进行检测之外，还应按照本节内容进行检测。

8.5.5.1 检测方式

访谈、检查。

8.5.5.2 检测对象

机房运行管理制度，关键数据实时容灾备份管理制度。

8.5.5.3 检测实施

应访谈安全管理人员，询问并查看关键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数据在不同的局址实时容灾备份管理制度。

8.5.6 同步网灾难恢复预案

除按照8.4.6节的要求进行检测之外，还应按照本节内容进行检测。

8.5.6.1 检测方式

访谈、检查。

8.5.6.2 检测对象

灾难恢复预案，设计/验收文档，演练记录，管理制度。

8.5.6.3 检测实施

应检查同步网管理制度，查看其是否具有灾难恢复预案管理制度。

8.6 第4级要求

同第3.2级要求。

8.7 第5级要求

待补充。