

国际电信联盟

ITU-T

国际电信联盟
电信标准化部门

X.1249

(01/2019)

X系列：数据网，开放系统通信和安全性
网络空间安全 – 反垃圾信息

**打击手机应用内植入的
广告垃圾信息的技术框架**

ITU-T X.1249建议书



ITU-T X系列建议书
数据网、开放系统通信和安全性

公用数据网	X.1 - X.199
开放系统互连	X.200 - X.299
网间互通	X.300 - X.399
报文处理系统	X.400 - X.499
号码簿	X.500 - X.599
OSI组网和系统概貌	X.600 - X.699
OSI管理	X.700 - X.799
安全	X.800 - X.849
OSI应用	X.850 - X.899
开放分布式处理	X.900 - X.999
信息和网络安全	
一般安全问题	X.1000 - X.1029
网络安全	X.1030 - X.1049
安全管理	X.1050 - X.1069
生物测定	X.1080 - X.1099
安全应用和服务	
组播安全	X.1100 - X.1109
家庭网络安全	X.1110 - X.1119
移动安全	X.1120 - X.1139
网页安全	X.1140 - X.1149
安全协议	X.1150 - X.1159
对等网络安全	X.1160 - X.1169
网络身份安全	X.1170 - X.1179
PITV安全	X.1180 - X.1199
网络空间安全	
计算网络安全	X.1200 - X.1229
反垃圾信息	X.1230 - X.1249
身份管理	X.1250 - X.1279
安全应用和服务	
应急通信	X.1300 - X.1309
泛在传感器网络安全	X.1310 - X.1339
PKI相关建议书	X.1340 - X.1349
网络安全信息交换	
网络安全综述	X.1500 - X.1519
脆弱性/状态信息交换	X.1520 - X.1539
事件/事故/探索法信息交换	X.1540 - X.1549
政策的交换	X.1550 - X.1559
探索法和信息要求	X.1560 - X.1569
标示和发现	X.1570 - X.1579
确保交换	X.1580 - X.1589
云计算安全	
云计算安全综述	X.1600 - X.1601
云计算安全设计	X.1602 - X.1639
云计算安全最佳实践和指导原则	X.1640 - X.1659
云计算安全实现	X.1660 - X.1679
其他云计算安全	X.1680 - X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

打击手机应用内植入的广告垃圾信息的技术框架

摘要

ITU-T X.1249建议书提供了一个打击手机应用内植入广告垃圾信息的技术框架。手机应用内植入广告垃圾信息是指手机应用内显示的强行推介的广告。这类强行推介的广告会以屏幕上方或下方的横幅、移动插页广告和重叠式广告等形式出现在移动装置显示屏上。随着手机应用的迅速发展，手机应用内植入广告急剧增长。过滤恶意广告可提升用户体验和安全性。因此，建立一个打击手机应用内植入广告垃圾信息的实用框架，将所有对策的优势适当地集于一体将十分有益。

历史沿革

版本	建议书	批准日期	研究组	唯一ID*
1.0	ITU-T X.1249	2019-01-30	17	11.1002/1000/13605

关键词

手机应用内植入广告、垃圾信息

* 欲查阅建议书，请在您的网络浏览器地址域键入URL <http://handle.itu.int/>，随后输入建议书的唯一识别码，例如<http://handle.itu.int/11.1002/1000/11830-en>。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：<http://www.itu.int/ITU-T/ipr/>。

© 国际电联 2019

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1	范围	1
2	参考文献	1
3	定义	1
	3.1 在其他处规定的术语	1
	3.2 本建议书定义的术语	1
4	缩写词和首字母缩略语	2
5	惯例	2
6	一般性内容	2
7	技术框架	2
8	功能组建	3
	8.1 预处理组件	3
	8.2 过滤引擎	3
	8.3 规则引擎	4
	8.4 审计平台	4
	8.5 手机应用内植入广告垃圾信息数据库	4
	8.6 反馈平台	4
9	过滤规则	4
	9.1 关键词	4
	9.2 黑名单/白名单	4
	9.3 常规表述	5
	9.4 功能检测	5
	9.5 行为	5
	9.6 模型核对	5
10	工作流	5
11	性能要求	6
	11.1 精确度要求	7
	11.2 效率要求	7
	参考文献.....	8

打击手机应用内植入的 广告垃圾信息的技术框架

1 范围

本建议书为打击手机应用内植入广告垃圾信息提供了一个技术框架。在此框架内，规定了功能组件过滤原则和工作流程。此外，该建议书建议为打击手机应用内植入广告垃圾信息搭建反馈平台。

该建议书适用于应用提供商和移动互联网服务提供商。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本文本中的引用而构成当前建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均面临修订；因此鼓励本建议书的使用者探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的ITU-T建议书清单定期出版。在本建议书中引用某个独立文件时，并未给予该文件建议书的地位。

无

3 定义

3.1 在其他处规定的术语

本建议书使用以下在其它文献中规定的术语：

3.1.1 移动电话（mobile phone） [b-ITU-T X-Sup.19]：用于通过无线电跨越大的地理区域接入公共移动网络来发起电话呼叫和传递文本信息、同时允许用户处于移动状态的电子设备。

3.1.2 智能电话（smartphone） [b-ITU-T X-Sup.19]：拥有强大计算能力、异质连接性和为第三方应用程序提供平台的先进操作系统的移动电话。

3.1.3 垃圾信息（spam） [b-ITU-T X.1242]：通过计算机、移动电话、电话等终端由发送方向接收方发送的电子消息，该信息对接收方来说通常是未经请求、无用和有害的。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 异步过滤：用来确定垃圾广告的文件处理技术，可同步处理若干标识。

3.2.2 移动应用：设计用来在智能电话和平板计算机等移动设备上运转的软件应用。

3.2.3 手机应用内植入广告：在手机应用中显示的广告。可以屏幕上方或下方的横幅、移动插页广告和重叠式广告等形式出现在移动装置显示屏上。

3.2.4 手机应用内植入广告垃圾信息：通常为强行推介的手机应用内植入广告，对于接收者而言既无用又有害。

注1 – “强行推介”在这里指“用户未要求”，“无用”指用户通过一些行为表达其拒绝，例如关闭接收某种广告的选项。

注2 – 手机应用内植入广告通常不加区分地大量重复发送。实际和有形伤害的例子包括欺诈或恶意代码的传输。

3.2.5 同步过滤：用来识别垃圾广告的文件处理技术，完成一项后再开始另一项。

4 缩写词和首字母缩略语

本建议书使用了下述缩写词和首字母缩略语：

AD	广告
API	应用程序界面
ID	身份
IP	互联网协议
URL	统一资源定位

5 惯例

无。

6 一般性内容

由于移动互联网的快速发展和操作系统的开放性质，手机应用内植入广告发展迅速。通常，手机应用启动一个由服务平台提供的应用程序界面（API）以提供广告（ADS）。由于移动应用提供的广告是免费或几乎免费的，手机应用内植入广告越来越普及。多数广告是合法的，适用于用户，但一些广告为垃圾信息。选择进入或选择退出等多项措施均用来阻止广告垃圾信息。

尽管为打击手机应用内植入广告垃圾信息采取了多项对策，但仍缺乏打击手机应用内植入广告垃圾信息的技术框架。手机应用内植入垃圾信息可能对应用和服务提供商造成许多不良影响。手机应用内垃圾广告信息消耗大量带宽并可能造成数据流量拥堵。这些垃圾信息还影响日常生活，甚至传送移动欺诈行为。全面解决垃圾信息问题没有一个灵丹妙药。因此，我们试图制定打击手机应用内植入垃圾广告信息的实用框架，将打击手机应用内植入广告垃圾信息措施合理地综合起来。

7 技术框架

打击手机应用内植入广告垃圾信息的过滤系统（如垃圾信息过滤系统）主要靠实施用于提供应用API的服务平台。这些应用可启动API，从而传送广告和其它消息。打击手机应用内植入广告垃圾信息的技术框架见图1。

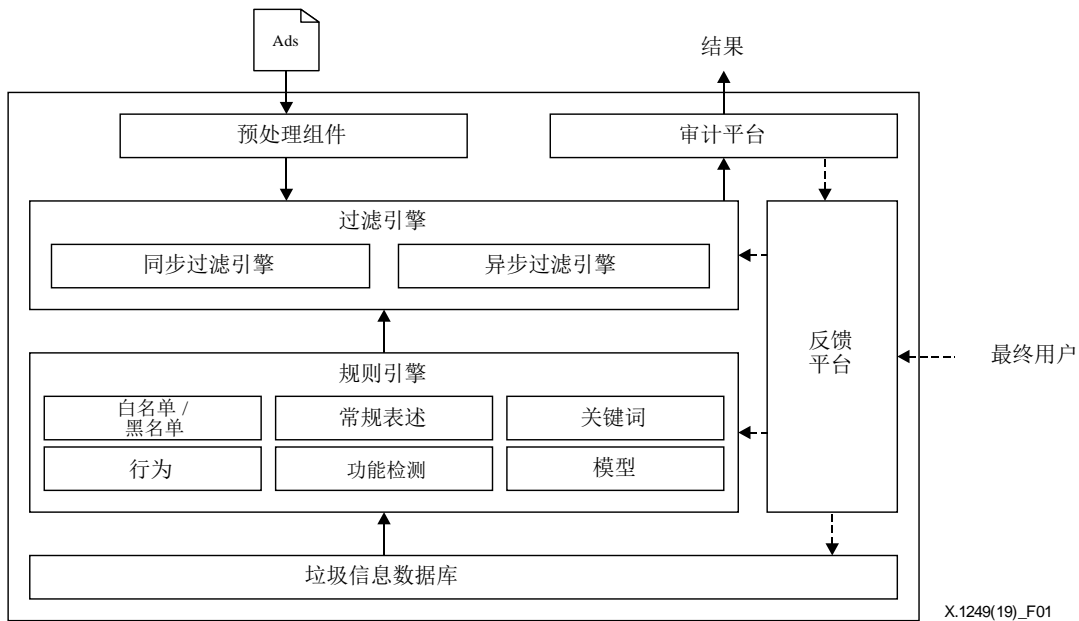


图1 – 打击手机应用内植入广告垃圾信息的技术框架

8 功能组建

8.1 预处理组件

预处理组件用来对原有的广告文件进行预处理，以便将这些广告转化为过滤引擎需要的格式，如将文本、图形、统一资源定位符（URL）、视频和音频等内容分离开来。

8.2 过滤引擎

过滤引擎是打击手机应用内植入广告垃圾信息的最重要组件。过滤引擎的主要目的是确定实际的手机应用内植入广告垃圾信息或出现这类信息的可能性。根据识别垃圾信息的不同方法，过滤引擎可分为同步或异步过滤。从时间效率来看，异步过滤引擎通常优于同步过滤引擎。

8.2.1 同步过滤引擎

同步过滤在完成一项过滤规则后再开始下一项规则。同步过滤指因复杂程度较低而进行的在线过滤。过滤结果可在很短时间内产生。一般情况下，同步过滤结果立等可取，这意味着在过滤结束后就可立刻做出决定。如一项过滤规则结果对之后过滤规则的执行具有影响，建议采用同步过滤。同步过滤可包含使用白名单/黑名单、常规表述、行为模型、功能检测等方式在内的过滤。

8.2.2 异步过滤引擎

异步过滤可使不同工作流程在同一时间内运行，即不同工作流程不依赖于相互间的成果。异步过滤指因对更加复杂的手机应用内植入广告垃圾信息进行的脱机过滤，通常这种过滤时间较长。异步过滤通常包括音频识别、视频识别、关键词匹配、深度建模等。

8.3 规则引擎

规则引擎提供过滤规则，包括用于过滤引擎的所有规则。过滤规则具有多个来源：运营商配置、垃圾信息数据库和第三方规则共享。规则引擎提供用来识别手机应用内植入广告垃圾信息的决定规则。一些决定规则以多个垃圾信息测试的加权值总和为基础（如过滤结果不确定）。规则引擎将提供门限（即，固定）值。如总和大于门限值。过滤引擎将决定该广告是否为垃圾信息。此外，规则引擎可将来自过滤引擎的不同检测因数整合起来以确定广告是否为手机应用内植入广告垃圾信息。

8.4 审计平台

过滤引擎不可能检测出所有手机应用内植入广告垃圾信息。因此，应使用人工方法进行手机应用内植入广告垃圾信息评估，因此审计平台应运而生。通过审计平台，审计人员可发现过滤引擎无法识别的未知手机应用内植入广告垃圾信息。审计平台的准确率通常高于过滤引擎。因此，审计平台产生的结果可置于手机应用内植入广告垃圾信息数据库，满足未来使用需求。

8.5 手机应用内植入广告垃圾信息数据库

该数据库用于存储手机应用内植入广告垃圾信息特性。这是一个逻辑数据库，可由每个服务提供商维护或由多个服务提供商共享。来自数据库的手机应用内植入广告垃圾信息特性可用来比对和过滤。丰富手机应用内植入广告垃圾信息数据库有助于改进规则引擎的性能。通过从新识别的手机应用内植入广告垃圾信息提取特性的反馈平台可丰富手机应用内植入广告垃圾信息数据库。

8.6 反馈平台

最终用户是手机应用内植入广告垃圾信息的目标、受害者和接收方。利用审计平台的结果，最终用户的参与有助于有效和高效地打击手机应用内植入广告垃圾信息。因此，反馈平台亦应考虑到最终用户的反应。需要建立这样的机制来支持这个目标，包括向垃圾信息广告数据库提供反馈。此外，反馈平台有必要采用标准格式登记反馈。这将使不同的运营商和实体共享反馈。垃圾信息制造者的主要地址可从共享反馈中获得并放到黑名单中。

9 过滤规则

9.1 关键词

关键词用来确定广告内容（词汇）是否与手机应用内植入广告垃圾信息数据库中发现的样本匹配。关键词具有以下来源：运营商配置、外部渠道、反馈平台和来自垃圾信息数据库的机器学习。关键词可在短暂的时间内以低成本精确识别高风险恶意广告，因此，通常用于同步过滤。为提高关键词的效率，有必要对原文进行预处理，从而过滤出一些故意混淆的字符，特别是URL过滤中关键词的一些不同编码类别。

9.2 黑名单/白名单

黑名单基于维护发送手机应用内植入广告垃圾信息的可疑互联网协议（IP）地址或域名的原则。这些名单还可包括设备身份（ID）、URL或服务平台中的发送方账户。实体通过这些做法可实现分享，服务平台通过采用和维护黑名单可满足自己的需求。

白名单基于列举所批准的或所识别的广告来源/实体的原则。这些名单还可将设备ID或发送方账户包含在服务平台中。

与关键词相似，尽管黑名单和白名单不可避免地包含不准确信息，黑名单可防止一些合法广告通过过滤引擎，黑名单和白名单是过滤手机应用内植入广告垃圾信息的有效解决方案。

9.3 常规表述

常规表述通常用来匹配和过滤恶意广告文本和一些具体模式。这些表述灵活、具有逻辑性和功能性。通常产生的最终结果不需要额外的判定或修改。与关键词或黑名单/白名单不同的是，常规表述可用来匹配在内容上不同，但形式别具一格的广告。这些亦广泛用于高效率同步过滤。常规表述广泛用于同步过滤的原因是因为，设计良好的常规表述具有很高的精确度。为避免不可预测的资源消耗，常规表述可在使用前经过全面测试，包括性能和准确度测试。

9.4 功能检测

功能检测是计算机愿景中的一个通用应用，通常基于模式识别和机器学习。最具有代表性的功能检测是在成千上万幅画面中识别恶意广告。功能检测需要计算。提取和存储输入手机应用内植入广告垃圾信息数据库的已知手机应用内植入广告垃圾信息的功能特性。在收到可疑画面后，功能检测计算画面的抽象信息并决定该点是否包含恶意广告。功能提取算法和相应的匹配算法决定是否可能很快和准确地查找到恶意广告图像。功能检测通常提供模糊结论，因而有必要将更多的决策程序包含在内，以便得出最终结果。由于计算的复杂性和对整个文件的比较，功能检测通常用于异步过滤。

9.5 行为

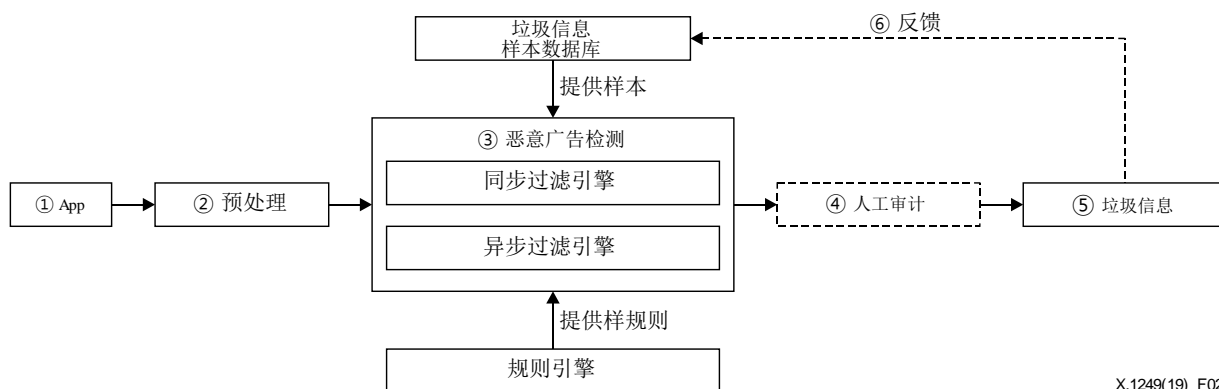
手机应用内植入广告垃圾信息通常采用批量方式、不加区别或重复地发送，同时还具备一些其它特别特性。过滤引擎可记录手机广告行为并计算出它们之间的相互关系。当接收广告行为与存储在垃圾行为数据库中的特性相符时，可以确定该文件很可能为恶意广告。由于广告行为在时间上是不确定的，行为检测可用来确定未知的恶意广告，因此更适用于异步过滤。

9.6 模型核对

模型核对是用来满足核对要求的重要方式，例如，相似性模型和决策树模型是检测手机应用内植入广告垃圾信息的有效方式。有时，单个模型无法确定广告是否为恶意广告，而综合若干种模型（如模型堆）方可做出全面的检测。模型核对既可用于同步过滤，也可用于异步过滤。

10 workflows

手机应用内植入广告垃圾信息过滤通常采用图2的系列程序，在一些情况下，同步过滤引擎和异步过滤引擎可并行使用。



X.1249(19)_F02

图2 – 用于垃圾信息广告过滤的工作流

一般采取的步骤如下：

- 1) 提供广告并将其传送至手机应用；
- 2) 这些广告应提前处理，例如，广告媒体的不同类型分为URL、文本、音频、视频等；
- 3) 根据过滤的风险和复杂度，内容将传送至同步过滤引擎或异步过滤引擎。这些引擎经过一些配置可按需求进行调整。为进行全面的监测，有时需要将同样的内容载入同步和异步过滤引擎。综合规则引擎和手机应用内植入广告垃圾信息样本数据库提供的规则和样本，核对广告以确定是否需要过滤。
 - a) 同步过滤引擎在步骤2后基于规则引擎的过滤规则检测手机应用内植入广告垃圾信息。如同步过滤模块发现手机应用内植入广告垃圾信息，垃圾信息过滤将完成，该广告将立即受到阻止，同时进入到步骤6，如URL或应用账户属于同步过滤引擎中的白名单，该广告将迅速传送。如广告无法评估，进入到步骤4；
 - b) 异步过滤引擎将在第2步后基于规则引擎中的过滤规则检测广告中的垃圾信息。如异步过滤模块发现垃圾信息，垃圾信息过滤将完成，该广告将立即受到阻止，同时进入到步骤6。如广告无法评估，则进入到步骤4；
- 4) 广告有时需要人工测试和评估。如检测并确认了垃圾信息，则进入步骤5；
- 5) 根据预配置，垃圾信息将得到处理，如记录、更替等；
- 6) 手机应用内植入广告垃圾信息存储在垃圾信息数据库中。此外，数据库中的手机应用内植入广告垃圾信息广告通过提取可作为新的规则，或载入规则引擎或用于优化规则引擎。

11 性能要求

手机应用内植入广告垃圾信息检测的精确度应通过综合错误正确和失误率予以衡量，这种精确应被看作平衡。

11.1 精确度要求

错误正确率是作为未识别为垃圾信息或具有恶意性的有效广告数字与有效广告数字总和之间的比计算的。如错误正确率高，这意味着，一些手机应用的有效广告已被阻止。因此，错误正确率应尽可能降低。

错误失误率是作为错误识别的手机应用内植入广告垃圾信息有效数字与垃圾信息或恶意广告总数之间的比计算的。如错误失误率高，这意味着，用户更容易受到手机应用内植入广告垃圾信息的侵犯。因此，错误失误率亦应尽可能降低。

11.2 效率要求

手机应用内植入广告垃圾信息过滤算法的效率可通过过滤引擎的时间和空间复杂性予以衡量。时间复杂性指用来运行过滤广告程序需要的时间，而空间复杂性指所需要的空间（内存）。这两项指标对过滤规则的应用类型具有重要影响。较低的时间和空间复杂性过滤规则可用于同步过滤引擎，而较高的过滤规则则可用于异步过滤引擎。

参考文献

- [b-ITU-T X.509] ITU-T X.509建议书（2016年），信息技术 – 开放系统互连 – 号码簿：公开密钥和属性证书框架。
- [b-ITU-T X.800] ITU-T X.800建议书（1991年），CCITT应用的开放系统互连安全体系结构。
- [b-ITU-T X.805] ITU-T X.805建议书（2003年），提供端到端通信的系统的架构。
- [b-ITU-T X.1231] ITU-T X.1231建议书（2008年），反垃圾信息技术策略
- [b-ITU-T X.1242] ITU-T X.1242建议书（2009年），基于用户指定规则的短消息业务（SMS）垃圾过滤系统。
- [b-ITU-T X.1254] ITU-T X.1254建议书（2012年），实体认证保证框架。
- [b-ITU-T X-Sup.19] ITU-T X-系列建议书 – 补充19（2013年），智能手机安全方面的补充。
- [b-ITU-T X-Sup.24] ITU-T X-系列建议书 – 补充24（2014年），关于通信装置安全应用分布框架的增补。

ITU-T 系列建议书

- 系列 A ITU-T 工作安排
- 系列 D 一般关税原则
- 系列 E 整体网络运营、电话业务、服务运营和人为因素
- 系列 F 非电话电信服务
- 系列 G 传输系统和媒体、数字系统和网络
- 系列 H 视听和多媒体系统
- 系列 I 综合服务数字网络
- 系列 J 有线电视网络和电视的传播，合理的计划和其他多媒体信号
- 系列 K 干扰防护
- 系列 L 环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
- 系列 M 电信管理、包括电信管理网和网络维护
- 系列 N 维护：国际广播节目和电视传输电路
- 系列 O 测量设备说明书
- 系列 P 终端和主观及客观的评价方法
- 系列 Q 交换和信令
- 系列 R 电报传输
- 系列 S 终端服务终端设备
- 系列 T 远程信息处理服务终端
- 系列 U 电报交换
- 系列 V 电话网络之上的数据通信
- 系列 X 数据网络、开放系统通信和安全**
- 系列 Y 全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
- 系列 Z 电信系统的语言和通用软件方面