国 际 电 信 联 盟

ITU-T X.1332

(03/2020)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务(2)– 智能电网安全

智能电网系统中智能电表业务的安全导则

ITU-T X.1332建议书

国际电信联盟

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(1)	
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(1)	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(2)	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	**X.1330–X.1339**
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
安全协议(2)	X.1450–X.1459
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
量子通信	X.1700–X.1729

ITU-T X.1332建议书

智能电网系统中智能电表业务的安全导则

摘要

智能电表业务在全球广泛使用，通过收集客户电力使用信息并向客户提供这一信息，从而能使得电网更加高效和可靠。这一信息可被用来估测客户的电力需求，而通过向客户提供这一估测信息，可以改变客户的电力需求或客户的电力消费行为。不过，智能电表业务也可能因为各种风险的存在而出现故障。比如，无效的计量信息可能导致做出错误的需求管理决定，滥用负荷控制函数可能导致客户出现经济和物理上的损失。ITU-T X.1332建议书为智能电表业务提供了安全导则，以使业务提供商能够实施适当的安全措施以确保其服务的安全性。本建议书识别了智能电表业务的安全威胁和攻击方法，并明确了安全要求和功能，以相应减弱这类威胁和攻击。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1332	2020-03-26	17	11.1002/1000/14086

关键词

高级计量基础设施、安全导则、智能电网、智能电表业务。

* 访问建议书，请在您的Web浏览器地址栏中输入网址http://handle.itu.int/，其次建议书的识别码，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）在电信，信息和通讯技术领域是国际电信联盟的常设机构。国际电信联盟电信标准化部门负责研究技术，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。

世界电信标准化大会（WTSA），每四年举行一次，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第一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和适应性等），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

国际电联提醒注意：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、有效性或适应性不表示意见。

至本建议书截止之日起，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，这可能并非最新消息，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/。

目录

ITU-T X.1332建议书

智能电网系统中智能电表业务的安全导则

1 范围

本建议书提供了智能电网中的智能电表业务的安全导则，包括以下内容：

– 识别了智能电表业务的安全威胁和攻击；

– 智能电表业务的安全要求；以及

– 满足安全要求的智能电表业务安全导则。

2 参考文献

无。

3 定义

3.1 它处定义的术语

本建议书使用了它处定义的以下术语：

3.1.1 需求响应（demand response）（DR）[b-ITU-T Y.2071]：智能电网的特征之一，允许消费者在峰值时降低或改变其电力使用模式，通常可用来换取财务激励。这类机制和激励允许电力公司、商业、工业和住宅客户在供电峰值或不稳定时段削减能源需求。需求响应是优化能源供给平衡的必须要素。

3.1.2 电力能源系统运营商（electric powersystem operator）[b-IEC 60050-617]：一个实体，负责在一特定区域安全和可靠地运营电力能源系统，并与电力能源系统的其他部分进行互联。

3.1.3 能源管理系统（energy management system）（EMS）[b-ITU-T Y.2071]：包含软件平台的计算机系统，由基本支持服务和一系列应用组成，提供发电和传输设施有效运行所需的功能，以确保以最低成本提供足够的能源供给安全性。

3.1.4 智能电表（smart meter）[b-ITU-T X.1331]：安装在驻地设备的一种装置，根据客户的需求响应信息，可对家庭智能设备的电力使用情况进行监督和控制。

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 数据集中器（data concentrator）：位于智能电表和电力公司系统之间的设备，主要作用是收集和管理来自智能电表的数据。

3.2.2 电表数据管理系统（meter data management system）（MDMS）：电表数据管理系统负责汇总、验证、预测并允许对能源利用、产生以及计量日志等计量数据进行编辑。在这类数据进入数据仓库之前的有限时段内，MDMS负责存储这一数据，并向被授权系统提供这一数据。

注 – 修改自 [b-ITU-T Y.2071]

3.2.3 智能电表业务（smart metering service）：该业务通过智能电表收集电力使用数据，并将分析后的数据提供给客户和电力公司；第三方业务提供商也可能参与这一业务，以便通过电力使用数据，向客户提供一项或一套服务。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

CDMA 码分多址

DDoS 分布式拒绝服务

DoS 拒绝服务

EMS 能源管理系统

EUIS 能源使用信息系统

HMAC 散列消息认证码

IHD 家用显示器

LTE 长期演进

MDMS 电表数据管理系统

PII 个人可识别信息

PLC 电力线通信

QoS 服务质量

TLS 传输层安全

VPN 虚拟专用网络

5 惯例

无。

6 概述

智能电表业务是智能电网的一个基本特征，已经在全球广泛部署，该业务通过收集客户信息并向客户提供这一信息，从而能使得电网更加高效和可靠。

智能电表测量、记录和传送客户使用的电力数量。计量数据将被周期性传送，比如每隔5或15分钟。基于这些数据，智能电表业务提供商能够预测客户的电力需求。根据这一预测信息，可以通过改变客户的电力需求或其电力消费模式，从而将电网变得更加可靠。

智能电表业务提供商能够向客户提供其电力使用情况以及实时电价、预计账单、统计数据或需求趋势等方面的信息。通过使用这些信息，客户可以尝试自愿降低其电力消费。比如，如果提供商使用动态定价以及基于电力需求改变价格的政策，则客户可以采取延迟或提前电力消费的行为。

但是，仍然存在一些可能导致智能电网出现故障的威胁。比如，无效计量信息可能导致采取错误的需求管理决策，滥用负荷控制函数可能导致对客户产生经济或物理上的损害。此外，当第三方业务提供商能够访问计量信息时，必须考虑对个人可识别信息（PII）的保护。

此外，电力使用信息、统计数据以及成本信息通常被传送至与客户联网的设备上，如智能电话或手持电脑等。因此，几乎所有能够影响移动设备的威胁也都能影响智能电表业务。

本建议书考察了智能电表业务上存在的安全威胁，并找出了能够确保智能电表业务安全的安全要求。

7 智能电表业务的架构

在描述智能电表业务的安全性之前，要先定义此类业务的架构，以便找出所有与智能电表业务相关的实体，并明确它们之间的关系。

为定义电表业务的一般模型，本建议书考虑以下应用场景：

– 收集来自计量设备的电力使用数据；
– 向客户提供电力使用趋势；
– 向第三方业务提供商提供电力使用信息；以及
– 向电力能源系统运营商提供提供电力使用信息。

图7-1给出了适用于上述应用场景的智能电表业务架构。在该模型中，有6个主要实体：计量设备、电力能源系统运营商、电表数据管理系统（MDMS）、电力公司（系统）、第三方业务提供商和客户。

计量设备测量客户的电力使用情况，并向位于电力公司的MDMS发送计量数据。电力公司提供能源使用信息系统（EUIS），向客户提供电力使用趋势。为生成统计信息，EUIS需要获取来自MDMS的计量数据。电力公司的计费系统也使用计量数据。在该架构中，EUIS和计费系统被概括为电力公司系统。

电力能源系统运营商使用计量数据来预测当前和未来阶段的能源系统状态。电力能源系统运营商的能源管理系统（EMS）接收来自MDMS的计量数据，并利用这些数据来分析电力需求趋势。基于这些预测的需求趋势，运营商可以调整电力供应量，以便能源系统能够实现供需平衡。

客户具有智能能源显示器或智能设备，能够显示能源使用的统计数据，并且控制连接到其住宅网络上的负载。客户可以利用若干类型的显示设备，包括智能手机、平板电脑、智能电视、个人计算机以及专业的家用显示器（IHD）等，以便访问电力公司的EUIS。

第三方业务提供商利用计量数据来改进其服务质量。比如，如果有线电视公司知道客户正在洗衣服，就可能向该客户播放一款清洁剂的商用广告。

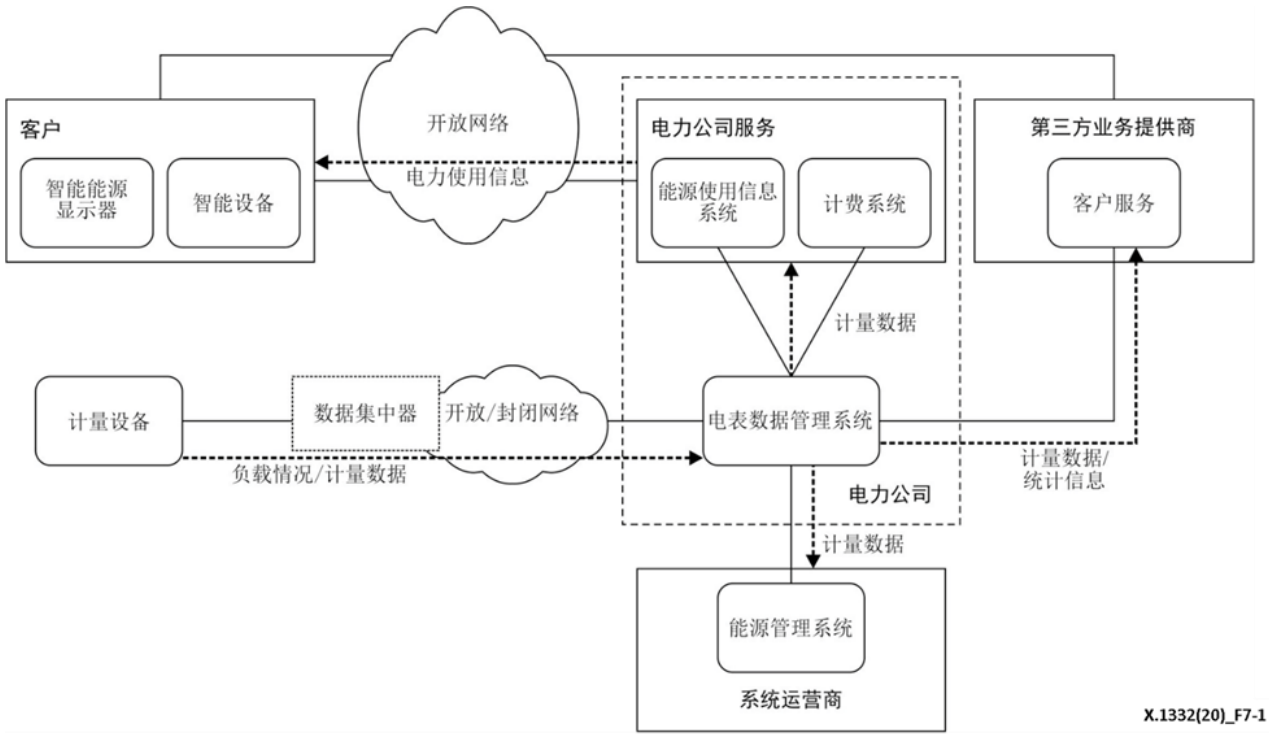

图7-1 – 智能电表业务架构

该架构模型中考虑了测量设备和MDMS、MDMS和EMS、MDMS和电力公司系统、MDMS和第三方业务提供商、客户和电力公司系统以及客户和第三方业务提供商等六方面实体之间的关系。

计量设备通过网络连接至MDMS。网络可以是开放的，比如LTE或CDMA，也可以是封闭的，如PLC或租用线网络。不管采用何种类型的网络，数据集中器将汇集一个区域的计量数据，并将集中后的数据发往MDMS。

MDMS和EMS相互之间通过具有服务质量（QoS）保证的电信网络进行通信。

MDMS和电力公司系统通常位于同一个网络内。如果它们之间不是通过相同网络连接的，则它们之间通常通过具有QoS保证的电信网络进行连接。

MDMS可以利用具有保证QoS的电信网络连接至第三方业务提供商。

因为客户使用的是如因特网之类的开放性网络，不论是电力公司系统还是第三方业务提商，都要通过开放网络与客户进行连接。客户可以通过WiFi、LTE和蓝牙等方式来访问网络。

8 智能电表业务的安全威胁

8.1 对计量设备和MDMS之间界面的威胁

计量设备和MDMS之间的界面用以收集和处理大量的客户电力使用数据，包括电表数据、负载情况、电力质量测量等。通过该界面传送的数据是攻击者的主要目标。攻击者通过截获、伪造和中继这些数据，来摧毁智能计量业务。

攻击者也通过对 MDMS 发起分布式拒绝服务（DDoS）攻击，从而拒绝智能计量业务。

计量设备和 MDMS 之间的界面容易受到以下威胁的影响：

– 信息泄露：智能计量设备（如智能电表）通过数据集中器向MDMS周期性发送电力负荷数据（计量数据）。在电网中，该周期很短（比如5分钟或更短）。因此，如果攻击者能够嗅探到计量数据，就可能获得客户的生活模式信息。

– 伪造计量数据：攻击者能够封堵实际计量数据，并取而代之向MDMS发送伪造的计量数据。这类攻击通过阻止MDMS和EMS访问实际采集的计量数据，从而导致生成错误的需求预测。这种失误也可能导致供需不平衡，导致动力故障。

– 伪造负荷曲线：攻击者能够对计量设备存储的负荷曲线进行非授权修改。因为计费系统基于其负荷曲线对客户进行收费，这一威胁可能导致对客户的不正确计费。

– 拒绝服务（DoS）：攻击者可能会执行一个DoS攻击，比如在很多计量设备或数据集中器上运行有害代码，或通过相当多的数据或大量的业务请求，对目标（通常是MDMS）进行“洪水攻击”。这样的攻击可以减慢甚至停止智能电表业务。

8.2 对MDMS和第三方业务提供商之间界面的威胁

MDMS和第三方业务提供商之间的界面被用以分享计量数据，从而使得后者可以为每个客户提供各种定制化的服务。因为，PII可能会通过这一界面进行传输，因此，攻击者主要以这些数据为目标，并通过截获和使用这些数据来破坏智能电表业务。

MDMS和第三方业务提供商之间的界面可能受以下威胁的影响：

– PII泄漏：攻击者可能通过发起包嗅探攻击或在第三方业务提供商联网系统上执行有害代码来截获PII。

8.3 对电力公司系统和客户之间界面的威胁

电力公司系统和客户驻地设备之间的界面提供了各种类型的信息，能够鼓励客户参与需求响应。这类信息包括客户电力使用趋势、实时电力价格、需求趋势、计费和统计数据。通过伪造实际传送信息，攻击者能够欺骗客户消费额外的电力。DoS攻击是另一类对连接到客户驻地设备的电力公司系统的严重潜在威胁。

电力公司系统和客户设备之间的界面容易受到以下威胁的影响：

– 伪造实时价格：攻击者可能对电力公司系统提供的实时价格进行伪造，并提供给客户以欺骗他们。如果伪造的价格低于实际价格，则客户设备（如智能能源显示器）可能指令一个电力消费设备（如电动汽车）消费更多的电力。相比较而言，如果伪造价格高于实际价格，消费者可能失去在低价时存储电力的机会。

– 拒绝服务：攻击者可能发起一个DoS攻击，在很多客户设备上运行有害代码，并利用大量的业务请求来对目标（通常是EUIS）进行“洪水攻击”。这样的攻击可以减慢甚至停止智能电表业务。

– PII泄漏：攻击者可能通过发起包嗅探攻击或在客户联网设备上执行有害代码来截获PII。

9 智能电表业务的安全要求

9.1 电力使用计量的安全要求

电力使用计量是智能电表业务中最重要的功能。当它正确运行时，MDMS能够收集必要的信息来生成电力使用趋势、每个客户的使用模式、电力公司账单等。此外，智能电表业务中的其他实体能够使用这一信息来正确发挥其作用。因此，计量数据的完整性、真实性以及保密性是信息收集程序的主要安全需求。

为正确应对智能电表和MDMS之间通信界面的威胁，应考虑以下安全要求：

– 应确保智能电表与MDMS之间通信界面传送的数据的端到端保密性。
– 应确保智能电表与MDMS之间通信消息的端到端完整性，以防止数据的非授权修改。
– 对于存储在智能电表、数据集中器和MDMS等设备上的计量数据和验证信息，应保护其不被非授权访问。
– 应确保每个通信联络的发送方的真实性。

9.2 客户所使用信息的安全要求

因为客户设备能够访问与后端电力能源系统相联的电力公司系统，它们成为智能电表业务的主要攻击目标。对于这一部分的智能电表业务，应保护客户设备的数据和应用。

为降低电力公司系统和客户之间通信界面威胁可能带来的副作用，应考虑以下安全要求：

– 应确保客户和电力公司系统之间通信界面的数据保密性。
– 应确保客户和电力公司系统之间的通信信息的完整性，以禁止对数据的非授权修改。
– 应确保每个通信联络的发送方的真实性。
– 应保护客户设备和电力公司系统所存储的信息免于非授权访问。
– 应考虑客户设备上的应用的完整性。

9.3 第三方业务提供商所使用信息的安全要求

这一问题主要考虑第三方业务提供商和MDMS之间的PII数据处理和PII泄漏。

为妥善处理对MDMS与第三方业务提供商之间通信界面造成的威胁，应考虑以下安全要求：

– 应确保MDMS和第三方业务提供商之间通信界面上的数据保密性。
– 应确保MDMS和第三方业务提供商之间的通信消息的数据完整性，以禁止对数据的非授权修改。
– 应确保每个通信联络的发送方的真实性。
– 为实现个性化服务，应仅在征得客户同意后才能将PII数据妥善处理，用于公开目的。
– 对于不使用PII的业务，不应提供与计量相关的PII。

9.4 电力能源系统运营商所使用信息的安全要求

为了妥善防止对MDMS和电力能源系统运营商之间界面造成的威胁，应考虑以下安全要求。

– 应确保MDMS和电力能源系统运营商之间通信界面的数据保密性。
– 应确保MDMS和电力能源系统运营商之间通信消息的数据完整性，以防止对数据的非授权修改。
– 仅应允许授权实体访问MDMS和电力能源系统运营商之间的通信界面。
– 不应提供计量相关的PII。

10 智能电表业务的安全导则

10.1 电力使用计量的安全控制

为实现电力使用计量的安全要求，应将以下安全控制视为每个电力计量实体具备的功能。

– 应对计量设备、数据集中器和MDMS采取计量数据访问控制。只有经过授权的实体才能够访问电力使用数据。
– 计量设备和MDMS之间应采取相互认证机制，以确保发送方的真实性。
– 应采取消息验证措施，以保护传送至MDMS的电力使用数据的完整性。比如，HMAC加密消息验证码可以作为这一措施的可能选项。
– 可以考虑将数据加密作为一项安全措施，以保护计费相关数据。
– 应在MDMS上实施数据完整性损坏监测和加密数据解密措施。
– 应在计量设备、数据集中器和MDMS上采取安全密钥管理机制，用于加密密钥的生成、接受、存储和刷新。
– 应使用数据保护机制来确保MDMS所存储数据的保密性和完整性。
– 可以在MDMS上采取安全措施来缓解DoS攻击所带来的影响。

10.2 客户所使用信息的安全控制

为了实现客户所使用信息的安全要求，应将以下安全控制视为每个实体具备的功能：

– 应在客户设备与电力公司系统之间的通信上，采取诸如TLS等安全通信措施。应在客户设备和电力公司系统之间提供相互认证、通信数据验证和加密功能。
– 对于提供电力使用信息的应用，应采取用户验证和对此类信息的访问授权。电力公司系统应只允许授权用户访问其自身数据。
– 应在客户设备上安全地存储用户认证数据和用于用户验证的加密密钥、安全通信和PII。
– 应启动完整性检查，对于每一个在客户设备上运行的应用，都要对其进行真伪检测。

10.3 第三方业务提供商所使用信息的安全控制

为了满足对第三方业务提供商所使用信息的安全要求，应将以下安全控制视为每个实体应具备的功能：

– 可采用租用专线，以防止非授权用户访问MDMS和第三方业务提供商之间的连接。

– 应确保在客户设备和电力公司系统之间的通信上采用诸如虚拟专用网（VPN）之类的安全通信措施。应在客户设备和电力公司系统之间提供相互认证、通信数据验证和加密功能。

– 如果PII被第三方业务提供商[b-GAO-08-343]访问，则应在PII的整个生命周期采取保护措施。如果识别数据对于第三方业务提供商不是必须的，则可以采取取消识别信息的措施。

10.4 电力能源系统运营商所使用信息的安全控制

为满足电力能源系统运营商所使用信息的安全要求，应将以下安全控制视为每个实体应具备的功能：

– 应采用租用专线来降低非授权访问对MDMS和电力能源系统运营商之间连接的影响。

– 应在MDMS和电力能源系统运营商之间的通信上采取诸如VPN之类的安全通信措施。应在MDMS和电力能源系统运营商之间提供相互认证、通信数据验证和加密功能。

– 如果识别数据对于第三方业务提供商不是必须的，则可以采取取消识别信息的措施。

参考资料

[b-ITU-T X.1331] ITU-T X.1331建议书（2018年），智能电网系统中家域网（HAN）设备的安全导则

[b-ITU-T Y.2071] ITU-T Y.2071建议书（2015年），微电网架构

[b-GAO-08-343] United States Government Accountability Office, GAO-08-343:2008, *Information Security: Protecting Personally Identifiable Information.* https://www.gao.gov/new.items/d08343.pdf

[b-IEC 60050-617] IEC 60050-617:2009, *International Electrotechnical Vocabulary – Part 617: Organization/Market of electricity*.

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	资费及结算原则和国际电信/ICT的经济和政策问题
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒介、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	环境与ICT、气候变化、电子废物、节能；线缆和外部设备其他组件的建设、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令，以及相关联的测量和测试
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	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
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2020年，日内瓦