ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la Normalisation

Recommandation

UIT-T X.1815 (03/2023)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité des IMT-2020

Lignes directrices et exigences en matière de sécurité pour les services informatiques en périphérie fondés sur les IMT-2020

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile (1)	X.1140–X.1149
Sécurité des applications (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1350–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1399
Sécurité de la technologie des registres distribués (DLT)	X.1400–X.1429
Sécurité des applications (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470–X.1489
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
Cyberdéfense	X.1590–X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
Protection des données	X.1770–X.1789
SÉCURITÉ DES IMT-2020	**X.1800–X.1819**

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1815

Lignes directrices et exigences en matière de sécurité pour les services informatiques en périphérie fondés sur les IMT-2020

Résumé

Le réseau IMT-2020 permettra de fournir une large gamme de services, parmi lesquels les services large bande mobiles évolués (eMBB), les services fondés sur des communications massives de type machine (mMTC) et les services fondés sur des communications ultra-fiables et à faible temps de latence (uRLLC), sur une infrastructure de réseau et de ressources informatiques. Conformément aux principales caractéristiques et aux exigences identifiées pour le réseau IMT-2020, il est exigé que ce réseau soit plus efficace, personnalisé, intelligent, fiable et souple.

Pour assurer les services types dans le réseau IMT-2020, en particulier les services eMBB et uRLLC, l'informatique en périphérie est reconnue comme étant l'une des principales technologies permettant de satisfaire les indicateurs fondamentaux de performance (IFP) particulièrement exigeants du réseau IMT-2020, surtout pour ce qui est du faible temps de latence et de l'efficacité d'utilisation de la largeur de bande.

L'informatique en périphérie permet à l'opérateur et au fournisseur de services tiers de déployer les services à proximité du point d'accès de l'utilisateur, ce qui permet de fournir des services avec une grande efficacité, grâce à la réduction du temps de latence et de la charge sur le réseau de transport.

Afin de garantir la sécurité du déploiement et de l'application des services informatiques en périphérie, il est nécessaire d'analyser les menaces pour la sécurité et les exigences de sécurité propres à ces services et d'établir un cadre général pour la sécurité.

La présente Recommandation vise à analyser le modèle de déploiement et les scénarios d'application types des services informatiques en périphérie, à décrire les menaces pour la sécurité et les exigences de sécurité propres aux services informatiques en périphérie dans les réseaux IMT-2020 et à établir en conséquence les capacités de sécurité à l'intention de l'opérateur, pour qu'il puisse protéger ses applications.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID Unique *
1.0	UIT-T X.1815	03-03-2023	17	11.1002/1000/15113

Mots clés

Services informatiques en périphérie, réseau IMT-2020, lignes directrices en matière de sécurité.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1815

Lignes directrices et exigences en matière de sécurité pour les services informatiques en périphérie fondés sur les IMT-2020

1 Domaine d'application

La présente Recommandation fournit un modèle de déploiement possible ainsi que des scénarios d'application types des services informatiques en périphérie, décrit les menaces pour la sécurité et les exigences de sécurité propres aux services informatiques en périphérie dans les IMT-2020 et définit en conséquence des lignes directrices concernant les capacités de sécurité à l'intention des opérateurs, pour qu'ils puissent protéger leurs applications.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation ou autre référence étant sujette à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T Y.3101] Recommandation UIT-T Y.3101 (2018), *Exigences relatives aux réseaux IMT-2020*.

[3GPP TS 23.501] 3GPP TS 23.50 (2022), *5G; System architecture for the 5G System (5GS) (version 17.4.0 Publication 17)*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 IMT-2020 [b-UIT-T Y.3100]: (conformément à la Recommandation [b-UIT-R M.2083]) systèmes, composantes de système et technologies associées qui fournissent des capacités nettement améliorées par rapport à celles décrites dans [b-UIT-R M.1645].

3.1.2 cheval de Troie [b-UIT-T E.800]: logiciel qui semble bénin, voire utile; mais le véritable but du logiciel, qui est caché, est de perturber le système ou de dérober des informations.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 service informatique en périphérie fondé sur les IMT-2020: service fourni via le système IMT-2020 qui permet d'héberger un service à proximité du point d'accès de l'équipement d'utilisateur, de manière à assurer une fourniture de services efficace, grâce à la réduction du temps de latence de bout en bout et de la charge sur le réseau de transport.

3.2.2 système IMT-2020: système défini par le Partenariat 3GPP, composé du réseau d'accès (AN) IMT-2020, du réseau central IMT-2020 et de l'équipement d'utilisateur (UE).

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AF fonction d'application *(application function)*

AMF fonction de gestion des accès et de la mobilité (*access and mobility management function)*

AN réseau d'accès *(access network)*

CDN réseau de fourniture de contenu *(content delivery network)*

DC centre de données *(data centre)*

DDoS déni de service réparti *(distributed denial of service)*

DN réseau de données *(data network)*

DNN nom de réseau de données *(data network name)*

DNS système de noms de domaine *(domain name system)*

EASDF fonction de découverte du serveur d'application en périphérie (*edge application server discovery function)*

EHE environnement d'hébergement en périphérie *(edge hosting environment)*

eMBB large bande mobile évolué *(enhanced mobile broadband)*

GW-C plan de commande de passerelle *(gateway-control plane)*

GW-U plan d'utilisateur de passerelle *(gateway-user plane)*

IFP indicateur fondamental de performance

IMS sous-système multimédia IP *(Internet protocol multimedia subsystem)*

IP protocole Internet *(Internet protocol)*

MEC informatique en périphérie de réseau mobile *(mobile edge computing)*

mMTC communications massives de type machine *(massive machine type communications)*

NAT traduction d'adresse réseau *(network address translation)*

NB IoT Internet des objets en bande étroite (*narrow band Internet of things*)

NEF fonction d'exposition de réseau *(network exposure function)*

NFVO orchestrateur de la virtualisation des fonctions de réseau *(network functions virtualization orchestrator)*

NRF fonction de référentiel de réseau *(network repository function)*

OSS systèmes d'appui opérationnels *(operation support systems)*

PDU unité de données de protocole *(protocol data unit)*

PSA ancrage de session d'unité de données de protocole *(protocol data unit session anchor)*

QoS qualité de service (*quality of service*)

RAN réseau d'accès radioélectrique *(radio access network)*

SBA architecture fondée sur les services *(service based architecture)*

SIM module d'identification de l'abonné (*suscriber identification module*)

SMF fonction de gestion de session *(session management function)*

TLS sécurité dans la couche transport *(transport layer security)*

UE équipement d'utilisateur *(user equipment)*

UPF fonction du plan d'utilisateur *(user plane function)*

URLLC communications ultra-fiables et à faible temps de latence *(ultra-reliable low latency communications)*

V2X de véhicule à tout autre élément *(vehicle to everything)*

VNFM gestionnaire des fonctions de réseau virtualisées *(virtualized network function manager)*

5 Conventions

La présente Recommandation utilise les conventions suivantes:

L'expression "**il est exigé**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

Le terme "**devrait**" indique une exigence qui est recommandée, mais qui n'est pas absolument nécessaire. Cette exigence n'est pas indispensable pour déclarer la conformité.

6 Aperçu de l'informatique en périphérie fondée sur les IMT-2020

Le réseau IMT-2020 permettra de fournir une large gamme de services, parmi lesquels les services large bande mobiles évolués (eMBB), les services fondés sur des communications massives de type machine (mMTC) et les services fondés sur des communications ultra-fiables et à faible temps de latence (uRLLC) [UIT-T Y.3101], sur une infrastructure de réseau et de ressources informatiques. Conformément aux principales caractéristiques et aux exigences identifiées pour le réseau IMT-2020, il est exigé que ce réseau soit plus efficace, personnalisé, intelligent, fiable et souple.

Pour assurer les services types dans le réseau IMT-2020, en particulier les services eMBB et uRLLC, l'informatique en périphérie est reconnue comme étant l'une des principales technologies permettant de satisfaire les indicateurs fondamentaux de performance (IFP) particulièrement exigeants du réseau IMT-2020, surtout pour ce qui est du faible temps de latence et de l'efficacité d'utilisation de la largeur de bande.

L'informatique en périphérie fondée sur les IMT-2020 permet à l'opérateur et au fournisseur de services tiers de déployer les services à proximité du point d'accès de l'utilisateur via le système des IMT-2020, ce qui permet de fournir des services avec une grande efficacité, grâce à la réduction du temps de latence et de la charge sur le réseau de transport.

6.1 Modèle de déploiement

L'architecture du système IMT-2020, tel que décrit par le Partenariat 3GPP dans son document sur le système IMT-2020, comprend deux options disponibles: l'une est fondée sur l'approche traditionnelle du point de référence et de l'interface, tandis que l'autre prévoit que les fonctions de réseau central interagissent entre elles au moyen d'une architecture fondée sur les services (SBA).

La Figure 6-1 décrit une architecture de système IMT-2020 reposant sur le Document [3GPP TS 23.501].

Du point de vue de l'opérateur, le modèle de déploiement des services informatiques en périphérie fondés sur les IMT-2020 et dotés d'une architecture SBA peut comporter les fonctions de réseau IMT-2020 suivantes:

– Fonction UPF (fonction du plan d'utilisateur, *user plane function)*: la fonction UPF est l'une des fonctions de réseau (NF) du réseau central IMT-2020. Elle est chargée de l'acheminement et de la retransmission des paquets, de l'inspection des paquets, du traitement de la qualité de service et de la session d'unités de données de protocole (PDU) externe pour l'interconnexion du réseau de données (DN), dans l'architecture des IMT-2020.

– Fonction AMF (fonction de gestion des accès et de la mobilité, *access and mobility management function)*: la fonction AMF reçoit toutes les informations relatives à la connexion et à la session de l'équipement UE via l'interface N1 et le réseau d'accès (radioélectrique) ((R)AN) via l'interface N2 (voir la Figure 1), mais est responsable uniquement du traitement des tâches liées à la gestion de la connexion et de la mobilité.

– Fonction SMF (fonction de gestion de session, *session management function)*: la fonction SMF est un élément fondamental de l'architecture SBA des IMT-2020. Elle est responsable, pour l'essentiel, de l'interaction avec le plan de données dissocié, de la création, de l'actualisation et de la suppression de sessions d'unités PDU, et de la gestion du contexte de session avec la fonction UPF.

– Fonction EASDF (fonction de découverte du serveur d'application en périphérie, *edge application server discovery function)*: la fonction EASDF comprend une ou plusieurs des fonctionnalités suivantes: inscription à la fonction de référentiel de réseau (NRF) pour la découverte de la fonction EASDF, sélection et traitement des messages du système de noms de domaine (DNS) conformément aux instructions provenant de la fonction SMF. La fonction EASDF dispose d'une connectivité directe avec le plan d'utilisateur (c'est-à-dire sans aucune traduction d'adresse réseau (NAT)) avec l'ancrage de session d'unités PDU (PSA) de la fonction UPF sur l'interface N6 pour la transmission de la signalisation du DNS échangée avec l'équipement UE.

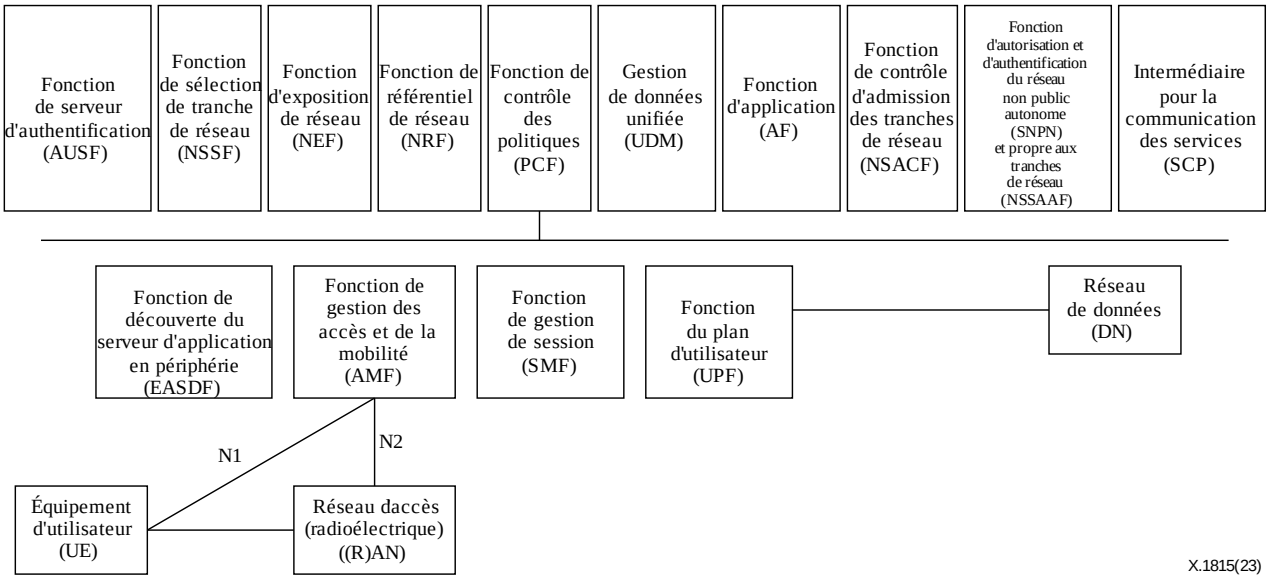

Figure 6-1 – Architecture du système des IMT-2020

La Figure 6-2 décrit un modèle de déploiement des services informatiques en périphérie fondés sur les IMT-2020.

Le système IMT-2020 prend en charge l'environnement d'hébergement en périphérie (EHE) déployé dans le réseau DN au-delà de l'ancrage PSA de la fonction UPF. Un environnement EHE peut être placé sous le contrôle l'opérateur ou de tiers [b-3GPP TS 23.548]. Le segment local du réseau DN dans lequel l'environnement EHE est déployé peut disposer d'une connectivité avec le plan d'utilisateur, avec à la fois un ancrage PSA déployé au niveau central et un ancrage PSA déployé au niveau local pour le même nom de réseau de données (DNN).

Du point de vue de l'opérateur, le modèle de déploiement des services informatiques en périphérie fondés sur les IMT-2020 est celui illustré dans la Figure 6-2.

– Centre de données en périphérie: fournit une fonctionnalité d'informatique en périphérie de réseau mobile (MEC) qui permet d'utiliser des services informatiques en périphérie fondés

sur les IMT-2020, ainsi que des fonctionnalités GW-U (plan d'utilisateur de passerelle) et UPF.

– Centre de données local: fournit les fonctionnalités suivantes: GW-U, CDN (réseau de fourniture de contenu) et UPF.

– Centre de données de la zone: fournit les fonctionnalités suivantes: GW-C (plan de commande de passerelle), AMF/SMF, Internet des objets (IoT) à bande étroite, sous-système multimédia IP (IMS), etc.

– Domaine de gestion: comprend une plate-forme de gestion en nuage, un orchestrateur de la virtualisation des fonctions de réseau (NFVO) et un gestionnaire des fonctions de réseau virtualisées (VNFM).

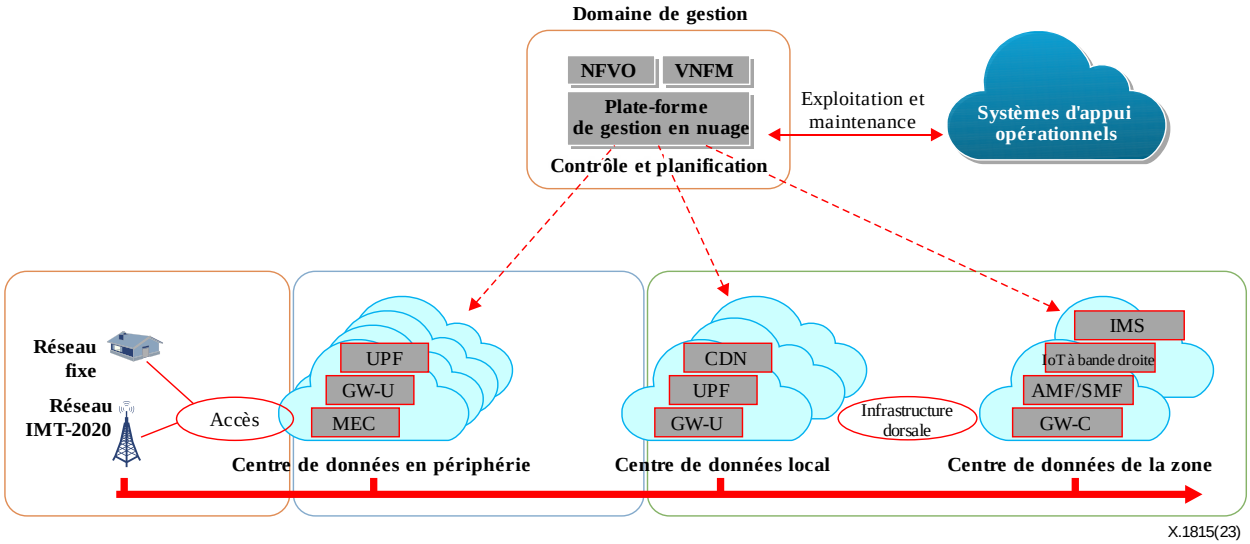

Figure 6-2 – Modèle de déploiement des services informatiques en périphérie fondés sur les IMT-2020

6.2 Scénario d'application type

6.2.1 Communications "de véhicule à tout autre élément" (V2X)

Dans le cas des communications V2X, la quantité de dispositifs connectés à applications multiples est à l'origine de besoins croissants en matière de transfert de données côté réseau. Le réseau est nécessaire pour fournir des capacités large bande et des capacités de calcul améliorées pour l'utilisation et le stockage des données.

En appliquant des technologies d'informatique en périphérie fondées sur les IMT-2020 pour les communications V2X, il est possible de déployer les applications dans le nœud d'extrémité, ce qui permet de réduire le temps de transmission de bout en bout et d'accroître la fiabilité conformément aux exigences propres aux différents services V2X (le service de conduite sans risque doit en effet être associé à des exigences rigoureuses en termes de temps de latence et de fiabilité), du fait de l'itinéraire de transmission plus court, et d'offrir des ressources de calcul et de stockage plus puissantes.

Les services fournis dans le cadre des communications V2X utilisant une technologie d'informatique en périphérie fondée sur les IMT-2020 sont notamment les suivants:

– Le service d'information: le service d'informatique en périphérie offre des fonctions de chargement et de mise à jour des cartes, de divertissement audio et vidéo et de détection à distance dans le véhicule. Ces fonctions requièrent un service d'informatique en périphérie offrant une capacité large bande mobile renforcée, par exemple au moins 25 Mbit/s pour le service de vidéo à haute définition 4K.

– Le service de conduite sans risque: le service d'informatique en périphérie aide le conducteur à prendre des décisions concernant la conduite du véhicule (par exemple, en émettant un avertissement de collision) grâce à l'acquisition d'informations sur le véhicule, sur les piétons et sur les unités situées en bord de route. Il est nécessaire que le service d'informatique en périphérie offre des capacités ultra-fiables avec un temps de latence faible (en règle générale, le temps de latence est de moins de 20 ms et la fiabilité des télécommunications est d'au moins 99%).
– Un service amélioré pour l'efficacité de la conduite: le service d'informatique en périphérie permet d'optimiser l'efficacité des installations de gestion du trafic sur la base des technologies de communication V2X fondées sur les IMT-2020 et des technologies d'analyse des mégadonnées, par exemple en ce qui concerne le contrôle des feux de signalisation et la vitesse du véhicule.

6.2.2 Internet des objets (IoT)

En appliquant des technologies d'informatique en périphérie fondées sur les IMT-2020 dans l'IoT, il est possible de déployer des applications dans le nœud d'extrémité, ce qui permet de réduire le temps de transmission de bout en bout du fait de l'itinéraire de transmission plus court et d'offrir des services plus efficaces grâce au calcul des données locales.

Les scénarios de service dans le cadre de l'IoT utilisant une technologie d'informatique en périphérie fondée sur les IMT-2020 comprennent notamment, mais non exclusivement:

– les villes intelligentes;
– les bâtiments intelligents;
– les maisons intelligentes.

6.2.3 Internet industriel

L'informatique en périphérie fondée sur les IMT-2020 prend en charge les services de l'Internet industriel (en particulier dans le cas des applications IoT en temps réel, pour lesquelles le traitement des données se fait généralement loin d'un centre de données centralisé et un temps de latence faible est une prescription obligatoire), en coordonnant le réseau IMT-2020 au moyen du contrôleur en périphérie, de la passerelle d'extrémité et du nuage en périphérie.

Le contrôleur en périphérie est chargé de l'orchestration des tâches, du déploiement des applications et de la gestion du cycle de vie depuis la passerelle d'extrémité, ainsi que du contrôle des dispositifs industriels, etc.

La passerelle d'extrémité met en œuvre l'orchestration des tâches, l'enregistrement des dispositifs industriels, le déploiement des applications et la gestion du cycle de vie depuis le nuage en périphérie et analyse les données en périphérie, etc.

Le nuage en périphérie met en œuvre l'orchestration des tâches, l'enregistrement des dispositifs industriels, le déploiement des applications et la gestion du cycle de vie depuis la passerelle en périphérie, coordonne les serveurs en périphérie et analyse les données en périphérie, etc.

7 Menaces pour la sécurité

Du point de vue des couches, la fourniture d'un service informatique en périphérie fondé sur les IMT-2020 suppose une couche infrastructure, une couche réseau et une couche application; c'est pourquoi il convient de tenir compte des menaces pour la sécurité liées à tous ces aspects. Il est important de noter que, même si l'informatique en périphérie de réseau mobile présente la caractéristique d'assurer la protection de la sécurité et de la vie privée car la transmission des données se fait directement à destination des serveurs MEC plutôt que par l'intermédiaire de serveurs centraux, ce qui réduit le risque de fuite lors de la transmission des données dans le réseau, l'exploitation d'un grand nombre de dispositifs mobiles et le déploiement de serveurs en nuage en périphérie amènent

des problèmes nouveaux en matière de sécurité. En particulier, les solutions traditionnelles pour assurer la sécurité dans l'informatique en nuage ne pourraient pas convenir pour l'informatique en périphérie de réseau mobile, étant donné que les environnements des dispositifs IoT en périphérie sont exposés à un certain nombre de menaces nouvelles très différentes de celles rencontrées dans la gestion traditionnelle du nuage. Dans la pratique, il est impossible d'appliquer aux dispositifs en périphérie les méthodes actuelles pour assurer la sécurité des données, car la plupart de ces dispositifs ont des ressources limitées et l'environnement très dynamique de l'informatique en périphérie de réseau mobile rend le réseau vulnérable. L'Agence de l'Union européenne pour la cybersécurité (ENISA) [b-ENISA] a effectué une évaluation complète des vulnérabilités portant sur les spécifications 5G définies dans la version 16 de la norme 3GPP. Ainsi, la mise en place d'un environnement MEC pour les applications 5G futures tout en garantissant la sécurité reste une question à examiner plus avant dans le proche avenir.

7.1 La couche infrastructure

7.1.1 Plate-forme de gestion du nuage

Le déploiement d'un service d'informatique en périphérie fondé sur les IMT-2020 peut nécessiter une plate-forme de gestion en nuage. Outre les menaces pour la sécurité en général qui pèsent sur une telle plate-forme, l'auteur d'une attaque peut utiliser l'interface entre la plate-forme de gestion en nuage et le réseau IMT-2020 pour lancer une autre attaque sur le réseau IMT-2020.

7.1.2 Infrastructure virtualisée

L'infrastructure virtualisée peut être indisponible si les ressources physiques sont attaquées ou endommagées. Cette vulnérabilité potentielle peut être exploitée par l'auteur d'une attaque pour obtenir un accès non autorisé au système de gestion des ressources virtuelles et modifier les informations relatives à la configuration.

7.1.3 Injection d'éléments matériels ou logiciels malveillants

Des éléments matériels et logiciels non autorisés, connus sous le nom de "chevaux de Troie" peuvent être injectés dans l'infrastructure, afin de dégrader l'efficacité des serveurs et des dispositifs de périphérie existants, voire de rendre possible l'exploitation des fournisseurs de services [b-Daniel]. Les entités qui fournissent des solutions logicielles et matérielles pour le service d'informatique en périphérie peuvent ainsi exécuter, sans le vouloir, des activités malveillantes pour le compte de l'auteur d'une attaque.

7.1.4 Altération physique volontaire des dispositifs

Une altération physique volontaire des dispositifs a davantage de chances de se produire, dans la mesure où, dans l'architecture en périphérie, les ressources informatiques sont plus proches des auteurs possibles d'une attaque. L'auteur d'une attaque peut détruire un nœud d'extrémité et, par voie de conséquence, compromettre l'efficacité de l'ensemble du réseau.

7.2 La couche réseau

7.2.1 Analyser le flux de réseau

L'auteur d'une attaque peut suivre et/ou dérober des données de liaison et analyser les caractéristiques des flux pour obtenir des informations sur les services, et ainsi poursuivre ses attaques sur le réseau.

7.2.2 "Reniflage" de la topologie de réseau

L'auteur d'une attaque peut compromettre le nœud de service qui peut être déployé dans des environnements ouverts, afin de lancer une attaque visant à "renifler" la topologie du réseau.

7.2.3 Attaque par déni de service réparti (DDoS)

L'auteur d'une attaque peut compromettre les utilisateurs abonnés et/ou les nœuds de service qui peuvent être déployés dans des environnements ouverts, afin de lancer une attaque par déni de service réparti. Lorsque des attaques par déni de service réparti sont commises, une ressource de réseau existante est submergée de trafic provenant d'autres ressources compromises dans le réseau, ce qui constitue un autre risque de sécurité lié à l'informatique en périphérie.

7.2.4 Écoute clandestine ou manipulation des données de communication

Les services qui utilisent l'informatique en périphérie fondée sur les IMT-2020 s'appuient sur le réseau hertzien ouvert. L'auteur d'une attaque peut écouter clandestinement ou manipuler les données de communication; dans certains scénarios, par exemple dans l'industrie manufacturière et les villes intelligentes, les données de communication peuvent comprendre des informations d'une importance centrale, comme les identificateurs et les justificatifs des utilisateurs, des informations commerciales et des informations concernant la sécurité publique.

7.2.5 Attaque transversale

Dans la mesure où le service d'informatique en périphérie au sein du réseau IMT-2020 doit coordonner les fonctionnalités entre le réseau d'accès, le réseau central et la plate-forme de gestion en nuage, l'existence de ce point faible peut entraîner une attaque transversale, qui rend indisponibles le réseau et le service.

7.2.6 Accès non autorisé

Afin de permettre à l'équipement d'utilisateur de se connecter au meilleur service d'informatique en périphérie, il est nécessaire de signaler les interactions entre l'équipement d'utilisateur et le réseau central IMT-2020. Si la signalisation est altérée par l'auteur d'une attaque, un accès non autorisé au service d'informatique en périphérie peut être obtenu, et une attaque par déni réparti peut même être possible.

7.2.7 Exposition du réseau aux applications en périphérie

Le réseau IMT-2020 peut exposer les informations de réseau à la fonction d'application locale, rendant possibles des scénarios tels que l'exposition des informations de réseau locales de l'ancrage PSA de la fonction UPF à la fonction d'application locale, directement ou via la fonction d'exposition du réseau local.

7.2.8 Attaques visant les informations de routage

Une attaque visant les informations de routage, ou plus simplement, une attaque au niveau du routage, se produit sur la couche réseau d'un réseau en périphérie. Les attaques au niveau du routage perturbent la manière dont le trafic est transféré au sein d'un réseau, ce qui peut avoir des effets sur le débit, le temps de latence et l'acheminement des données.

7.2.9 Détournement de session

Le pirate intercepte et détourne une session d'utilisateur pour obtenir l'accès aux données et aux services d'utilisateur.

7.3 La couche application

7.3.1 Vulnérabilité du cadre technique

Dans les services d'informatique en périphérie fondée sur les IMT-2020, dans la mesure où une très grande quantité de nœuds utilisent le même cadre technique pour différents scénarios et secteurs verticaux, si un nœud est compromis, les autres le sont également.

7.3.2 Utilisation non autorisée

La menace liée à une utilisation non autorisée se produit lorsqu'un utilisateur non autorisé ou non abonné obtient un accès aux services d'informatique en périphérie fondée sur les IMT-2020, en se faisant passer pour une entité autorisée.

7.3.3 Chevaux de Troie et virus

Les attaques fondées sur les chevaux de Troie et les virus se produisent lorsqu'un service d'informatique en nuage fondée sur les IMT-2020 malveillant ou un assaillant se fait passer pour un fournisseur de services légitime et injecte des chevaux de Troie ou des virus dans une application, ce qui peut porter atteinte aux dispositifs et aux données de l'utilisateur, voire déclencher une attaque supplémentaire sur le réseau de télécommunication mobile.

7.3.4 Divulgation de données

La divulgation des données se produit lorsque les assaillants se font passer pour une entité légitime afin de recueillir des données durant les processus de migration, de transmission, de stockage, de partage et de destruction des données d'application d'un service d'informatique en périphérie.

8 Exigences en matière de sécurité

8.1 Couche infrastructures

Les exigences en matière de sécurité d'une plate-forme de gestion en nuage devraient être les suivantes:

a) Prise en charge, par la plate-forme de gestion en nuage, de l'authentification et de l'autorisation pour la passerelle du plan de données, la gestion de la plate-forme d'informatique en périphérie et l'application d'informatique périphérique.

b) Protection des données sensibles afin de bloquer les accès non autorisés et d'empêcher l'altération des données (par exemple, dans les scénarios industriels, il est nécessaire de protéger les données sensibles concernant la production pour mener à bien les processus industriels et éviter les interruptions dues aux attaques visant le réseau).

c) La plate-forme de gestion en nuage devrait être isolée de manière sécurisée par des éléments du réseau central IMT-2020 (par exemple les fonctions NEF et UPF).

d) Analyses des canaux latéraux, pour détecter les chevaux de Troie à l'aide d'analyses de la synchronisation, de l'alimentation et de la température spatiale. Cette méthode permet essentiellement de détecter les micrologiciels ou logiciels malveillants installés sur les nœuds périphériques, en identifiant les comportements inhabituels du système, tels que l'augmentation du temps d'exécution et de la consommation d'énergie.

e) Méthodes de détection des chevaux de Troie, permettant de comparer le matériel infecté et le matériel qui ne l'est pas, pour détecter les attaques malveillantes.

f) Sécurité physique de tous les nœuds périphériques qui ne sont pas placés dans des centres de données périphériques hautement sécurisés, par exemple en utilisant des techniques de protection physique supplémentaires pendant la fabrication ou en mettant en œuvre des mécanismes de verrouillage et d'autres protections physiques sur le terrain.

g) Indépendamment de ce qui précède, il est exigé que les parties du système périphérique responsables du matériel cryptographique soient protégées contre les attaques par canal latéral moyennant, par exemple, l'utilisation de cartes SIM renforcées et résistantes.

Les exigences en matière de sécurité de l'infrastructure virtualisée devraient être les suivantes:

a) Si l'infrastructure du service informatique en périphérie IMT-2020 est déployée par une machine virtuelle, la vCPU, la mémoire et les entrées/sorties de la machine virtuelle devraient être isolées de manière sécurisée.

b) L'infrastructure virtualisée devrait gérer l'isolation sécurisée des conteneurs.

c) L'infrastructure virtualisée devrait également gérer la duplication miroir des bases de données et des signatures.

d) La segmentation avec le découpage de réseaux devrait séparer le trafic et isoler les ressources de calcul [b-ENISA].

8.2 Réseau

Les exigences en matière de sécurité des réseaux de télécommunications devraient être les suivantes:

a) Prise en charge de la protection de la confidentialité et de l'intégrité pour la transmission de données.

b) Utilisation d'un protocole de sécurité (par exemple, TLS v1.2) pour établir un canal sécurisé entre les éléments du réseau.

c) Utilisation du chiffrement du trafic de données entre les parties au moyen d'un protocole de transport sécurisé de bout en bout, utilisation d'une chaîne ou d'un nombre long et aléatoire comme clé de session, et réinitialisation de l'identificateur de la session après chaque connexion réussie.

d) Prise en charge de la capacité de protection contre les attaques DDoS en filtrant soigneusement le trafic, afin que les demandes non légitimes ne soient pas autorisées, et que les demandes légitimes soient transmises sans retard significatif.

Les exigences en matière de sécurité relatives à la gestion du réseau devraient être les suivantes:

a) Les systèmes d'appui à l'exploitation (OSS) devraient prendre en charge l'authentification et l'autorisation pour l'interaction avec la plate-forme de gestion en nuage.

b) Les fonctions entre la gestion des services informatiques en périphérie et l'OSS devraient être isolées de manière sécurisée.

c) Le réseau devrait être constamment surveillé pour savoir s'il est lent ou défectueux, et les attaques ou problèmes de réseau devraient être signalés à temps.

d) Des protocoles de routage fiables devraient être mis en place.

8.3 Couche application

Les exigences en matière de sécurité relative à l'application périphérique devraient être les suivantes:

a) Mise en œuvre d'une évaluation de la sécurité comprenant un contrôle de la conformité en matière de sécurité, la gestion des actifs, une recherche des virus, etc.

b) Prise en charge par l'application périphérique de l'authentification et de l'autorisation pour les interactions entre la plate-forme de gestion en nuage et d'autres applications périphériques.

c) Protection des données sensibles afin de bloquer les accès non autorisés et d'empêcher l'altération des données.

d) Prise en charge de la vérification de l'intégration pour l'application périphérique.

e) Vérification de l'identité et de l'autorité de l'administrateur pendant le chargement et l'utilisation de l'application périphérique.

f) Prise en charge de la protection de la confidentialité et de l'intégration en ce qui concerne les processus de migration, de transmission, de stockage, de partage et de destruction des données.

g) Prise en charge de la fonction d'identification automatique et de sécurité renforcée fondée sur l'extension de la sécurité du langage du programme et l'analyse statique du programme.

h) Prise en charge des fonctions de surveillance, d'analyse et d'alarme en temps réel pour la qualité de fonctionnement de l'application, le trafic, le canal source et l'environnement client.

i) Prise en charge de l'audit de l'application, recueil régulier des journaux de sécurité des dispositifs d'extrémité et applications périphériques, stockage et analyse de ces journaux, puis notification et traçage des violations et des abus commis par l'application ainsi que de ses comportements anormaux.

9 Lignes directrices relatives aux capacités de sécurité du service informatique en périphérie

9.1 Couche infrastructure

Pour répondre aux exigences en matière de sécurité de l'infrastructure, les capacités de sécurité requises devraient être les suivantes:

a) Surveillance des risques liés à la sécurité des données et notification rapide permettant d'empêcher l'altération et la fuite des données.

b) Stockage sécurisé des données, avec des capacités de stockage crypté et d'encapsulation des données sensibles.

c) Capacités de protection de la sécurité de la plate-forme virtualisée, par le renforcement de la sécurité du système, l'isolation de la sécurité, le contrôle de la sécurité, le cryptage des données et d'autres capacités permettant de garantir la sécurité des données dans le réseau virtualisé.

d) Fonctions de sécurité permettant de garantir la sécurité des fonctions NF virtualisées, notamment:

- procédures d'authentification;
- contrôle d'accès;
- vérification à distance de la sécurité du système;
- sécurité des communications;
- attestation;
- duplication miroir;
- signature;
- isolation de sécurité;
- enclaves d'exécution passant par le matériel;
- racine de confiance relative au matériel;
- cryptage matériel;
- environnement d'exécution fiable;
- stockage à cryptage automatique;
- accès direct à la mémoire;
- modules de sécurité matériels;
- protection et vérification de l'intégrité des logiciels.

9.2 Couche réseau

Les capacités de sécurité pour la couche réseau qui devraient être fournies sont notamment, mais non exclusivement, les suivantes:

a) Capacités de protection de la confidentialité et de l'intégrité de la transmission des données, telles que l'horodatage, le numéro de série, le cryptage des liaisons et autres mécanismes.

b) Prise en charge des capacités visant à empêcher le détournement de session, telles que le cryptage du trafic de données entre les parties, l'utilisation d'une chaîne ou d'un nombre long et aléatoire comme clé de session, et la réinitialisation de l'identificateur de la session après une connexion réussie.

c) Contrôle de la sécurité des données pour les nœuds périphériques, y compris l'authentification de l'identité, l'isolation de sécurité, la surveillance continue et l'alerte rapide, ainsi que le cryptage, la désensibilisation et la sauvegarde des données.

d) Protocoles de routage fiables.

9.3 Couche application

Les capacités de sécurité pour la couche application qui devraient être fournies sont notamment, mais non exclusivement, les suivantes:

a) Contrôle des autorisations d'application pour les différents utilisateurs et scénarios, afin de garantir la confidentialité, l'intégrité et la disponibilité des données et des services de l'application.

b) Protection contre les attaques de virus et mise à jour en temps utile de la base de données des virus, afin d'éviter les fuites ou vols de données.

c) Identification et évaluation des données sensibles, y compris l'autorisation de désensibilisation, le stockage crypté, la surveillance et le suivi, l'alarme en cas de conditions anormales, la gestion des audits, la destruction et d'autres capacités.

d) Identification de l'identité, suivi continu et alerte rapide.

Bibliographie

[b-ITU-T E.800] Recommandation UIT-T E.800 (2008), *Définition de termes relatifs à la qualité de service.*

[b-ITU-T X.1811] Recommandation UIT-T X.1811 (2021), *Lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes IMT-2020.*

[b-ITU-T Y.3100] Recommandation UIT-T Y.3100 (2017), *Réseaux IMT-2020: termes et définitions.*

[b-ITU-R M.1645] Recommandation UIT-R M.1645 (2006), *Cadre et objectifs d'ensemble du développement futur des IMT-2000 et des systèmes postérieurs aux IMT-2000.*

[b-ITU-R M.2083] Recommandation UIT-R M.2083 (2015), *Vision pour les IMT ainsi que les cadres et les objectifs généraux du développement futur des IMT à l'horizon 2020 et au-delà*.

[b-3GPP TS 23.548] 3GPP 23.548 (2021), 5G system enhancements for edge computing (version 17.2.0 release 17) (*Améliorations du système 5G destinées à l'informatique en périphérie*).

[b-Daniel] B. Daniel, Is edge computing secure? Here are 4 security risks to be aware of (*L'informatique en périphérie est-elle sûre? 4 risques de sécurité dont il faut être conscient*) 9 décembre 2020. https://www.trentonsystems.com/blog/is-edge-computing-secure.

[b-ENISA] Agence de l'Union européenne pour la cybersécurité (ENISA), *ENISA Threat Landscape for 5G Networks (État des lieux des menaces de l'ENISA concernant les réseaux 5G),* décembre 2020. Disponible à l'adresse: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2023