RINA™ Recursive InterNetwork Architecture

Nouvelle génération Internet

Rolland Tran Van Lieu

Forum ATENA

V2.0-8 Février 2022 (Photo Source Shutterstock)

Table des matières

GLOSSAIRE 3

CHAPITRE 1 : INTRODUCTION 5

CHAPITRE 2 : CHOIX FONDATEURS DE RINA™ 8

CHAPITRE 3 : COMPOSANTS FONCTIONNELS D'UN PROCESSUS APPLICATIF RINA™ 10

CHAPITRE 4 : ECHANGES ENTRE AP AU SEIN D'UN DIF 13

CHAPITRE 5 : PROJETS DE RECHERCHE 17

CHAPITRE 6 : PROJETS INDUSTRIELS 22

CHAPITRE 7 : SOUVERAINETE NUMERIQUE DE L'EUROPE 27

ANNEXE 1 : RAPPEL DES NOTIONS SUR L'OSI 29

ANNEXE 2 : CYBER SECURITE 31

ANNEXE 3 : EVENEMENTS SUR RINA™ 32

ANNEXE 4 : LIVRES SUR LES TELECOMS 33

L'AUTEUR 34

Glossaire

Acronyme	Définition
AE	Application Entity
AF	Allocate Flow
AFNOR	Association française de normalisation
ANSSI	Agence Nationale de la sécurité des systèmes d'information
AP	Application Process
API	Application Programming Interface
ASN 1	Abstract Syntax Notation 1
ATM	Asynchronous Transfert Mode
BGP	Border Gateway Protocol
CDAP	Commun Distributed Applicatif Protocol
CEP_id	Connection End Point Identifier
CMIP	Common Management Information Protocol
CRC	Calcul de Checksum
DA	DIF Allocator
DAF	Distributed Application Facility
DIF	Distributed IPC Facility
DNS	Domain Name System
DNSSEC	Domain Name System Security
DTP	Data Transfert Protocol
DTPC	Data Transfert Protocol Control
ETSI	European Telecommunications Standards Institute
EFCP	Error and Flow Control Protocol
FA	Flow Allocator
FTP	File Transfert Protocol
FTAM	File Transfert Access and Management
HTTP	Hypertext Transfert Protocol
IA	Intelligence Artificielle
IDD	Inter DIF Discovery
IEC	International Electrotechnical Commission
IOT	Internet Of Things
ISO	International Standardization Organization
IPC	Inter Processus Communication
IRM	IPC Resource Manager
ITU	International Telecommunications Union
IP	Internet Protocol Version 4 ou Version 6
IPsec	Internet Protocol Security
IS-IS	Intermediate System to Intermediate System (protocole de routage OSI)
LDAP	Lightweight Directory Acces Protocol
MMS	Manufacturing Message Specification

MPLS	Multi-Protocol Label Switching IP/MPLS et MPLS_TP (Transport Protocol)
NTP	Network Time Protocol
OAM	Operation Administration and Maintenance
OS	Operating System
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PCI	Protocol Control Information
PDU	Protocol Data Unit
PIM	Protocol Independent Multicast
QOS	Quality Of Service
RA	Ressource Allocator
RIB	Ressource Information Base
RIB Deamon	Ressource Information Base Deamon
RINA	Recursive InterNetwork Architecture
RMT	Relaying and Multiplexing Task
RSVP	Resource Reservation Protocol
URL	Uniform Resource Locator
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SI	Système d'Information
SIIV	Système d'Information d'importance Vitale
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfert Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TP	Transport OSI
UCP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
X25	Protocole de commutation par paquet

(*) L'objectif de ce Livre blanc est de partager et diffuser les connaissances sur **RINA™** en France. Il s'adresse en premier lieu aux étudiant(e)s dans le domaine du numérique (informatique, télécom et cyber sécurité). Ce livre blanc est accessible à un professionnel de l'IT et à un public non spécialiste mais curieux. De nombreux liens vers les projets de recherche et industriels vous permettent d'approfondir ainsi vos connaissances.

Bonne lecture et au plaisir d'échanger avec vous sur RINA™ à travers Forum ATENA.

Chapitre 1 : Introduction

INTERNET bâtit dans les années 1970, a permis le développement et l'essor d'E-commerce (**BtC, BtB, BtM**) que nous connaissons aujourd'hui. Le marché mondial s'est élevé en 2021 à 4891 milliards de dollars[1]. D'après InternetLiveStats[2], on comptabilise en 2022 plus de 1,9 milliards de sites Web et plus de 5 milliards d'utilisateurs dans le monde.

De nouvelles technologies apparaissent: Réseau mobile 5G, IoT, WIFI 6, IA, Blockchain, Réseau optique à ultra haut débit, Ordinateur quantique, Big data, Constellation satellitaire.

Des nouveaux usages se développent: Usine 4.0, Voiture connectée, Jumeaux numériques, Smartgrid, Smartcities, Domotique, Vidéo en streaming 4K/8K, Jeux vidéo en réseau, Télémédecine, Metaverse.

Une question légitime qui nous vient à l'esprit : est-ce que l'INTERNET, pensé et développé depuis plus de 40 ans jusqu'à maintenant, peut-il faire face à ces nouveaux défis ?

Des voix célèbres (Mr Louis Pouzin et Mr John Day) se lèvent pour demander une refondation de l'INTERNET actuel :

- Mr **Louis Pouzin** est le concepteur du réseau Cyclades qui était le 1er réseau datagramme au monde (à l'IRIA en 1974 ancêtre de l'INRIA actuel). Il est actuellement fondateur de la société « **Open-Root** » concurrent de l'ICANN.

- Mr **John Day** est un des anciens concepteurs du réseau d'ARPANET ancêtre du réseau INTERNET actuel. Il a aussi participé activement à la définition du célèbre modèle OSI en 7 couches et des protocoles OSI associés (FTAM, CMIP, ASN1, MMS, transport TP).

Le socle technique de l'INTERNET est basé sur les 4 composants **TCP**, **IP**, **DNS** et **BGP**. Ce socle sur lequel se repose l'économie numérique mondiale, est bancal: problème de sécurité, pas de qualité de service en natif, pas de multi homing, pas de multicast, pas de mobilité. Bref, l'exploitabilité d'INTERNET devient très complexe au fil des années.

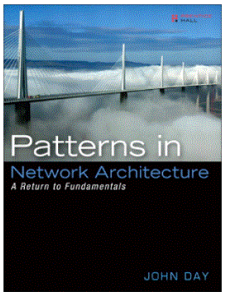
De nombreux protocoles additionnels sont développés pour compenser les faiblesses de ces derniers: La liste est très longue : TLS, IPsec, MPLS, RSVP, IP V6, DNSSEC, OSPF, SNMP, Mobile IP…

[1] https://www.alioze.com/chiffres-web#ecommerce-2020
[2] https://www.internetlivestats.com/

Pour Mr John Day et Mr Louis Pouzin, Il est temps de tourner la page d'INTERNET qui est devenu trop complexe à gérer et à administrer. La nouvelle architecture proposée a pour nom **RINA™** (**Recursive InterNetwork Architecture**).

RINA™ est issu des travaux de recherche de Mr John Day (Université de Boston). RINA™ bénéficie de son retour d'expériences de plus de 50 ans dans le domaine des systèmes informatiques répartis. RINA™ est une architecture générique. RINA™ est conçu pour une grande variété de machines, de réseaux, d'applications et de services actuels et futurs.

La spécification de l'architecture RINA™ est décrite dans le livre de Mr John Day « **Patterns in Network Architecture, a return to Fundamentals** ».



Dans Internet, une application ne possède pas de nom (URL) à proprement parlé. Elle est identifiée et rattachée par son adresse réseau IP et par son port TCP/UDP.

Une adresse IP n'est pas unique pour une machine donnée. L'adresse IP est fortement liée à son interface Ethernet. Un routeur IP, rattaché à 3 interfaces Ethernet, possède 3 adresses IP différentes (1 adresse IP par interface). Cette contrainte fait augmenter la taille des tables de routage et complexifie la mise en œuvre du multi-homing et de la mobilité.

Les ports TCP/UDP de certaines applications sont connus de tous : FTP (port 20/21), SMTP (port 25), DNS (port 53), HTTP (port 80), NTP (port 123), LDAP (port 389), BGP (179). Les écoutes de ports et les attaques par saturation de ports pour faire tomber l'application sont légions.

Le serveur DNS offre un service de résolution de nom d'URL par exemple www.forumatena.org en une adresse IP et inversement. Le DNS racine est géré par l'ICANN un organisme lié au département du commerce américain. Le DNS, indispensable pour le bon fonctionnement de l'Internet, est très vulnérable aux cyber-attaques : attaque pour corrompre les requêtes DNS, pollution de cache DNS par exemple.

BGP4 est un protocole utilisé entre les opérateurs télécoms de niveau Tier1, Tier2 et Tier3 pour annoncer respectivement leurs AS et leurs routes IP publiques. Les routeurs BGP sont interconnectés au niveau des points de Peering situés généralement dans des Datacenters.

BGP est basé initialement sur la confiance entre les opérateurs. Une session entre 2 routeurs voisins n'est pas authentifiée. De plus, aucune vérification n'est effectuée lors des annonces des routes. Il n'y a pas de chiffrement des échanges. Des problèmes de sécurité apparaissent inévitablement :

. Man in the Middle, usurpation de routes IP, détournement de trafic IP…

Des contres mesures existent. Mais elles ne sont pas généralisées. En effet il faut pour cela mettre à jour l'ensemble des routeurs BGP et avoir une même politique de sécurité au niveau mondial. Ce n'est pas encore le cas.

IP v6 (RFC1752) est une nouvelle version du protocole IP avec les fonctionnalités suivantes :

. 128 bits pour l'adressage au lieu de 32bits avec IPv4

. Mobilité, Gestion des priorités, Qualité de services

. Sécurité, authentification, chiffrement des paquets (IPsec)

IPV6 est incompatible avec IPV4 et son déploiement est lent chez les opérateurs télécoms. Les entreprises hésitent à migrer leurs réseaux privés (intranet, industriels) vers IPV6 à cause des investissements lourds dans les équipements réseaux et surtout dans les applications métiers. Elles n'ont pas de contraintes de saturation d'adresses IP publiques car elles utilisent des plages d'adresses IP privées (RFC 1918).

Cette modernisation est incomplète car au-dessus d'IPV6 on retrouve les protocoles TCP/UDP avec les mêmes faiblesses. De plus sur le plan politique, ICANN qui a la main mise sur le DNS mondial IPV4 a peur de migrer vers un DNS IPV6 de peur de perdre son hégémonie. La Chine par contre accélère à grand pas la migration vers IPV6.

Chapitre 2 : Choix fondateurs de RINA™

RINA™ est bâti autour d'un ensemble de concepts simples, puissants. Cette architecture «**générique**» repose sur 8 choix fondamentaux qui sont:

- **La récursivité** : Les composants génériques sont décrits au chapitre3 de ce livre blanc. Ils offrent des services de base qui sont réutilisables lors de la construction d'un nouveau DIF. Cette propriété récursive évite aux développeurs de ré écrire du code. Les gains de coût et de délai de développement sont conséquents. Un DIF peut être vu comme un groupe fermé d'abonnés (notion X25) ou VPN (MPLS).

- **L'unification des communications**: Toutes les communications entre processus se font par échanges de messages asynchrones (datagramme) au sein d'un même DIF (IPC Inter Processus Communication). Un service élémentaire de communication est en mode connecté et de type bidirectionnel.

- **Le nommage et l'adressage** : Tout processus applicatif est identifié par un nom (chaine de caractères) qui est unique et univoque au sein d'un DIF. Un DIF est composé d'un ensemble de processus applicatifs. L'ensemble des noms sont stockés dans un annuaire de noms. Un processus applicatif RINA™ est composé d'un nom et d'une adresse au sein d'un DIF.

- **La mobilité** : Elle est native dans RINA™ du fait que le processus applicatif est identifié par son nom. Ainsi un processus applicatif RINA™ peut se déplacer (notion de roaming dans les réseaux mobiles) à l'intérieur d'un DIF. Il sera toujours identifié par son nom. Si le processus applicatif change de DIF, son nom sera conservé et aura par contre une nouvelle adresse au sein de ce nouveau DIF.

- **Le multi homing** : il est natif dans RINA™ du fait que le processus applicatif est identifié par son nom. Ainsi un processus applicatif RINA™ peut être raccordé simultanément à 2 (ou plusieurs) réseaux pour augmenter la disponibilité. En cas de perte d'un premier réseau, le flux applicatif transite via le deuxième réseau.

- **La qualité de services** : Elle est native dans RINA™. La QOS est caractérisée par les indicateurs suivants : la bande passante, le délai de transit (temps mis par un datagramme pour parcourir l'ensemble du chemin jusqu'à sa destination), la gigue (écart temporel séparant deux datagrammes à leur arrivée alors qu'ils ont été envoyés consécutivement), le taux de perte de trames.

- **La sécurité des échanges** : La sécurité est native dans RINA™. Plusieurs mécanismes sont mis en place pour assurer cette sécurité globale.

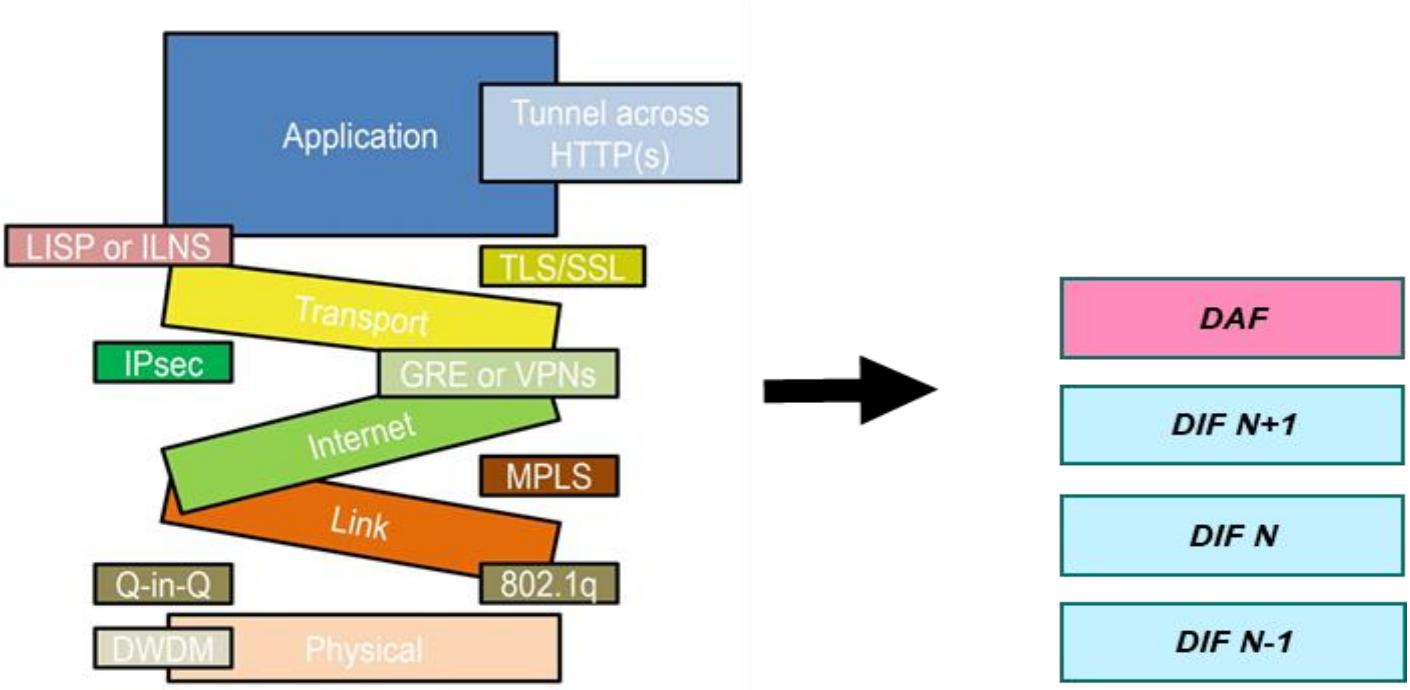
    - l'architecture RINA™ propose le concept de groupe fermé d'abonnés ou VPN. Un nouvel IPC doit faire partie d'un DIF pour pouvoir s'échanger. Le nouvel IPC doit respecter pour cela une procédure d'enregistrement à un DIF

    - les ports RINA™ ne sont pas transmis dans les entêtes contrairement à TCP/UDP. Ils ont une signification locale. Ce qui rend caduc le scanning de port et les attaques par saturation de port

    - l'utilisation des certificats normalisés X509 permet d'authentifier et chiffrer les échanges entre 2 applications AP

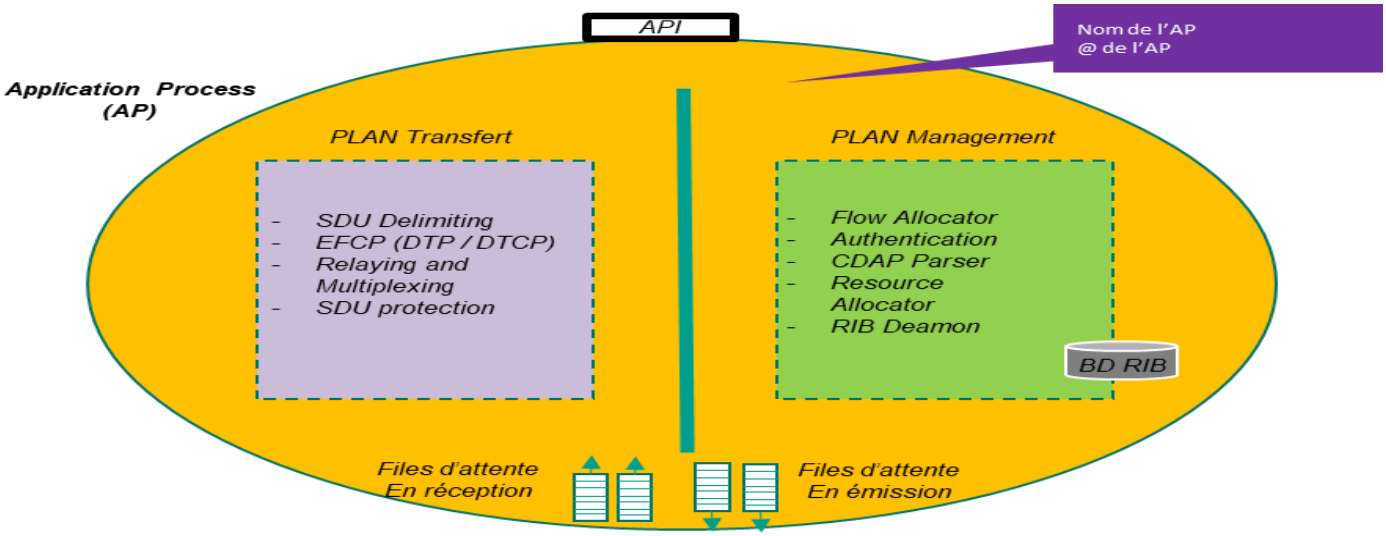
- **La supervision et l'administration** globale de l'architecture RINA™ sont natives ce qui permet de garantir la performance, la disponibilité et la sécurité.

L'objectif sera de passer de l'architecture actuelle basée sur TCP/IP qui est bancale vers l'architecture RINA™ :



Chapitre 3 : Composants fonctionnels d'un processus applicatif RINA™

Ce chapitre détaille le rôle des composants génériques qui sont essentiels au bon fonctionnement d'un processus applicatif RINA™ :



L'accès aux services RINA™ se fait via un API standardisé qui est composé de 6 services de base :

- **Register Application** : permet d'enregistrer un processus applicatif au sein d'un DIF
  Lors de l'appel de cette fonction, les paramètres à passer sont (nom du processus applicatif, nom du DIF)

- **Allocate Flow**: permet d'établir une connexion entre 2 processus applicatifs. Des ressources nécessaires sont allouées pour les échanges entre un processus applicatif émetteur et un processus applicatif récepteur. Lors de l'appel de cette fonction, les paramètres à passer sont (nom AP source, nom AP destinataire, type d'échange DTP/DTPC, niveau de QOS, niveau de sécurité..). En retour l'appel de fonction fournit un port en émission/réception

- **Send** : permet d'envoyer les messages (SDU) par un processus applicatif émetteur. Lors de l'appel de cette fonction, les paramètres à passer sont (port, le message à envoyer)

- **Receive** : permet de recevoir les messages par un processus applicatif récepteur. Lors de l'appel de cette fonction, le paramètre à passer est (port). En retour, l'appel de fonction indique le message reçu

- **Deallocate Flow** : permet de fermer une connexion applicative établie. Les ressources réservées pour les échanges sont ainsi désallouées

- **Unregister Application** : permet de désinscrire un processus applicatif au sein d'un DIF
  Lors de l'appel de cette fonction, les paramètres à passer sont (nom du processus applicatif, nom du DIF)

Pour permettre les échanges applicatifs, Un processus applicatif (AP) s'appuie sur 2 plans. Chaque plan joue une fonction particulière :

⇨ **Plan de gestion « Management » :** est organisé en 2 services

- **Contrôle :** Il permet d'établir dynamiquement une connexion entre 2 AP (source et destinataire) au sein d'un DIF

- **Gestion :** il permet de gérer les opérations d'exploitation-administration-maintenance (OAM - Operation Administration Maintenance)

Ces 2 grandes fonctions sont basées sur le protocole CDAP (Common Distributed Application Protocol).

Les 8 messages protocolaires (PDU) CDAP sont les suivants:

- *M_Connect*: demande de connexion
- *M_Release*: demande de déconnexion
- *M_Create*: demande de création d'un objet dans la BD RIB
- *M_Delete*: demande de suppression d'un objet dans la BD RIB
- *M_Read*: demande de lecture d'un objet dans la BD RIB
- *M_Write*: demande d'écriture d'un objet dans la BD RIB
- *M_Start*: demande de démarrage d'un appel de fonction
- *M_Stop*: demande d'arrêt d'un appel de fonction

Les composants qui participent à ces 2 services sont :

- **Flow allocator** et **ressource allocator** : alloue ou désalloue les ressources

- **Authentication** : Authentifie le processus applicatif émetteur/récepteur

- **CDAP parser/generator** : basé sur 'Google Buffer' ou ASN1 pour la définition et l'encodage des données

- **RIB** : Ressource Information Base est une BD qui stocke l'ensemble des données (nom des processus applicatifs, les paramètres de QOS et de sécurité)

- **RIB deamon** : Il est en charge du routage, de la recherche du chemin le plus court pour joindre le processus applicatif récepteur. Il est en charge aussi du mapping entre le nom du processus applicatif avec son adresse au sein d'un DIF. Il maintient la base RIB à jour

  CDAP est un protocole de routage de type "link state" basé sur le coût, le débit de la liaison, le temps de transit. La charge de trafic correspondante est négligeable. La taille des tables de routage est faible. Le temps de convergence est beaucoup plus rapide (quelques secondes)

  Les tables de routage sont modifiées régulièrement en fonction de l'évolution de la topologie du réseau. CDAP assure des fonctions de routage adaptatif et permet une sécurisation en cas de rupture d'un lien, de défaillance d'un routeur ou de congestion

⇨ **Plan de transfert de données « Data transfert » :** Une fois que la connexion est établie par le protocole CDAP, ce plan a pour but de transférer les données de bout en bout entre 2 processus applicatifs (source et destinataire).

Il s'appuie pour cela sur le protocole EFCP qui offre 2 services :

- échange rapide mais non fiable avec DTP (équivalent à UDP)
- échange moins rapide mais plus fiable avec DTPC (équivalent à TCP)

Les datagrammes sont délivrés en respectant l'ensemble des engagements de QoS (bande passante, gigue, délai de transit, perte de paquets) négociés à travers les services du Plan de gestion.

Les composants qui participent à ces 2 services sont:

- **EFCP** :
  - s'appuie sur le protocole d'échange de bout en bout qui a pour nom Delta-T développé par Richard Watson (chercheur chez IBM). Il gère le contexte des échanges suivants les services demandés DTP ou DTPC

    Ce composant est en charge entre autre :
    . de l'ajout des entêtes DTP ou DTPC
    . du contrôle de flux (limiter le débit aux capacités du réseau)
    . du fragmentation et du réassemblage des messages
    . du contrôle d'erreur (perte, duplication de paquets)
    . du séquencement des messages

- **SDU delimiting** :
  - Dans le sens émission les gros messages (SDU) applicatifs sont fragmentés en petits messages. L'entête protocolaire (PCI) au format DTP ou DTPC est ajoutée à chaque message. Le paquet PDU obtenu (PCI+SDU) est prêt pour être émis

  - Dans le sens réception ce sont les opérations inverses (décapsulation de l'entête PCI de chaque petit message, réassemblage…)

- **Relaying and multiplexing** :
  - Dans le sens émission, les PDU à émettre, vers le même processus applicatif destinataire et avec les mêmes caractéristiques QOS, sont mis dans une même file d'attente d'émission

  - Dans le sens réception, les PDU reçus sont mis dans des files en réception. Chaque PDU reçu est ensuite analysé. Si le PDU est bien pour le bon processus applicatif destinataire, il sera enlevé de la file d'attente et remis à l'application finale sinon il sera de nouveau mis dans une file d'attente pour être réémis

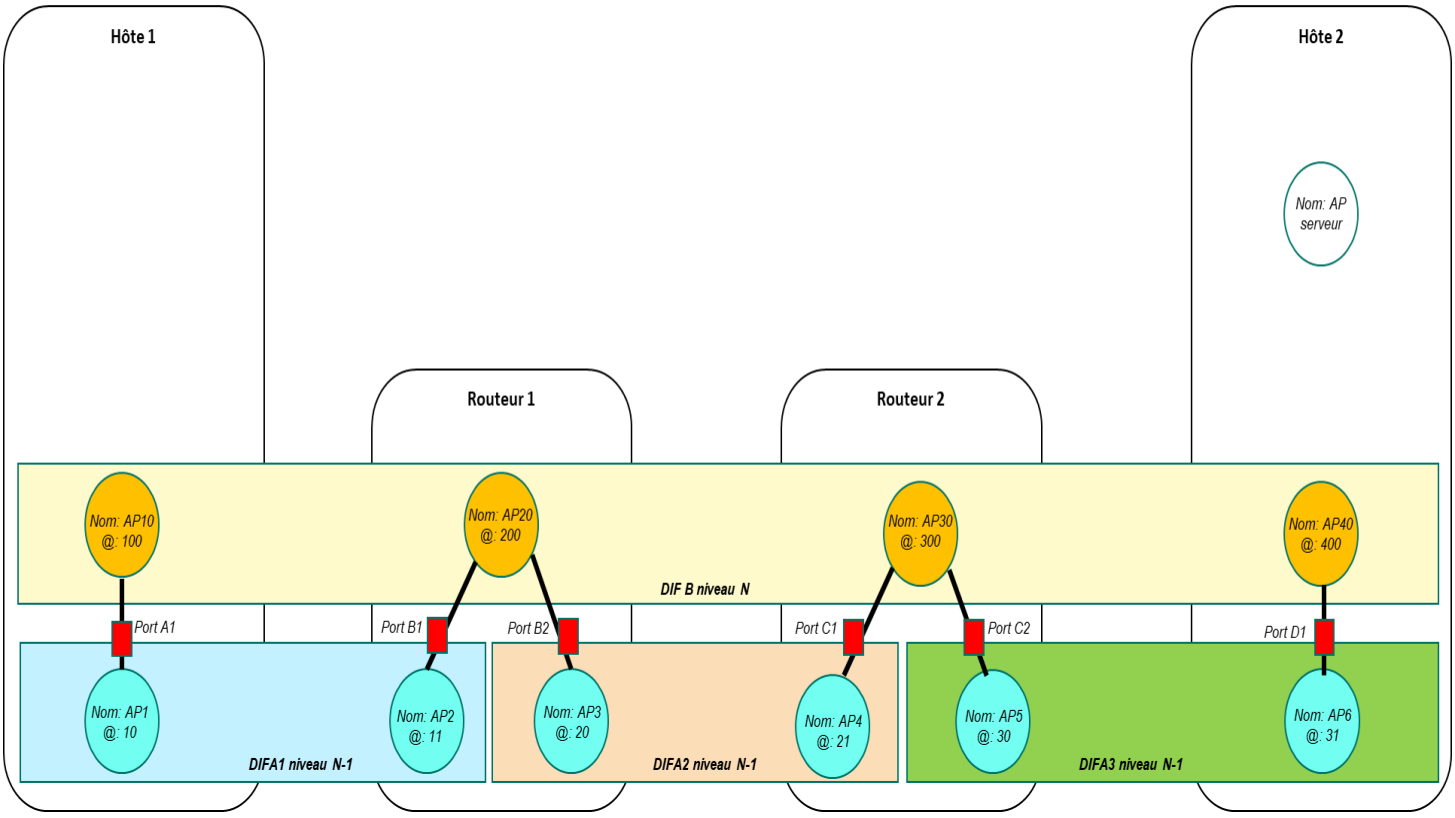
- **SDU Protection** :
  - Calcul du Checksum des datagrammes, assure la Sécurité, authentification, chiffrement des messages

Chapitre 4 : Echanges entre AP au sein d'un DIF

Ce chapitre présente le fonctionnement d'un réseau simplifié basé sur RINA™ avec une vision plus système indépendamment des choix d'implémentation. Pour des questions de clarté, quatre étapes sont identifiées pour ce cas d'usage :

- ⇨ **Etape1** : état initial
- ⇨ **Etape2** : enregistrement d'un AP au sein d'un DIF
- ⇨ **Etape3** : établissement d'une connexion entre 2 AP
- ⇨ **Etape4** : échange de messages entre 2 AP

ETAT INITIAL



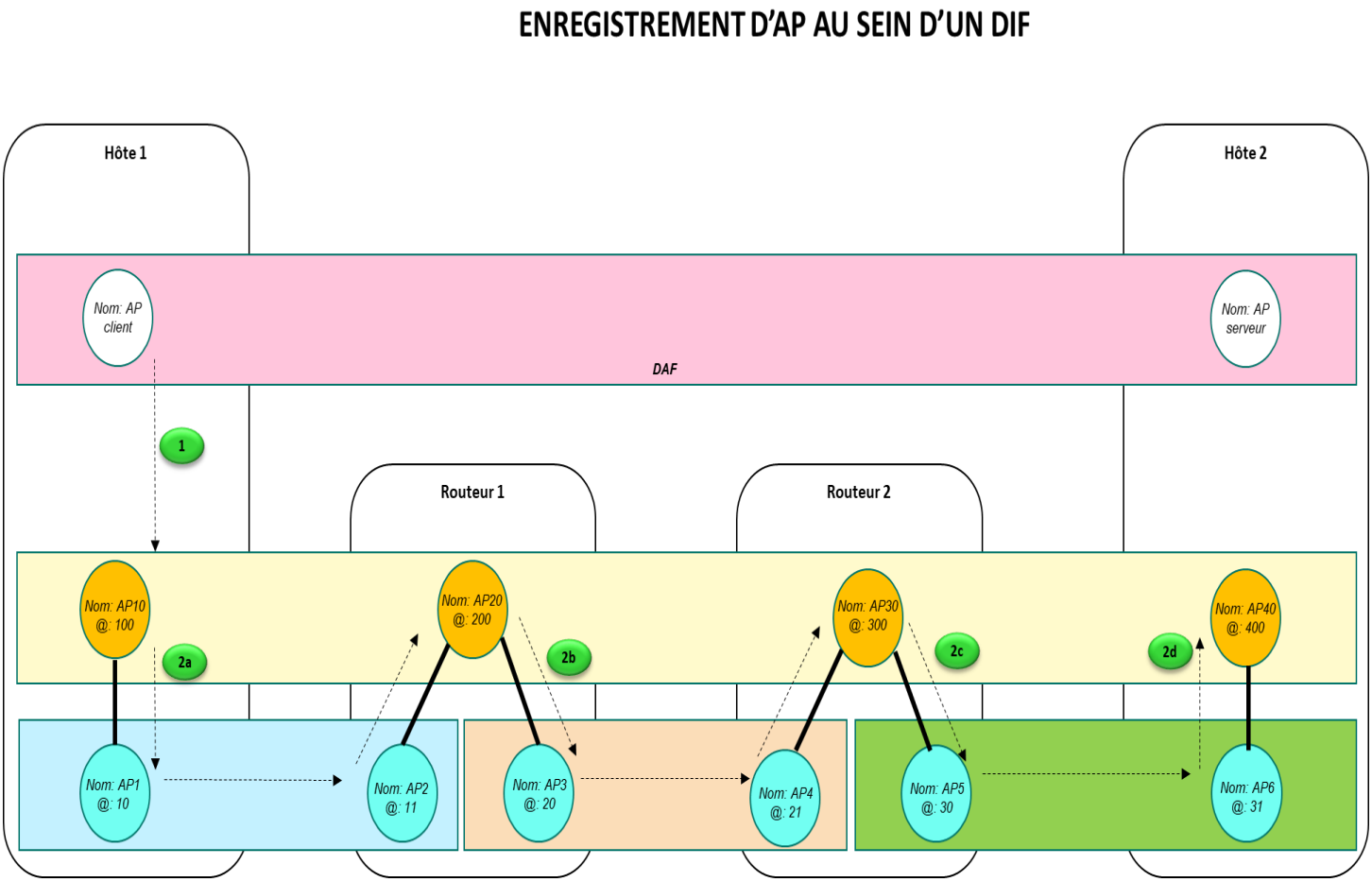
A l'état initial, on a la situation suivante :

- Un **DIF B de niveau N** avec 4 processus applicatifs qui ont respectivement pour nom et adresse (AP10, @100), (AP20, @200), (AP30, @300), (AP40, @400)
- Un **DIF A1 de niveau N-1** avec 2 processus applicatifs qui ont respectivement pour nom et adresse (AP1, @10), (AP2, @11)
- Un **DIF A2 de niveau N-1** avec 2 processus applicatifs qui ont respectivement pour nom et adresse (AP3, @20), (AP4, @21)
- Un **DIF A3 de niveau N-1** avec 2 processus applicatifs qui ont respectivement pour nom et adresse (AP5, @30), (AP6, @31)

Les ports suivants sont créés :

- L'AP10 est relié à l'AP1 via le port A1
- L'AP20 est relié à l'AP2 et l'AP3 via les ports B1 et B2
- L'AP30 est relié à l'AP4 et l'AP5 via les ports C1 et C2
- L'AP40 est relié à l'AP6 via le port D1

L'AP serveur est déjà enregistré auprès de l'AP40 DIF B de niveau N

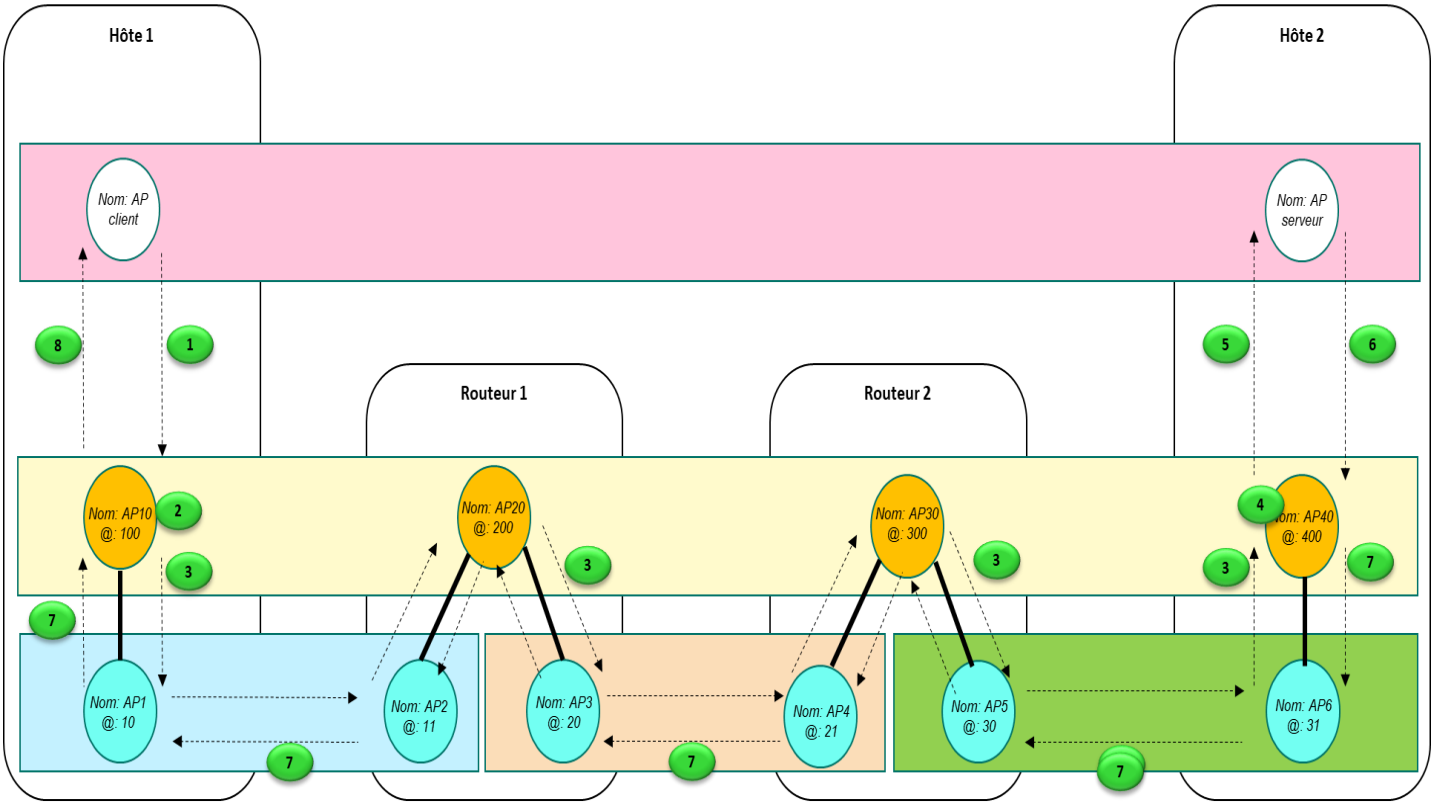


Pour échanger avec l'AP serveur, l'AP client doit d'abord s'enregistrer auprès de l'AP10 du DIF B de niveau N. Pour cela l'AP va faire un appel de fonction **[1]** « Register Application » en passant en paramètres (son nom, le nom du DIF auquel il souhaite s'enregistrer).

Le **Plan de management** d'AP10, après avoir enregistré l'AP client **[2a]**, va alors diffuser le nom de l'AP client aux autres AP de son DIF **[2b]**, **[2c]**, **[2d]** via l'envoi du PDU CDAP M_Write. Les AP20, AP30, AP40 ont ainsi la connaissance de l'enregistrement de la présence de l'AP client.

L'AP client et l'AP serveur forment alors un DAF (Distributed Application Facility).

ETABLISSEMENT D'UNE CONNEXION ENTRE 2 AP



Pour s'échanger avec l'AP serveur, l'AP client doit faire appel de fonction **[1]** « Allocate Flow request» en passant en paramètres (nom AP source, nom AP distant, le type d'échange DTP ou DTPC, le niveau de QOS souhaité, le niveau de sécurité souhaité…).

Le **Plan de management** d'AP10 va allouer les ressources nécessaires pour l'AP client **[2]** :

- Cep_id source: identificateur de connexion
- EFCP instance : identificateur de l'état des échanges (état de l'automate d'échange)
- Port_id source : port d'émission/réception entre l'AP10 et l'AP client (file d'attente)
- QOS_id source : identificateur de Qualité de services
- Security_id source : identificateur de Sécurité

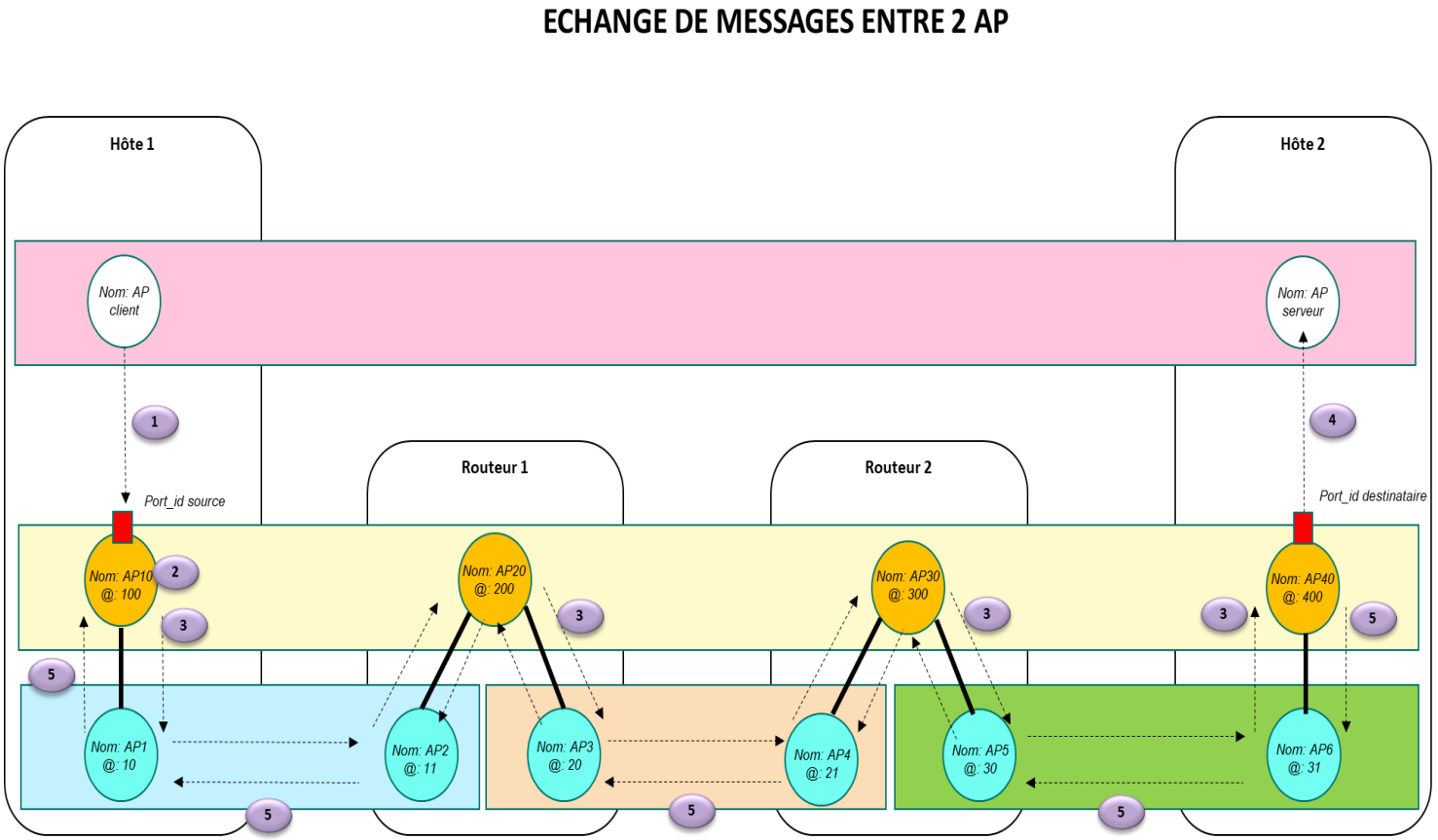
Le **Plan de management** d'AP10 va envoyer ensuite le PDU M_Connect request à l'AP20 pour effectuer les allocations de ressources. Puis le **Plan de management** de l'AP 20 va relayer à l'AP30 et ainsi de suite jusqu'à AP40 **[3]** qui va allouer les ressources nécessaires à son tour **[4]** :

- Cep_id destinataire: identificateur de connexion
- EFCP instance : identificateur de l'état des échanges (état de l'automate d'échange)
- Port_id destinataire : port d'émission/réception entre l'AP40 et l'AP serveur (file d'attente)
- QOS_id destinataire : identificateur de Qualité de services
- Security_id destinataire : identificateur de Sécurité

L'AP40 va avertir **[5]** l'AP serveur de la demande de l'AP client qui accepte la demande par exemple dans notre cas **[6]**.

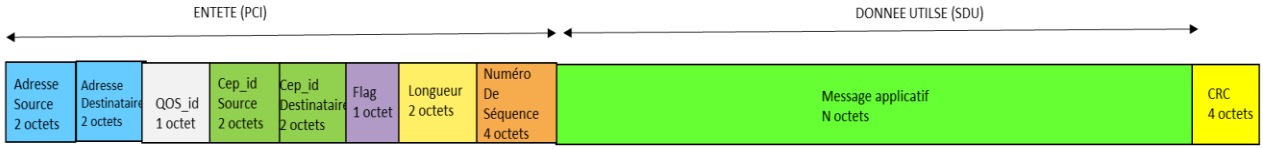
Le **Plan de management** d'AP40 va envoyer le PDU M_Connect response à l'AP30 qui va le relayer à l'AP20 et ainsi de suite jusqu'à AP10 **[7]**.

L'AP10 va avertir à l'AP client de l'ouverture de la connexion entre l'AP source client et l'AP destinataire serveur en lui indiquant le port_id source.



L'AP client peut envoyer maintenant à l'AP serveur des messages. l'AP client doit faire appel de fonction **[1]** « Send » en passant en paramètres (Port_id source, le message SDU).

Le **Plan de Transfert de donnée** de l'AP10 va construire un PDU message pour l'envoyer à l'AP40 en ajoutant l'entête suivant (PCI) **[2]**:



Ce PDU message sera routé successivement par l'AP20 puis par l'AP30 jusqu'à l'AP40 **[3].** Sur réception de ce dernier, l'AP 40 le redonne à l'AP serveur **[4]** et envoie un PDU acquittement à l'AP10 **[5].**

Chapitre 5 : Projets de recherche

L'Europe est à l'initiative du financement de nombreux projets de recherche autour de RINA™ depuis 2008 jusqu'à maintenant. Des laboratoires de recherche et de nombreuses universités et des industriels ont répondu présent. On peut les citer à titre d'informations :

. Le laboratoire de recherche fondamentale TSSG de Dublin, le laboratoire de recherche fondamentale I2CAT de l'université de Barcelone et l'université de Patras en Grèce, l'université de Ghent en Belgique, l'Université d'Oslo en Norvège, l'Université Brno

. Les opérateurs télécoms (Vodafone, Telefonica, Interoute, Geant Network), les équipementiers télécoms (Juniper, Ericsson), les industriels (Nextworks, Iminds, PNSol,Thales, ATOS)

. L'université de Boston et Telecom SudParis sont respectivement la seule université américaine et la seule école d'ingénieur française à participer à l'aventure

Les objectifs sont multiples :

- **Développer** des plateformes logicielles, des outils autour de RINA™ dans des environnements OS Linux et multi langages (Java, C/C++, Python)

    . Souche OPENSOURCE ProToRINA développée par l'université de Boston : https://github.com/ProtoRINA/users/wiki

    . Souche OPENSOURCE rlite développée dans le cadre du projet IRATI :

    https://github.com/rlite/rlite

    - Simulateur RINASim développé par l'université technologique Brno : https://omnetpp.org/download-items/RINASim.html

- **Tester** de nouveaux algorithmes autour du transport des données en utilisant le protocole DeltaT

- **Valider** la QOS, la mobilité, la congestion dans un réseau, le Multicast

- **Expérimenter** en grandeur réelle l'architecture RINA™ à travers des réseaux PAN Européens

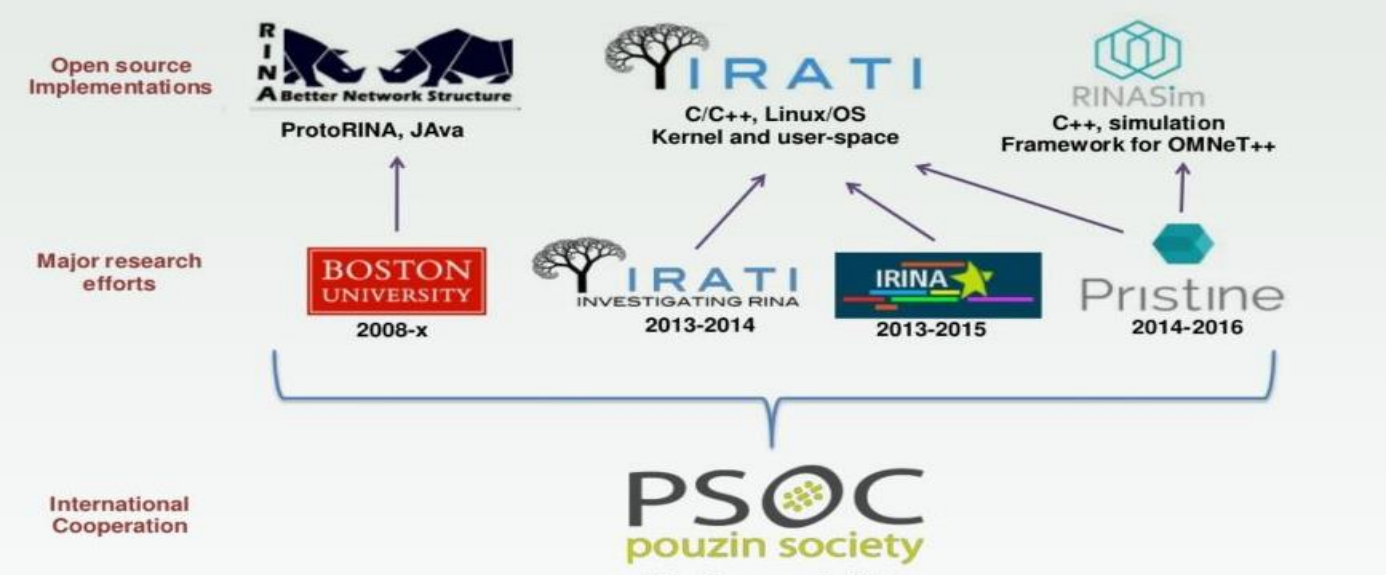
- **Intégrer** les gestionnaires de supervision/administration

- **Calculer** la performance du système

- **Capitaliser** et diffuser les connaissances sur RINA™

PSOC (Pouzin Society) est créé sous l'initiative de l'Université de BOSTON pour fédérer l'ensemble des projets de recherches autour de RINA™. Le schéma ci-dessous résume les projets durant la période 2013-2021 :

- https://pouzinsociety.org/



(Source : Pouzin society)

Les premiers résultats sont très prometteurs. Pour plus de détails sur les différents thèmes de recherche, vous pouvez consulter les sites des projets indiqués ci-dessous :

. **IRATI** : https://irati.eu/research/
[Partenaires: I2cat, Boston University, Nextworks, Iminds, Interoute]

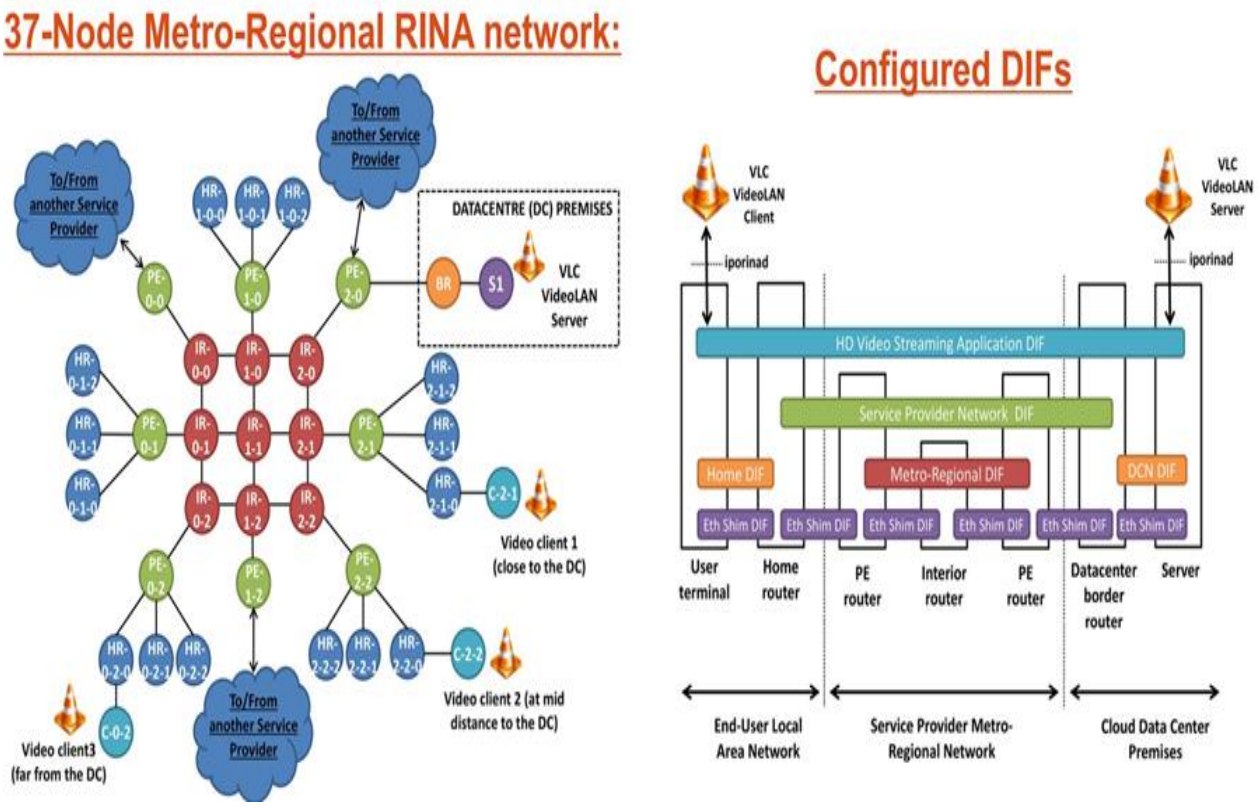
. **ARCFIRE** : https://ict-arcfire.eu/
[Partenaires: Ericsson, I2cat, Nextworks, Telefonica, Iminds, Boston University]

. **PRISTINE** : http://ict-pristine.eu/
[Partenaires: TSSG, I2cat, Telefonica, Ericsson, Nextworks, Thales, Nexidi, BISDN, ATOS, Juniper, University Oslo, University Brno, Telecom SudParis, Create Net, Iminds, PNSol]

. **OCARINA** : https://www.mn.uio.no/ifi/english/research/projects/ocaRINA/
[Partenaires: Boston University, Lancaster University, I2cat, TSSG]

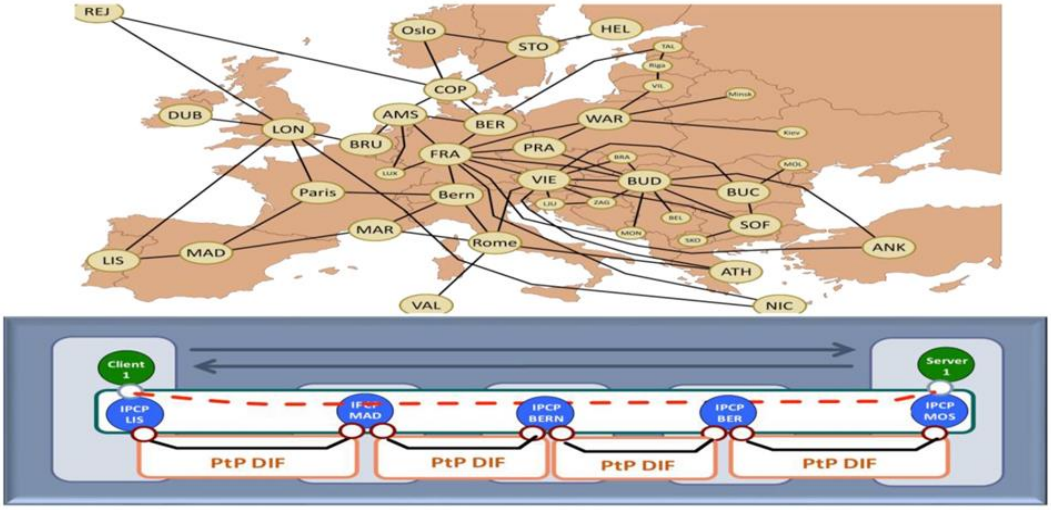
. **PRoToRINA** : http://csr.bu.edu/RINA/index.html
[Partenaires: Boston University]

Le premier schéma ci-dessous détaille l'architecture RINA™ mise en œuvre dans le cadre d'un POC sur la QOS :



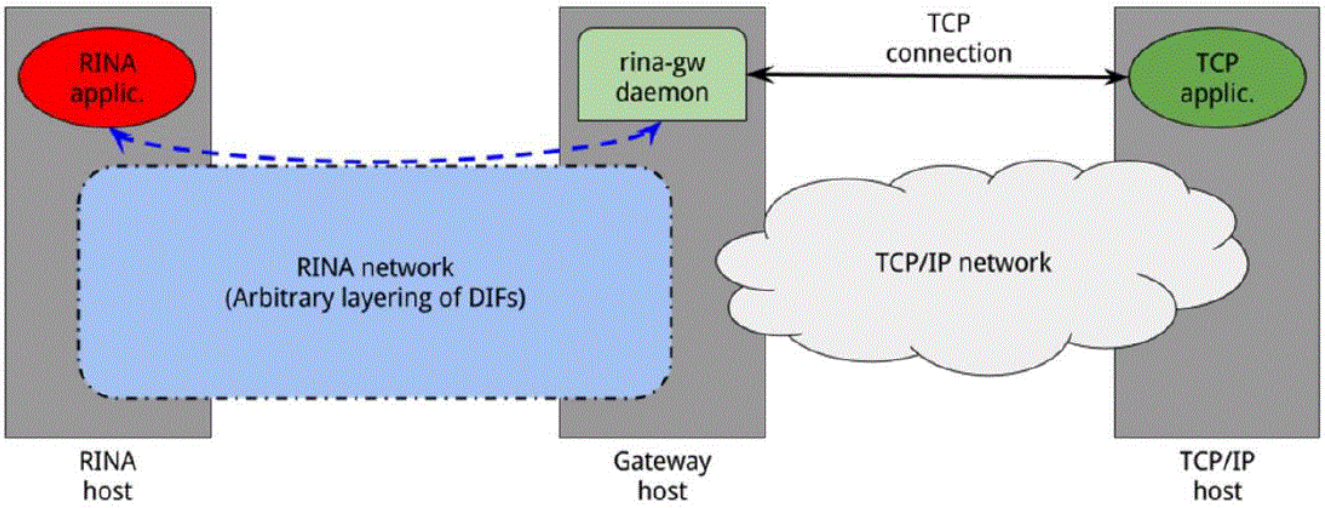
(Source : ERASER)

Le deuxième schéma ci-dessous détaille l'architecture RINA™ mise en œuvre dans le cadre d'un POC avec le réseau GEANT. Ce réseau Pan Européen à très haut débit relie les centres de recherches européens et les universités. L'équivalent en France, c'est le réseau RENATER2 :



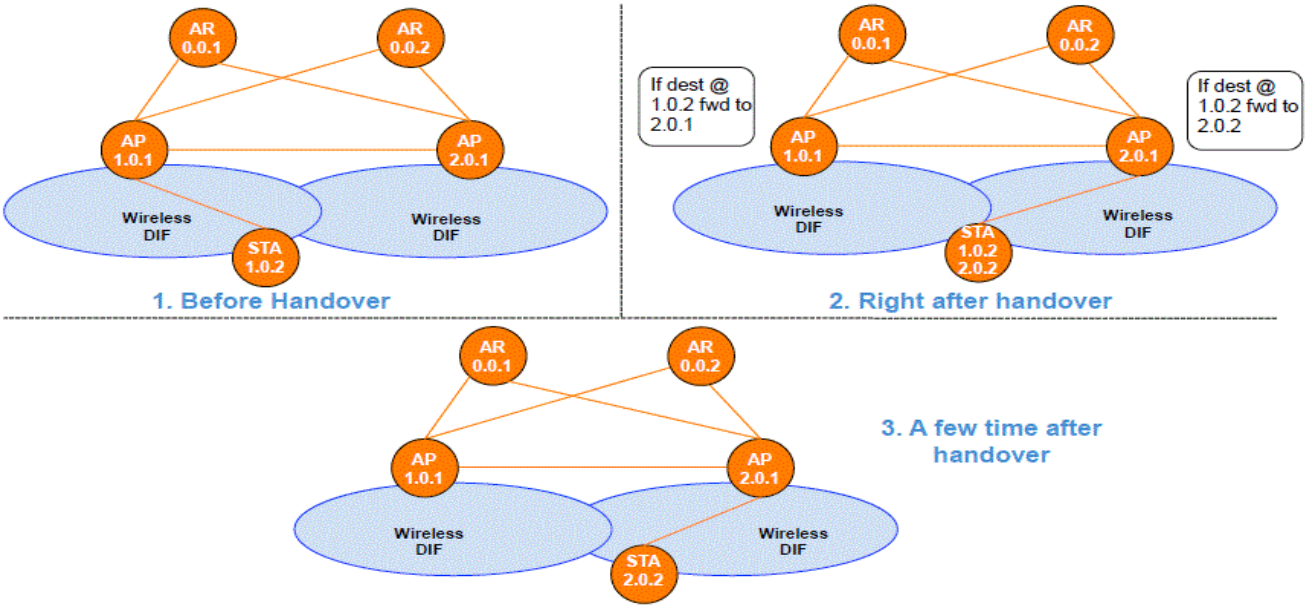
(Source : ARCFIRE)

Le troisième schéma ci-dessous détaille l'architecture d'une passerelle de communication (Gateway) qui interconnecte les 2 systèmes (RINA™ et TCP/IP) :



(Source : ARCFIRE)

Le quatrième schéma ci-dessous détaille les tests sur la mobilité dans RINA™ (changement de cellule-handover):



(Source : ARCFIRE)

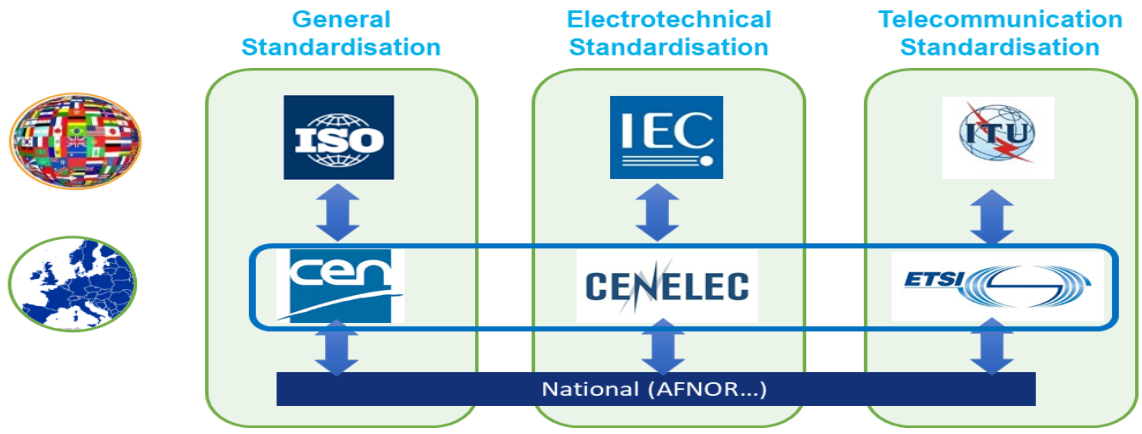
Lors du septième International Workshop sur RINA™ **ICIN 2020** (Innovation in Clouds, Internet and Networks) à Paris, des futurs axes de recherche sont identifiés:

- Multicast
- Security: authentication, access control, confidentiality
- Implications of RINA for AI-based network management
- RINA scalability
- Policies for large-scale RINA DIFs
- Deployment scenarios for RINA
- Deployment of 5G network slices enabling RINA networks
- Analysis of case studies showing benefits of RINA
- RINA for satellite constellations networking (LEO, MEO, GEO)
- Specific RINA policies and DIF designs for wireless networks
- Specific RINA policies and DIF designs for RINA in datacentre networks
- Specific RINA policies and DIF designs for RINA in IoT networks
- Specific RINA policies and DIF designs for RINA in service provider networks
- RINA applied to vehicular networking
- Specific RINA policies and DIF designs for RINA as a next generation virtual network overlay
- Supporting the requirements of large-scale decentralized applications (e.g. blockchains)

ETSI (European Telecommunications Standards Institute) s'intéresse à RINA™ dans le cadre de son **projet NGP** (Next Generation Protocoles). Vous pouvez télécharger le document de l'ETSI via le lien suivant :

https://www.etsi.org/deliver/etsi_gr/NGP/001_099/009/01.01.01_60/gr_NGP009v010101p.pdf

La figure ci-dessous fait un rappel des Organismes de Normalisations clefs :



ISO / *International Organisation for Standardization*
IEC / *International Electrotechnical Commission*
ITU / *International Telecommunication Union*

CEN / *European Committee for Standardization*
CENELEC / *European Committee for Electrotechnical Standardization*
ETSI / *European Telecommunications Standards Institute*

(Source : EDF)

Ce système de gouvernance est à 3 niveaux :

- internationale sous la gouvernance de l'ISO, de l'IEC et de l'ITU
- européenne sous la gouvernance du CEN, CENELEC et de l'ETSI
- nationale sous la gouvernance d'AFNOR

Chapitre 6 : Projets industriels

Après une phase de 10 ans en R&D, des applications autour de RINA™ commencent à voir le jour. Le champ d'application est très vaste grâce à son architecture récursive et grâce ces qualités intrinsèques en terme de **performance**, d'**évolutivité**, de **sécurité**, de **mobilité**, de **qualité de service** et de **faible coût de développement** (Framework générique réutilisable).

RINA™ c'est du logiciel pur. Et comme tout logiciel, RINA™ peut être implémenté sur n'importe quelles plateformes matérielles (Intel, AMD, ARM) et dans un environnement multi OS (linux, Windows, Android, IOS, systèmes embarqués).

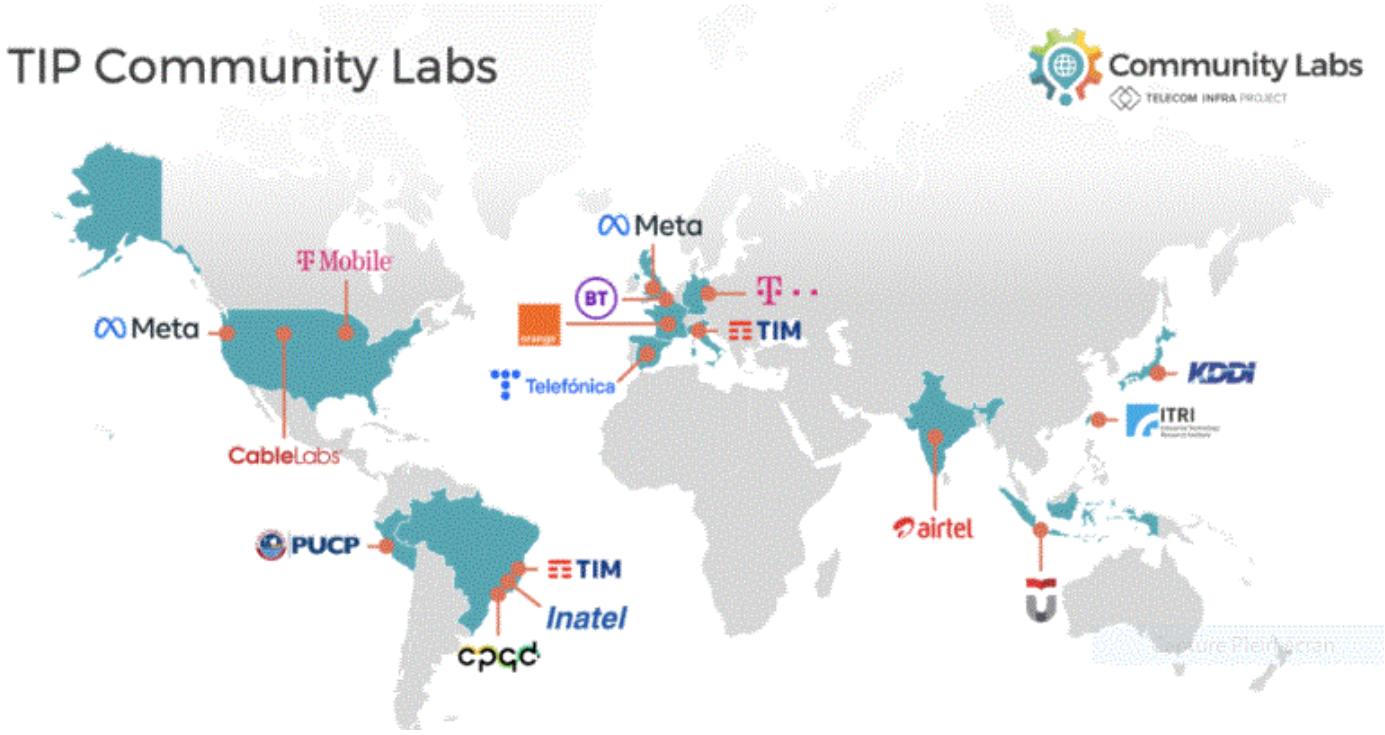
Des nombreux projets industriels basés RINA™ sont ainsi lancés :

- chez l'opérateur anglais (**British Telecom**) et de l'équipementier télécom américain (**Ciena**) :
  Le développement de nouveaux usages tels que le streaming musical et vidéo 4K, la télémédecine, les réseaux sociaux, les jeux en réseau, la réalité virtuelle et la croissance exponentielle de l'E-commerce dû à la pandémie, fait exploser la consommation en bande passante. L'arrivée de la 5G ne fait qu'accentuer le problème.

  Aujourd'hui, la croissance des opérateurs n'est plus assurée par le développement du parc d'abonnés mais par la multiplication des nouveaux services à valeur ajoutée et la fidélisation des clients. Les SVA sont pour les opérateurs télécoms le moyen d'afficher une image novatrice et dynamique dans un contexte où la concurrence fait rage. Ils permettront de satisfaire aussi bien une cible jeune (jeux en ligne) via des services branchés, une cible de technophile grâce à des services avancés ou encore professionnelle grâce à de multiples fonctions élaborées facilitant la communication et l'organisation.

  La gestion dynamique, en temps réel et intelligente de la QOS de bout en bout est devenue un enjeu capital pour ces opérateurs et leurs fournisseurs. Des composants logiciels RINA™ seront mis en œuvre sur toute la chaine des télécoms (depuis les accès fixes/mobiles en passant par les équipements « cœur de réseau » jusqu'aux serveurs **cloud**).

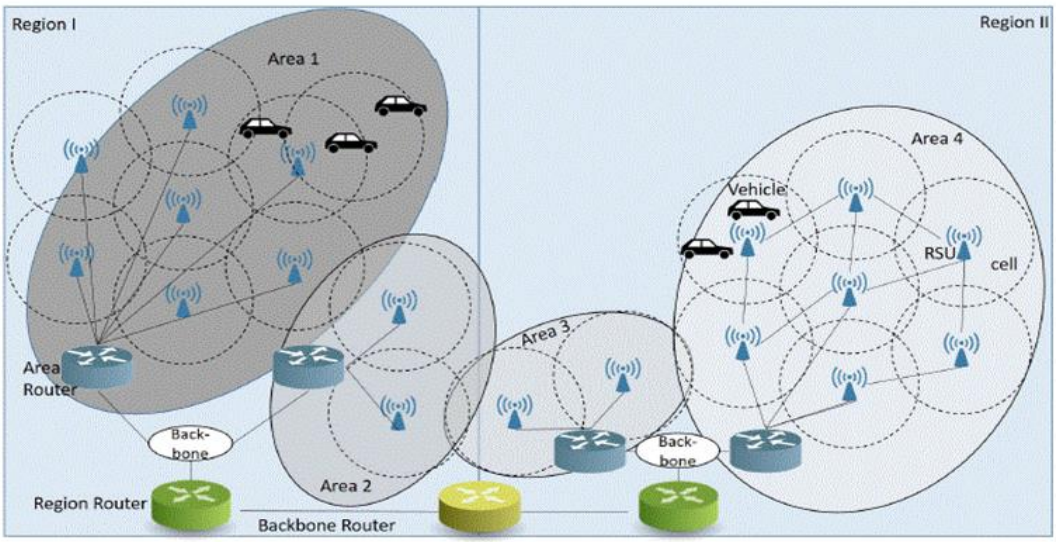
  C'est l'objectif du programme « Adaptative Network » chez Ciena et chez BT c'est du vaste projet « Telecom Infra project » :
  - https://www.ciena.com/insights/articles/Can-Orchestrating-an-End-to-End-E2E-Network-Slice-Be-as-Easy-as-1-2-3.html
  - https://telecominfraproject.com/e2ens/



(Source : projet BT)

TIP représente plus d'une centaine de sociétés à travers le monde (opérateurs télécoms, constructeurs télécoms, intégrateurs…).

- L'automobile moderne sera 100% électrique pour respecter la politique de réduction des émissions des GES (**G**az à **E**ffet de **S**erre) et elle sera surtout ultra communicante. Les investissements dans ce domaine sont considérables. Le projet **VANET** donc l'objectif est la gestion des voitures intelligentes adopte pour cela RINA™ :
    - https://www.cs.bu.edu/fac/matta/Papers/VTC-2018-submission.pdf



(Source : projet VANET)

- La société **Japonaise GLBB-Japan** qui développe et sécurise la Blockchain Cardano, a choisi RINA™ pour faire évoluer son architecture Blockchain :
    - https://cryptoast.fr/fiche-cardano/

- L'ARMENIE est le premier pays au monde à vouloir mettre en place un réseau national basé sur RINA™. Une initiative privée, supportée par le ministère IT, a approfondi la compréhension en vue de déployer RINA™. C'est la fondation e-Hayt qui s'est chargée de cela au travers d'une initiative baptisée **RINArmenia**. Les résultats concrets ont permis d'envisager un vrai déploiement et une commercialisation qui sera bientôt publique. L'ARMENIE possède actuellement un centre international de formation sur RINA™ :
    - https://rinarmenia.com/

De plus, tout un écho système industriel se crée rapidement autour de RINA™ :

- La société française « **Open-Root** », fournisseur des services TLD (Top Level Domain), concurrente de l'ICANN, est choisie par RINARMENIA pour mettre en place le premier service d'annuaire RINA™ (DIF Allocator) :
    - https://www.open-root.eu/la-societe/

- La société américaine **Trianetworksystems** basée en Floride et à Montréal, propose des services de développement, d'intégration, de conseil et d'expertises autour de RINA™ :
    - http://trianetworksystems.com/

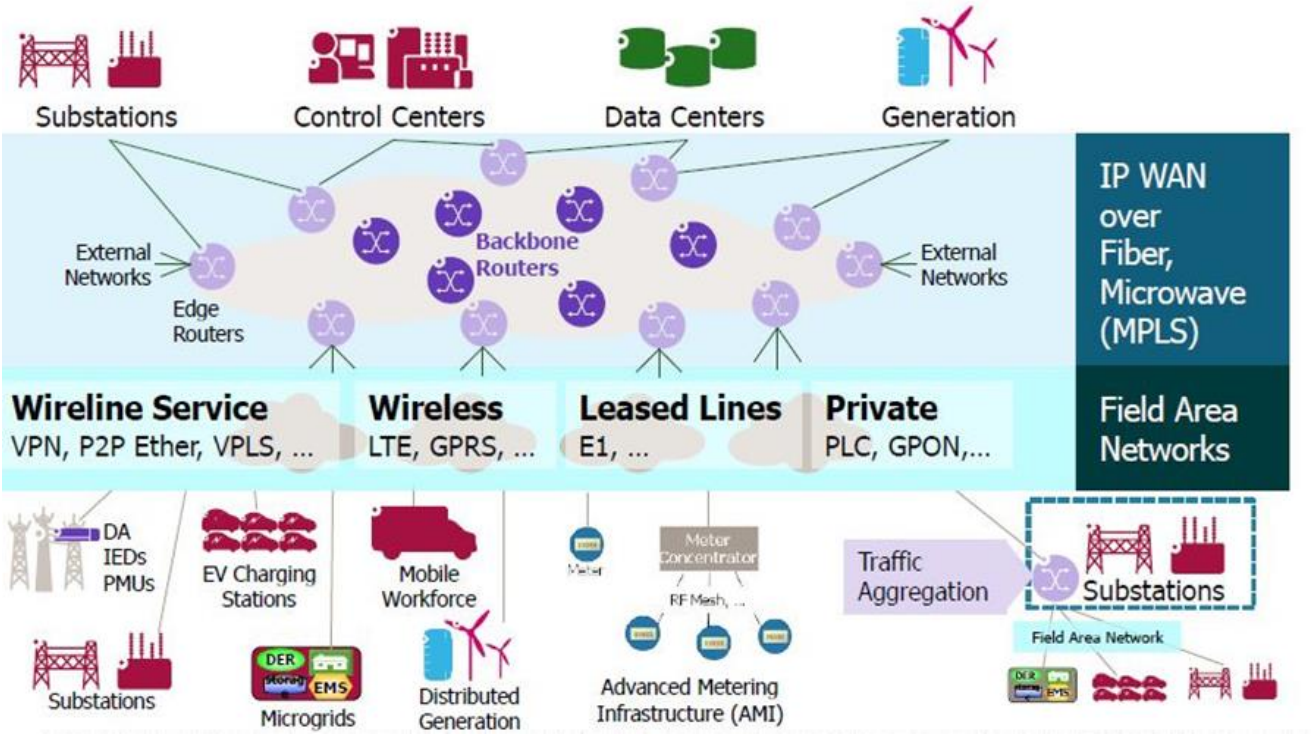
- Un site des utilisateurs de RINA™ est créé au Japon par la société **GLBB-Japan**. Il a pour nom « *Ouroboros over RINA ».* Son objectif est de diffuser les connaissances autour de RINA™ au Japon :
    - http://rinauser.group/

-

D’autres domaines d’application sont possibles :

- le domaine du **Smart grid** où la sécurité du système électrique est un enjeu vital.

  Le Smart grid est la convergence du réseau électrique, des télécommunications et du système d’information. C’est justement les déploiements d’équipements communicants (capteurs de nouvelles générations, IOT) et de nouvelles applications (systèmes experts, Big Data) qui permettent de rendre le système électrique « plus intelligent ». Ces applications offrent une meilleure gestion et un pilotage plus fin des flux d’électricité du client final jusqu’au cœur du réseau électrique.



(Source : Alcatel Lucent)

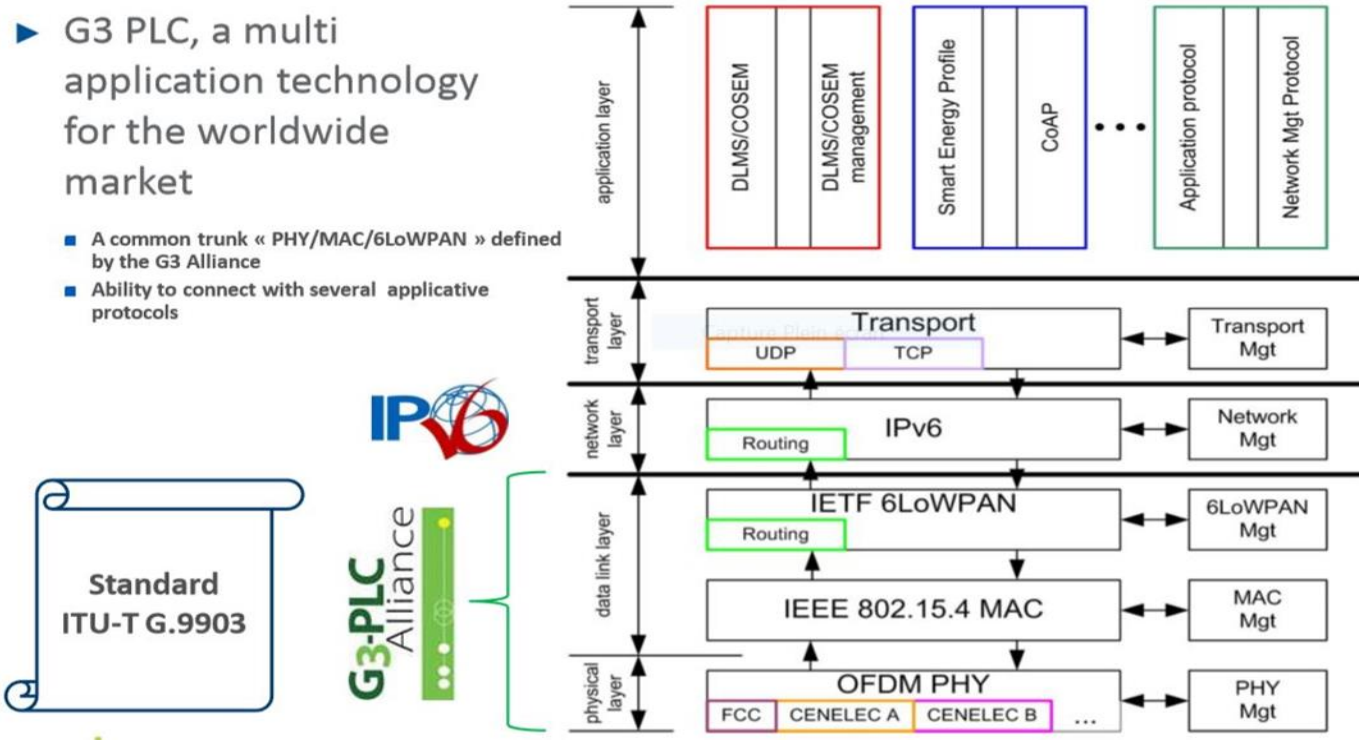
⇨ **les futurs routeurs RINA™ pourront remplacer les routeurs IP actuels pour renforcer la sécurité des Systèmes d’Information d’Importance Vitale (SIIV).**

- le domaine des compteurs intelligents (**smart metering**) :

  Les différents composants qui constituent l’infrastructure de comptage moderne sont les suivants :

  - Les compteurs
  - Les concentrateurs regroupant plusieurs grappes de compteurs
  - Une application centralisée traitant les données de comptage pour la facturation

  Les échanges entre les compteurs et les concentrateurs sont sous forme « numérique ». Le schéma ci-dessous décrit les couches de protocoles mis en œuvre dans le cadre de Linky:



(Source ENEDIS)

⇨ **la future génération des compteurs intelligents pourra intégrer dans l'avenir RINA™. Il existe** différents types de compteurs : pour l'eau, le gaz, l'électricité. Le marché du smart metering est énorme.

- les domaines de SmartCities, du spatial, du militaire…

Est-ce que RINA™ sera une future « Killer application » des prochaines années ? L'avenir nous le dira…

Chapitre 7 : Souveraineté numérique de l'Europe

Le secteur du numérique est d'importance stratégique pour l'Europe qui se dote, d'un fond d'investissement de 7,5 milliards d'euros sur 7 ans (**Digital Europe Program 2021-2027**). La plaquette ci-dessous détaille la répartition de ce fond dans 5 domaines clés :

- **Calcul à haute performance**
  - Obtenir des machines « exascale »,
  - Mettre à jour les superordinateurs existants,
  - Soutenir le développement de l'informatique quantique,
  - Rendre le calcul intensif accessible à travers l'Europe,
  - Élargir l'utilisation du calcul de haute performance.
  - …
- **Intelligence artificielle**
  - Étendre les bases de données européennes,
  - Intensifier la création de lieux de tests et d'expérimentation,
  - Accroître la plateforme européenne d'IA pour accéder aux technologies IA testées.
  - …
- **Cybersécurité**
  - Déployer des réseaux de centres de compétences, en lien avec les États membres,
  - Bouclier de cybersécurité, communication quantique,
  - Systèmes de certification,
  - Outils dédiés à la cybersécurité.
  - …
- **Compétences numériques avancées**
  - Cours de master,
  - Formations de courte durée et stages,
  - Aide à la recherche d'emploi,
  - Plateforme pour l'emploi et les compétences numériques.
  - …
- **Large utilisation des technologies numériques dans l'ensemble de l'économie et de la société**
  - Pôles d'innovation numérique (Digital Innovation Hubs – EDIH),
  - Déploiement à large échelle,
  - Élargissement de l'utilisation intelligente des technologies numériques.
  - …

Il faut espérer que les projets de recherche sur RINA™ auront un budget conséquent.

Le secteur du Numérique est un levier formidable de croissance pour l'Europe -renforcement de la R&D, filière d'excellence pour l'enseignement, renouveau de l'industrie, création d'emplois- à condition d'avoir une vision industrielle de long terme.

(Source : Commission Européenne)

Mais il faut rester lucide. En effet le budget de R&D européen reste faible au regard des investissements privés américains ou asiatiques dans le secteur des nouvelles technologies de l'information en 2020. Les 6 plus gros investisseurs mondiaux[3], sont :

- Alphabet (Google) : 22,5 milliards d'Euros
- Huawei : 17,5 milliards d'Euros
- Microsoft : 16,9 milliards d'Euros
- Samsung : 15,9 milliards d'Euros
- Apple : 15,3 milliards d'Euros
- Facebook : 15 milliards d'Euros

[3] https://www.clubic.com/

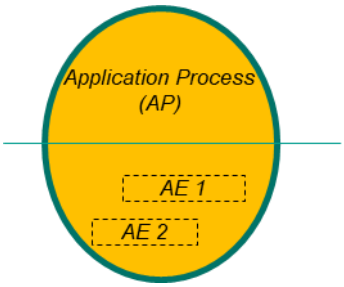
Annexe 1 : Rappel des notions sur l'OSI

Les protocoles OSI n'ont pas su s'imposer face à des protocoles TCP/IP. Tout n'est pas à jeter. Le protocole de routage IS-IS est mis en œuvre par les opérateurs télécoms dans le cœur du réseau IP. Le temps de convergence d'IS-IS est meilleur par rapport à OSFP. De protocoles applicatifs MMS (messagerie) et l'ASN1 (définition et encodage des données) sont encore très utilisés dans les réseaux industriels (Smartgrid norme IEC 61850 et TASE2).

Des protocoles OSI comme ACSE (gestion des associations), CMIP (supervision et administration des réseaux) sont modernisés et utilisés dans RINA™ (protocole CDAP).

Le concept du modèle OSI est toujours d'actualité. Certaines notions élémentaires sont rappelées.

⇒ **Notion AP** : un processus applicatif (AP) est modélisé de la manière suivante (voir schéma ci-dessous) :

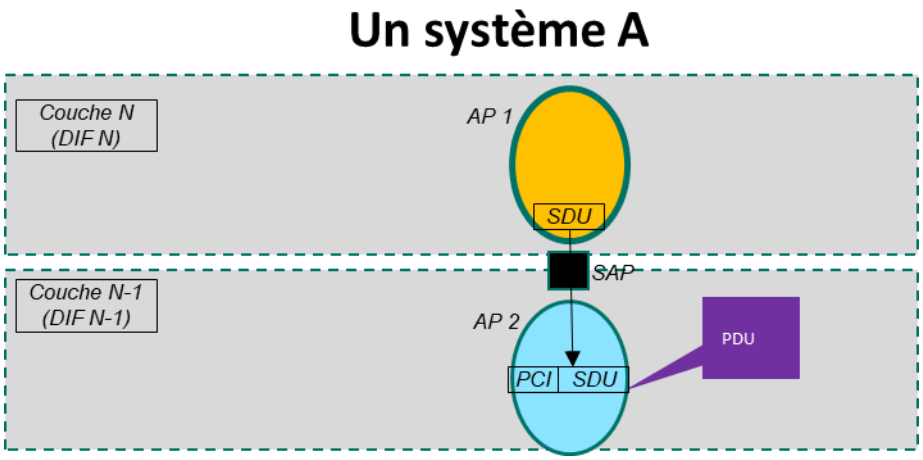


- la partie haute (Application Process ou Processus Applicatif) : gère la logique « métier ».
- la partie basse (Application Entity) : gère les échanges protocolaires avec les couches basses (ouverture/fermeture d'une connexion entre les processus applicatifs).

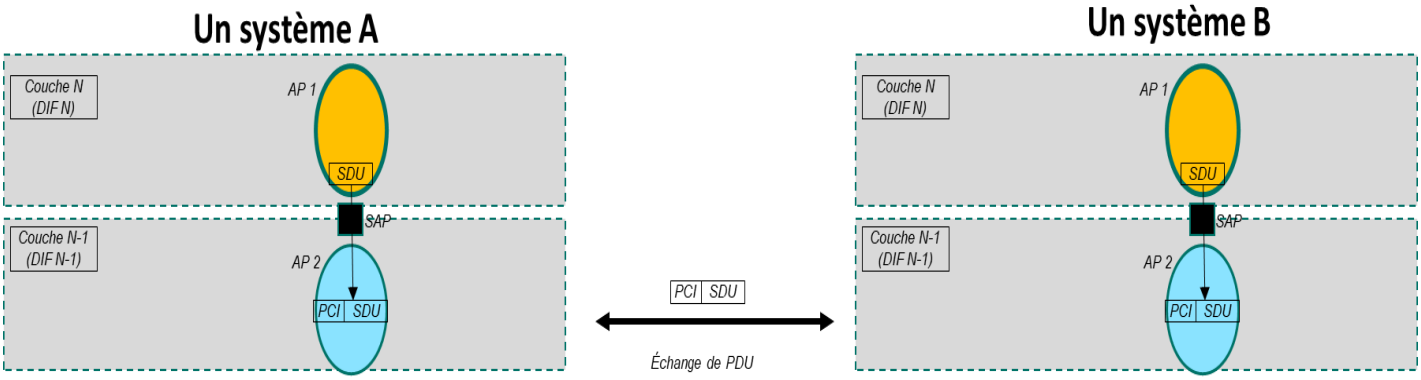
  Un AP peut avoir plusieurs AE (plusieurs connexions simultanément).

⇒ **Notion de services** : La couche N-1 (ou DIF N-1) offre des services à la couche N (DIF N)

- On dira que la couche N et la couche N-1 du même système A s'échangent des SDU (service data unit) à travers un SAP (service access point)
- La couche N-1 ajoute une entête complémentaire PCI (protocol control information) à la SDU
- PCI + SDU devient ainsi un PDU (protocol data unit)



⇒ **Notion de protocoles** : les PDU sont échangés entre la couche N-1 du système A et la couche N-1 du système B.
Un protocole est une règle de dialogue entre 2 couches de même niveau.



Annexe 2 : Cyber sécurité

Les principales réglementations en cybersécurité sont :

En France:

• Loi de Programmation Militaire (LPM 2014-2019): votée en décembre 2013, elle définit dans son chapitre IV de nouvelles dispositions relatives à la protection des infrastructures vitales contre la cyber menace; ces dispositions sont organisées en décrets d'applications et en arrêtés d'applications sectorielles. La LPM 2019-2024 est sortie.

En Europe:

• La Directive NIS (NIS Directive, Directive on Security of Network and Information Systems): adoptée par le parlement européen le 6 juillet 2016, elle représente une composante majeure de la stratégie de cyber sécurité européenne visant à renforcer la cyber résilience en Europe et la coopération entre les différents secteurs. L'application de la directive NIS dans les pays de l'UE est effective depuis mai 2018. Elle a été transposée en France.

• Le Cyber Act: est un règlement européen sur la cyber sécurité (adopté début 2019). Le projet de Cyber Act, présenté au Parlement européen et au Conseil de l'Europe en septembre 2017, propose plusieurs dispositions, dont le renforcement du mandat de l'ENISA. Le Cyber Act reconnait l'importance de prendre en compte les spécificités sectorielles et fait référence à des exigences spécifiques à certains secteurs.

Le RGPD (Règlement général de protection des données) est appliqué depuis le 25 mai 2018 dans l'Union Européenne. Il Impose une nouvelle réglementation sur les données personnelles.

Ses objectifs sont :

- **Une même règle juridique pour les états membres**
- **Une responsabilisation des entreprises sur la collecte, le traitement et les échanges des données personnelles des citoyens européens**
- **Un meilleur contrôle de la vie privée du citoyen. Il aura ainsi le droit de récupérer les données transmises à une plateforme. Il aura le droit d'en exiger la rectification, la suppression totale ou la limitation du traitement dans le temps**
- **Une application de sanctions en cas d'infraction de l'entreprise.**

Annexe 3 : Evénements sur RINA™

- **Forum Atena** a organisé en novembre 2018 « un dîner Networking avec Mr Louis Pouzin sur le thème « Nouveaux Internet » avec RINA™

- Mr Philippe Poux (Président fondateur de RINArmenia, philippe@rinarmenia.com) a lancé le projet RINArmenia en Arménie en 2018

- Mr Christophe Dubois Damien (Trésorier du **Forum ATENA** et président de l'association IESF) a organisé en 2019 un entretien avec Mr Louis Pouzin sur RINA™ au siège d'IESF (Ingénieurs Et Scientifiques de France) :
  https://forumatena.org/comedies-francaises-deric-reinhardt/

- Mr Jean-Jacques Urban-Galindo (membre du **Forum ATENA**) a rédigé en 2019 un article sur RINA™, voici son lien linkedin :
  https://www.linkedin.com/pulse/rina-recursive-inter-network-architecture-pour-les-un-urban-galindo/

- Mr Jean Pierre Hauet (associé au cabinet kbintelligence) a rédigé en 2018 un article sur« RINA™ dans la revue REE (Revue de l'électricité et de l'électronique) :
  http://www.kbintelligence.com/Medias/PDF/20181128_Rina.pdf

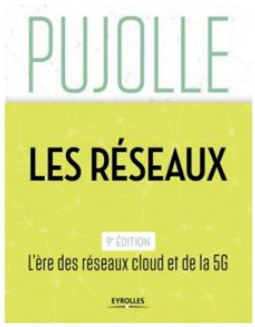
- Mr Gérard Peliks a organisé en octobre 2020 avec le MEDEF Hauts de Seine & l'Université de Paris dans le cadre des « **Lundi de la Cybersécurité** » des échanges en visioconférence avec Mr John Day et Mr Louis Pouzin sur le thème « RINA™, l'Internet non IP qui va remplacer TCP/IP »

Annexe 4 : Livres sur les télécoms

Voici quelques livres pour approfondir ainsi vos connaissances dans les télécoms :

- ⇨ Un livre sur **Mr Louis Pouzin** l'un des pères de l'INTERNET (rédigé par Mme Chantal Lebrument et Mr Fabien Soyez) :

- ⇨ Le livre du **Mr Guy Pujolle** sur les réseaux et télécoms (une référence en France) :



L’auteur

Rolland Tran Van Lieu a obtenu le DESS de téléinformatique (sous la direction du **professeur Guy Pujolle**) en 1990 à l’Université Pierre et Marie Curie (Sorbonne université). Il a intégré la R&D de Cegelec (Alstom power). Il a travaillé sur le développement d’un Scada pour la conduite des centrales électriques (gestion des alarmes, télécommande, protocole de raccordement aux automates industriels). Il a participé à la mise en service du système en Inde.

Au département R&D de TRT (Alcatel Lucent), il était responsable de l’intégration du gestionnaire PHAMOS pour la supervision et l’administration des équipements télécoms optiques SDH/ATM dans un environnement 100% OSI (souche Marben, routage ES/IS, CMIP, ASN1…).

Il a rejoint ensuite SITICOM, Cabinet de conseil en télécom/SI/Sécurité, pour piloter des projets « de schéma directeur, d’appels d’offres, d’audit, d’optimisation des coûts télécoms, d’évolution des organisations et des processus métiers» chez des opérateurs fixes, mobiles et Internet en France, en Europe et Afrique du Nord. Il a été Co-Manager du pôle de compétences Télécom (35 consultants). Il a rédigé de nombreux articles pour 01Réseau, BFM, Réseaux&Télécoms et a participé à de nombreuses tables rondes sur le haut débit, sur les offres d’hébergement, sur la mutualisation des points hauts avec Euroforum.

Chez RTE (EDF) depuis 2009, il a mené de nombreuses études stratégiques sur l’évolution de la téléconduite nationale à l’horizon 2025 : abandon du réseau propriétaire ARTERE, définition d’une nouvelle architecture cible basée sur des protocoles normalisés, élaboration de la stratégie de migration vers cette architecture cible, rédaction des RFI/RFP sur les Scada du commerce, appel d’offre. Il est responsable du domaine Architecture et Cyber sécurité dans le cadre du projet de modernisation des Scada de Téléconduite. Il est en interface avec ANSSI.

Il est Expert auprès de l’AFNOR (**UTE 57**) sur les aspects de normalisation des Smartgrids (IEC OPC UA, IEC 61850, CIM, Cyber sécurité). Et depuis 2016, il est membre du Think Thank « **Forum ATENA** » qui se situe à la convergence du numérique, des entreprises et de l’enseignement supérieur. Il y anime l’atelier Smartgrid.