

**CÖNFLUENS**  
smart-home digital network for services

# SOMMAIRE

- ▶ introduction
- ▶ le réseau confluens
- ▶ le cloud de sécurité confluens
- ▶ le logiciel confluens
- ▶ prédisposition aux services

# introduction

les acteurs de la chaine de confiance

- ▶ industriel
- ▶ distributeur
- ▶ installateur
- ▶ promoteur
- ▶ utilisateur



# introduction

## glossaire



- ▶ réseau physique => réseau IP physique local du bâtiment, habitat collectif ou privé, tertiaire.
- ▶ réseau confluens => réseau privé virtuel Confluens
- ▶ cloud de sécurité=> autorité cloud du réseau global Confluens
- ▶ host => équipement découvert sur le réseau physique
- ▶ device => équipement labellisé **Confluens Ready** avec le logiciel Confluens préinstallé
- ▶ node => device authentifié et identifié participant au réseau Confluens
- ▶ profile => un profil métier permet de décrire les composantes Confluens d'un device
- ▶ service => service opéré par un industriel ou un tiers sur le réseau Confluens
- ▶ domain => espace utilisateur privé dans l'écosystème Confluens

introduction

la promesse

**C**ONFLUENS

Un **réseau d'interopérabilité collaboratif, sécurisé, équitable et serviciable**, prédisposé pour les **services** du bâtiment intelligent.

**Confluens**, le **réseau** numérique de la **ville durable**.

# introduction

## la solution



- ▶ Les équipements hétérogènes **Confluens Ready**, qui participent au **réseau Confluens**, partagent leurs **capacités, ressources** et **informations**.
- ▶ La solution d'**interopérabilité** Confluens est **respectueuse** des fonctionnalités des équipements et de leurs protocoles.
- ▶ Les **industriels** ou **tiers opèrent** les **services** du bâtiment intelligent en **partageant** des **messages** sur le **réseau Confluens** (**scénarios** et **données**).
- ▶ Le réseau **privé virtuel Confluens** est mis en œuvre par notre **logiciel préinstallé** dans tous les équipements **Confluens Ready**. Le **logiciel Confluens** utilise le **réseau IP physique local** pour créer le **réseau privé virtuel Confluens**.



# introduction

## sécurité

- ▶ La sécurité est omniprésente dans toutes les couches logicielles et prend racine dans notre Cloud de sécurité qui représente l'autorité cloud du réseau global.
- ▶ Rappelons que le niveau de sécurité global d'un logiciel est exactement la même que la solidité d'une chaîne en métal. Sa solidité est égale au niveau de solidité du maillon le plus faible.
- ▶ Les éléments de sécurité sont mis en avant tout au long de ce document.

# LE RESEAU CONFLUENS



- ▶ Le **logiciel** Confluens utilise le **réseau IP physique local** pour créer le **réseau privé virtuel Confluens**.
- ▶ Tous les **équipements authentifiés** et **identifiés** participent équitablement au réseau Confluens.
- ▶ Le **réseau** Confluens est **automatique** (plug & play), **sécurisé** et fonctionne quelque soit le ou les équipements présents sur le réseau physique.

# réseau schéma

CONFLUENS

services

life  
confort

energy  
charge & stockage

security  
contrôle d'accès

multimedia  
vidéo

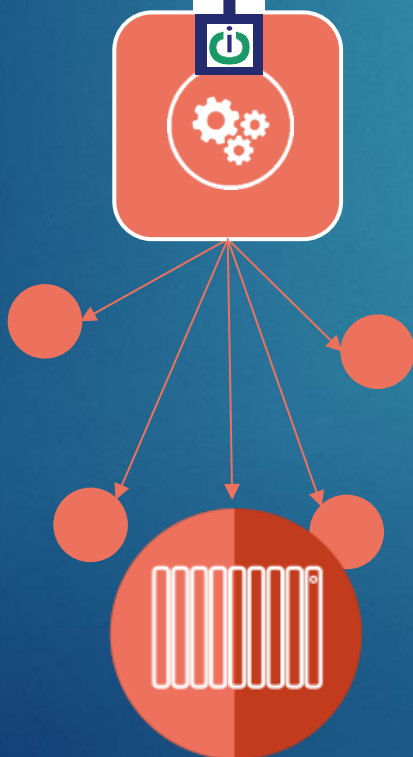
réseau confluents  
réseau physique local IP

exemples  
d'équipements

écosystèmes

protocoles

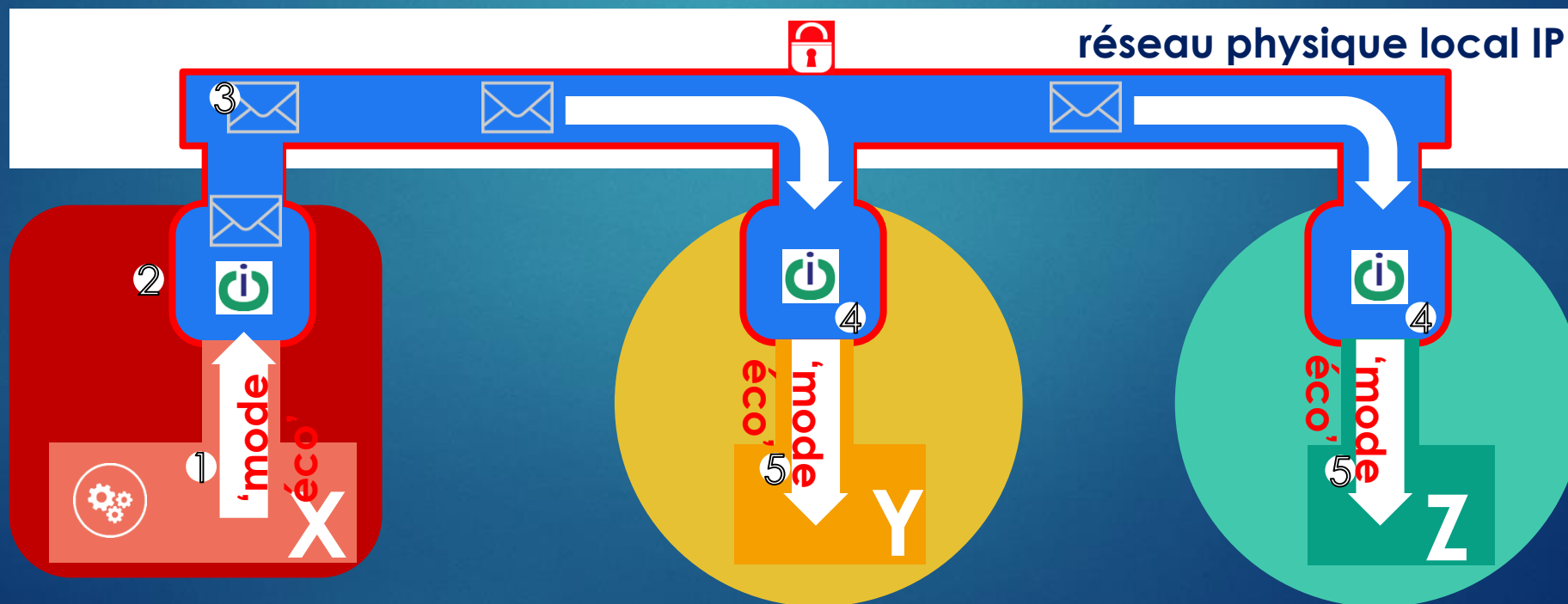
objets



# réseau

transmission d'un message (ex: scénario)

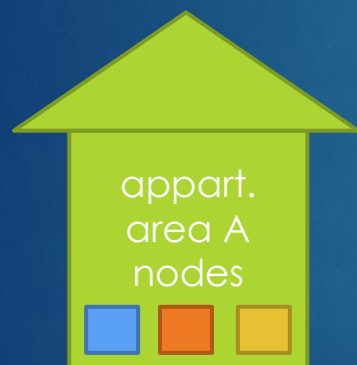
- 1 X active le mode « éco » de son système selon sa logique métier et sa responsabilité
- 2 il partage l'action « éco » avec les systèmes compatibles Confluens
- 3 en publiant '**mode éco**'
- 4 tous les systèmes connectés et compatibles Confluens reçoivent le message '**mode éco**'
- 5 à réception du message, chacun réagit ou pas, selon sa logique métier et sa responsabilité





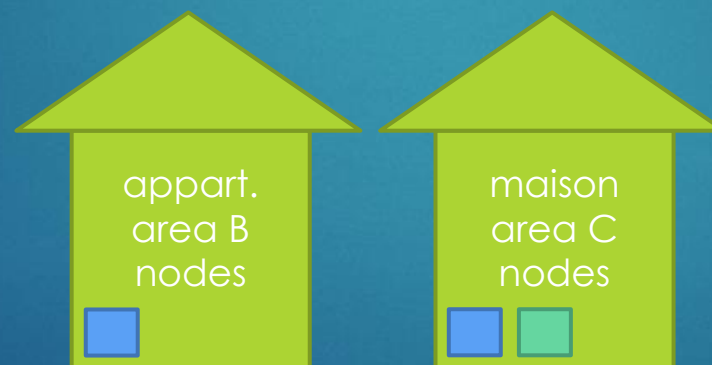
domain 1

Famille Dupont



domain 2

Famille Durand



domain 3

Bailleur

(Appartements des familles Dupont et Durant)

sub-domain 3.1 (résidence XY)



- ▶ Chaque Node possède un Logical-Id unique permettant de l'identifier.
- ▶ Format: CFID-1M-XXXXXXXX-YYYYYYYYY...
  - ▶ 1 => version 1
  - ▶ M => type « mac »
  - ▶ XX => product id
  - ▶ YY => 32 octets permettant l'identification unique du Node

- ▶ Chaque Node possède une Logical-Address unique sur le réseau confluens.
- ▶ Format: CFL3-1NFR-DDDDDDDD-SSSS-AAAA-NNNNNNNN
  - ▶ 1 => version 1
  - ▶ N => type
  - ▶ FR => région France
  - ▶ D => Domain: espace utilisateur privé
  - ▶ S => Sub-Domain: utilisé pour de grandes installations
  - ▶ A => Area: zone géographique de regroupement des nodes
  - ▶ N => Node: Device possédant une stack confluens ready



# réseau

cartographie OSI

messages  
(niveau 7)

rx scene  
0004

rx scene  
0004

tx scene  
0004

réseau confluent  
(niveau 3)

NODE  
(master)

NODE

NODE

découverte  
(niveau 2)

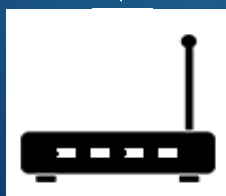
HOST

NODE  
(stack)

NODE  
(stack)

NODE  
(stack)

réseau  
physique  
(niveau 1)



1

2

3

4

5

le Node 5 émet un scénario « je rentre » sur le réseau Confluents

élection du Node master pour la création du réseau Confluents

collecte des données par la découverte des Hosts et authentification des Nodes

réseau physique des Devices de la maison



# réseau

## technologies par niveau

- ▶ Le réseau Confluens est composé d'un ensemble de couches logicielles.
  1. Supervision de l'interface réseau physique (niveau 1)
  2. Découverte des équipements sur le réseau physique (niveau 2)
  3. Election du maître, porteur du réseau Confluens (niveau 2 bis)
  4. Etablissement du réseau Confluens (niveau 3)
  5. Extension vers un réseau Confluens Global (niveau 3)
  6. Sécurité

# réseau

## 1 – supervision de l'interface réseau physique (niveau 1)

- ▶ Toutes les communications utilisent les technologies de l'IP et des Sockets de l'équipement dans lequel le logiciel Confluens s'exécute.
- ▶ Les communications IP gérées par les Sockets sont des fonctionnalités offertes par les systèmes d'exploitation; Linux, Windows et BSD. Afin de canaliser les communications du logiciel Confluens, seule une interface réseau physique est utilisée et supervisée.
- ▶ Ainsi, tous changements sur cette interface réseau physique sont pris en compte. Que ce soit un changement d'état de celle-ci, lors d'un branchement ou débranchement de câble Ethernet ou un changement d'adresse IP.

## 2 - découverte des équipements sur le réseau physique (niveau 2)

- ▶ La découverte est nécessaire à la mise en œuvre d'un réseau automatique. Les protocoles de découverte mdns, upnp et dhcp sont utilisés pour créer une cartographie consolidée des équipements (Hosts) présents sur le réseau physique.
- ▶ Tel un sonar, les équipements s'annoncent régulièrement avec un nom de Host propre.
- ▶ Lorsqu'un équipement cherche à rejoindre le réseau, il fait une annonce pour découvrir quels sont les Hosts déjà présents.
- ▶ Seuls les Hosts authentifiés s'annonçant avec le service Confluens sont pris en compte dans la phase suivante de l'élection.

## 3 - élection du maître, porteur du réseau confluens (niveau 2 bis)

- ▶ L'élection du maître permet de déterminer quel Node sera le porteur du réseau Confluens. Dès que le niveau 1 est opérationnel, l'algorithme d'élection démarre afin de déterminer quel sera le maître du réseau.
- ▶ Si un maître déjà présent est découvert, l'élection est considérée comme un succès.
- ▶ Si aucun maître n'est présent, le Node ayant le score et l'adresse IP la plus grande pose sa candidature en l'annonçant. Si aucun autre Node légitime ne lui dispute la victoire, alors celui-ci sera élu maître et l'élection est considérée comme un succès.
- ▶ Dans tous les autres cas, l'élection est redémarrée afin de déterminer un nouveau maître.

## 4 - établissement du réseau (niveau 3)

- ▶ Le Node maître identifié devient un serveur TCP pour les autres Nodes qui vont se connecter sur celui-ci. (**Dorénavant toutes les communications d'un niveau supérieures ou égales passeront par le réseau confluens**)
- ▶ Immédiatement après l'établissement d'un canal de communication TCP avec le maître, une requête DHCP est envoyée afin de déterminer l'adressage et d'échanger des informations complémentaires.
- ▶ Ensuite le réseau est établi et peut transmettre des messages authentifiés et chiffrés encapsulés dans un paquet IPv6.
- ▶ Lors d'une coupure réseau, le maître « perdu » est temporairement considéré comme défaillant et mis dans une liste grise pendant 2 minutes pour l'élection du nouveau maître.



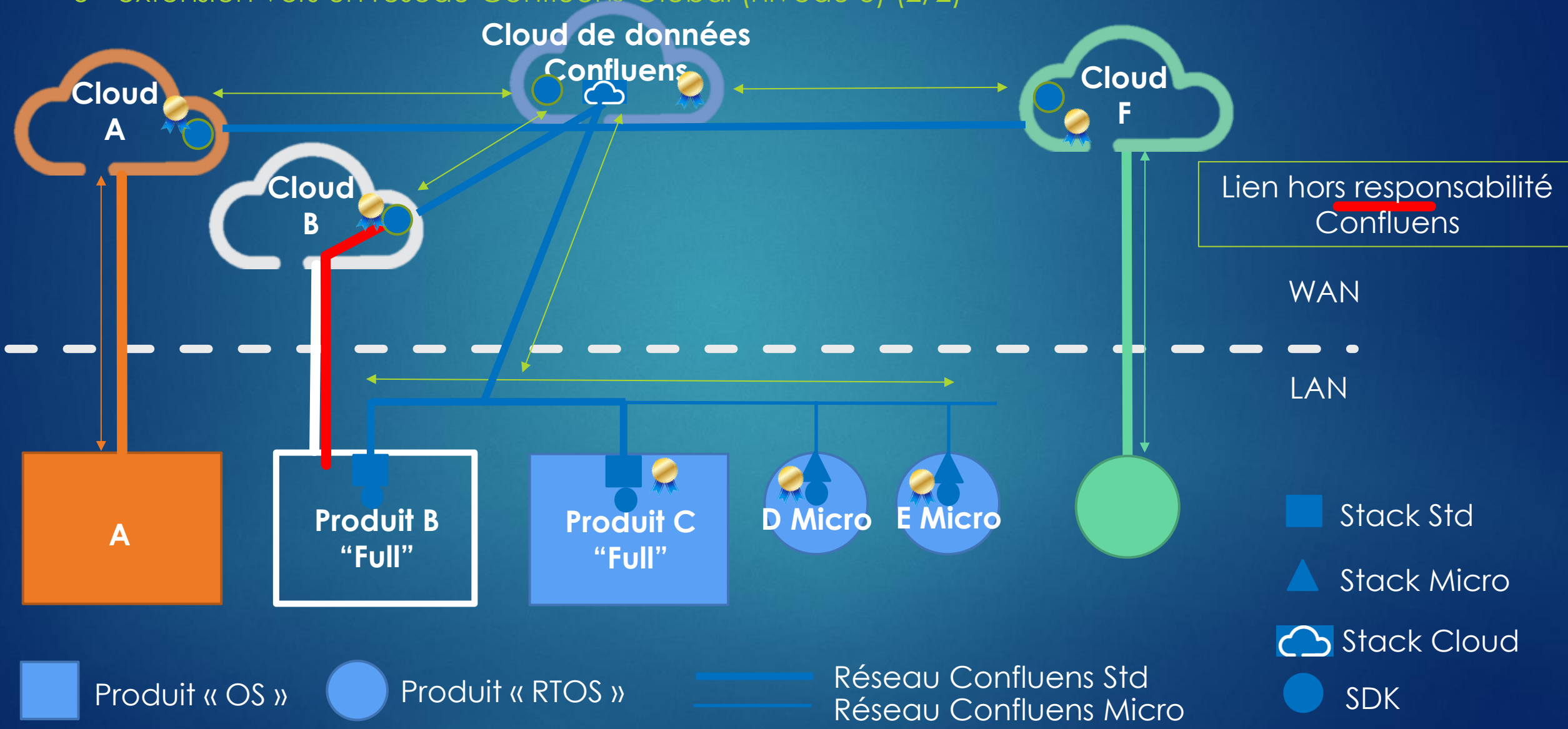
# réseau

## 5 - extension vers un réseau Confluent Global (niveau 3) (1/2)

- ▶ **Les messages peuvent être échangés entre tous les équipements du domaine de l'utilisateur quelque soit sa localisation.**
- ▶ Afin de permettre cette interopérabilité globale, le maître du réseau local se connecte au Cloud de données Confluent et joue le rôle de passerelle.
- ▶ La mise en place d'un réseau global nécessite la création d'une clé unique de réseau par domaine. Une application smartphone donne le contrôle à l'utilisateur du déploiement de cette clé dans les équipements souhaités.

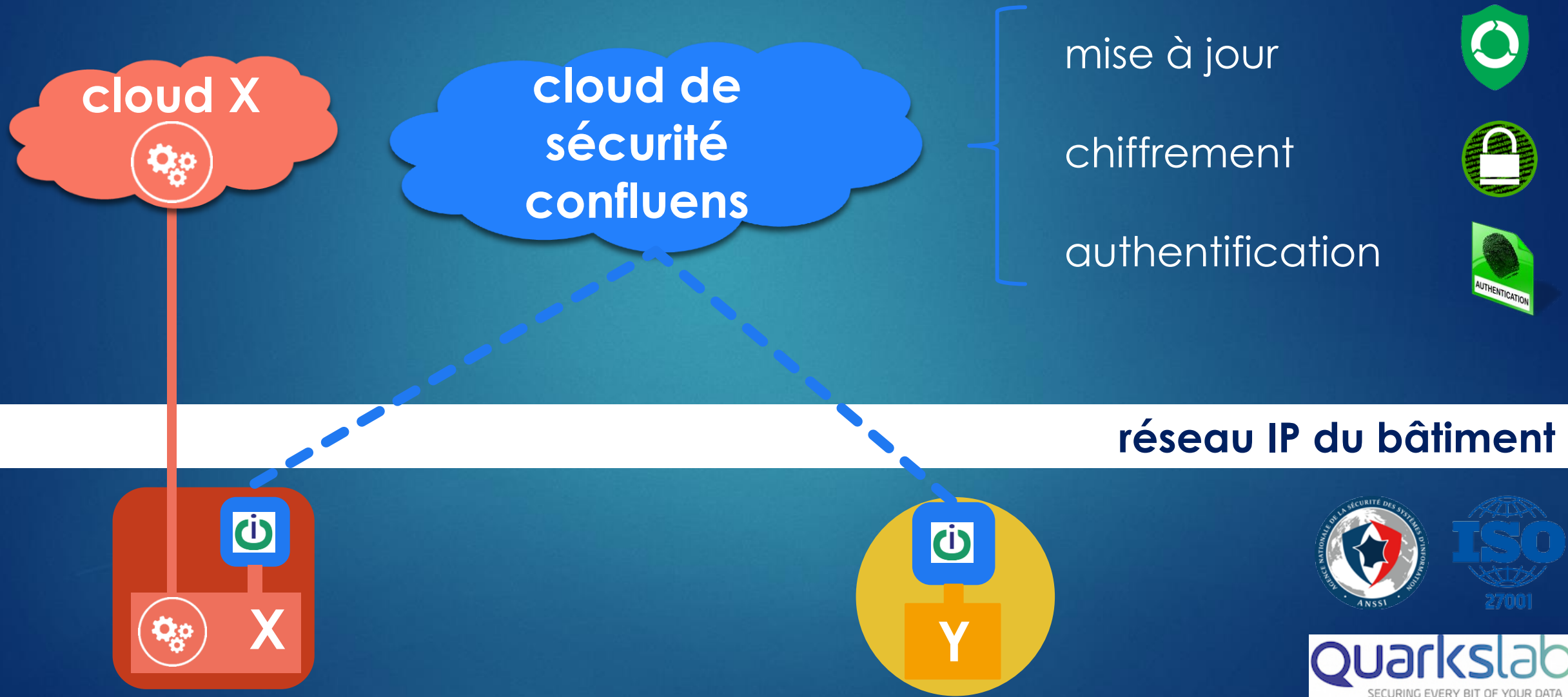
# réseau

5 - extension vers un réseau Confluents Global (niveau 3) (2/2)





# CLOUD DE SECURITE CONFLUENS



# cloud de sécurité

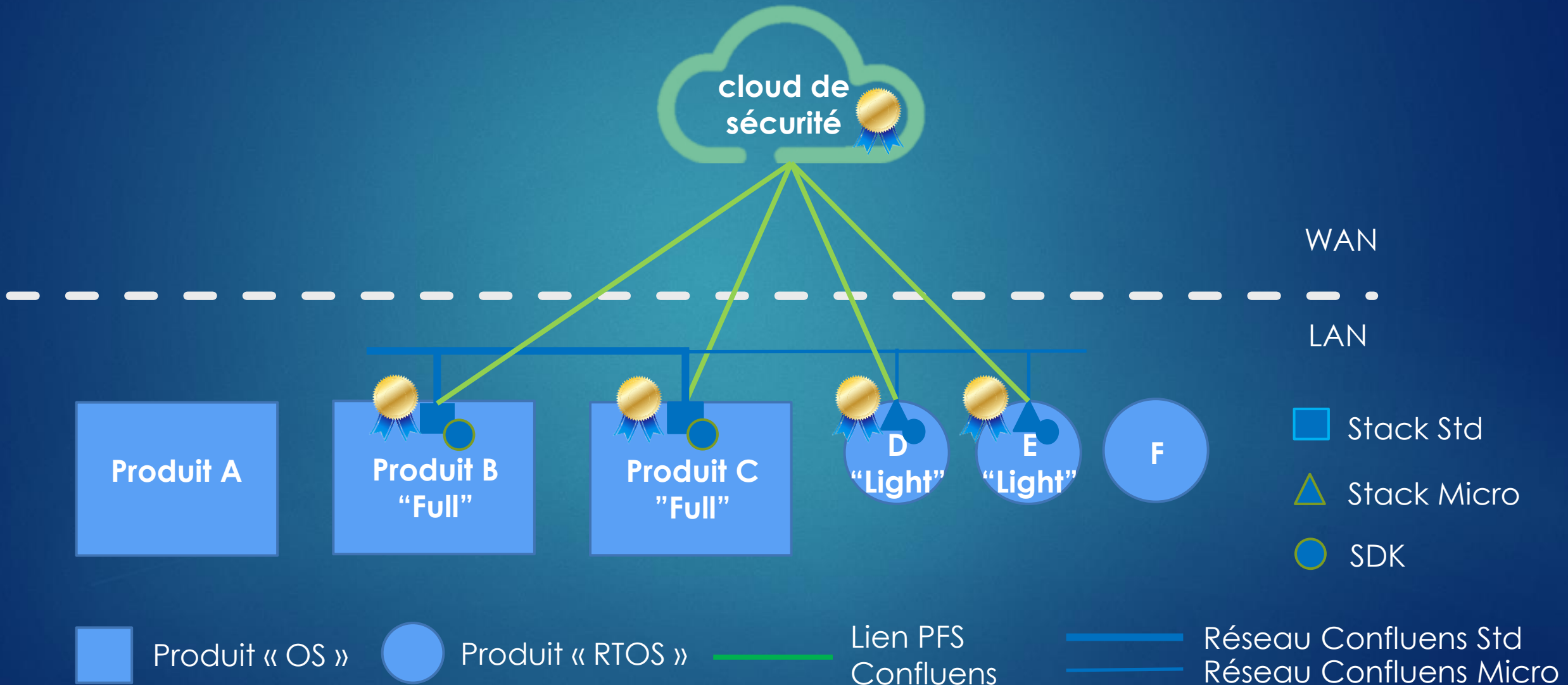
## description



- ▶ Le cloud de sécurité Confluens est l'autorité du réseau global. Il est le garant de la sécurité des réseaux et des logiciels Confluens.
- ▶ Il joue un rôle majeur dans l'Infrastructure à Clés Publiques (PKI). Il est notamment le garant de la distribution des versions logicielles contenant les certificats. Tous les logiciels Confluens contactent régulièrement le Cloud de sécurité pour appliquer la politique de mise à jour souhaitée. Il peut donc déployer des patches de sécurité permettant de garantir un haut niveau de sécurité quelques soient les circonstances.
- ▶ Le Cloud peut autoriser ou révoquer les droits d'accéder aux réseaux Confluens des bâtiments d'un ou de tous les logiciels Confluens préinstallés dans les équipements des industriels.

# cloud de sécurité

schéma



# LES LOGICIELS CONFLUENS

# 1- LE LOGICIEL CONFLUENS Micro



# Le logiciel micro « stack micro »

- ▶ **Il s'agit d'un Proof of Concept.**
- ▶ La stack micro sera un logiciel embarqué, en version alpha, permettant d'étendre l'interopérabilité Confluens avec des produits de type micro-contrôleurs.
- ▶ Ce logiciel implémente la norme COAP (RFC 7252) particulièrement adapté aux produits fortement contraints
- ▶ L'architecture est conçue pour être portable et a ce jour le logiciel support Posix et FreeRTOS
- ▶ L'empreinte mémoire est de 100Ko en stockage et quelques dizaine de Ko en ram



# 2- LE LOGICIEL CONFLUENS CLOUD

# Le logiciel CLOUD

- ▶ **Architecture prédéterminée**
- ▶ **Non développé**

# **3- LE LOGICIEL CONFLUENS STANDARD**

- ▶ Le réseau **privé virtuel Confluens** est mis en œuvre par notre **logiciel préinstallé** dans tous les équipements **Confluens Ready**. Le **logiciel Confluens** utilise **le réseau IP physique local du bâtiment** pour créer **le réseau privé virtuel Confluens**.
- ▶ Le logiciel Confluens **fonctionne** sur un grand nombre d'**équipements hétérogènes**. Le code source est donc portable afin d'être compatible avec les processeurs tels **x86** et **ARM**, ainsi que les systèmes d'exploitation **Linux**, **Windows** et **BSD**.
- ▶ Le logiciel est **performant** afin de transmettre les messages **sécurisés rapidement**.  
**Ex: l'envoi et la réception de bout en bout d'un scénario entre deux équipements prend moins de 200ms.**

# logiciel

## description (1/2)

- ▶ une souche logicielle unique
- ▶ mémoire: 10Mo flash, 2Mo ram
- ▶ portabilité: Linux, Windows, BSD
- ▶ réseau confluens: IPv6, DHCPv6, UDPv6
- ▶ sécurité: IPSec ESP, ECDH, ECDSA, AES-128-GCM, SHA256

CONFLUENS

manufacturer  
application

SDK

scenes

data

messages

security & update

confluens  
network

TCP  
IPv4/IPv6

**IP Network**

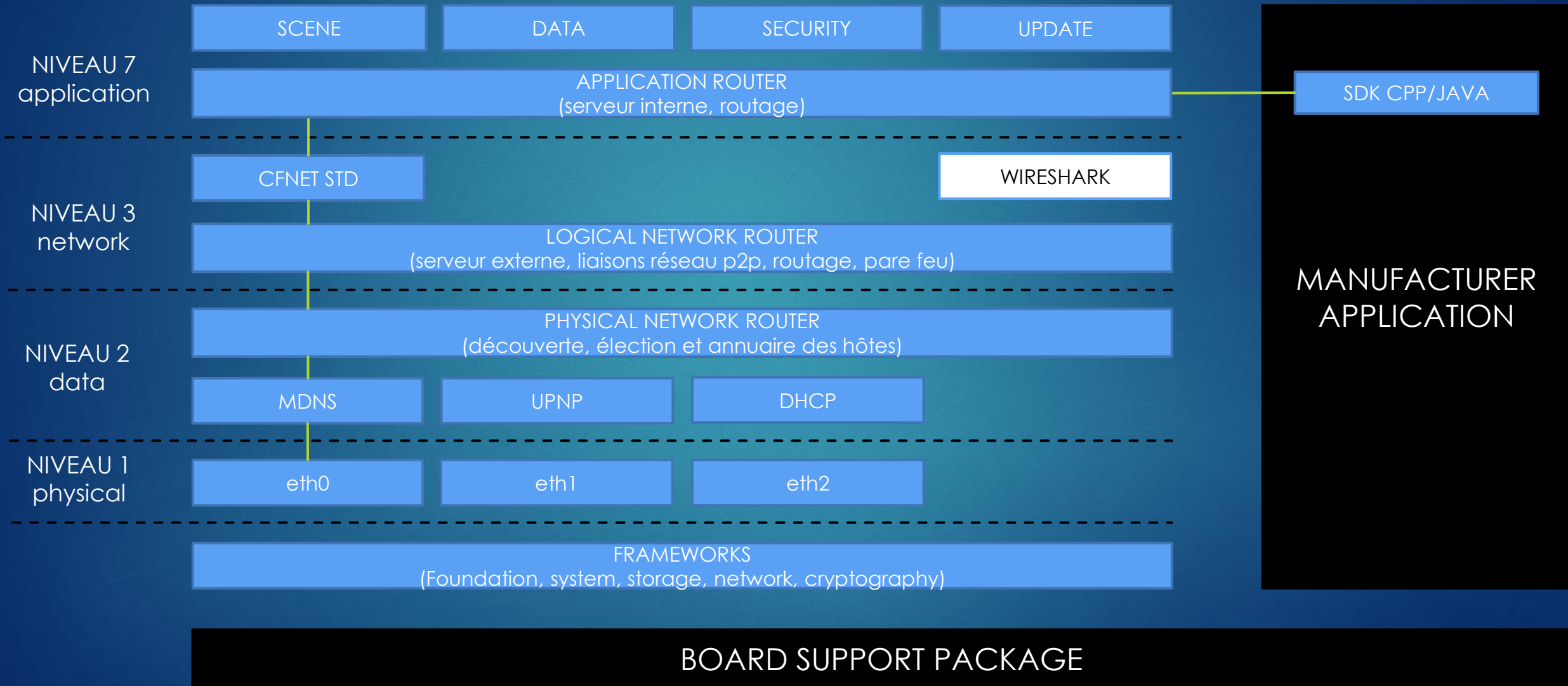
# logiciel

description (2/2)

CONFLUENS

- ▶ Le **logiciel Confluens** est conçu avec une architecture **Service Oriented Architecture** et une mise en œuvre **portable, asynchrone** et **multi-threadée**.
- ▶ Le **logiciel** s'exécute dans **l'environnement** de l'équipement de **l'industriel**, Confluens doit **s'adapter** au **matériel**, au **système d'exploitation** et au système de **sécurité** choisi par les équipes techniques de industriel.
- ▶ L'ensemble des **mécanismes** et de nos **couches logicielles** sont conçus pour offrir une **qualité de service équivalente** quelque soit l'environnement de l'équipement dans lequel le logiciel s'exécute.
- ▶ Le **logiciel** est **rapidement intégrable** dans un équipement (Quelques **jours**)







équipement

LOGICIEL  
CONFLUENS

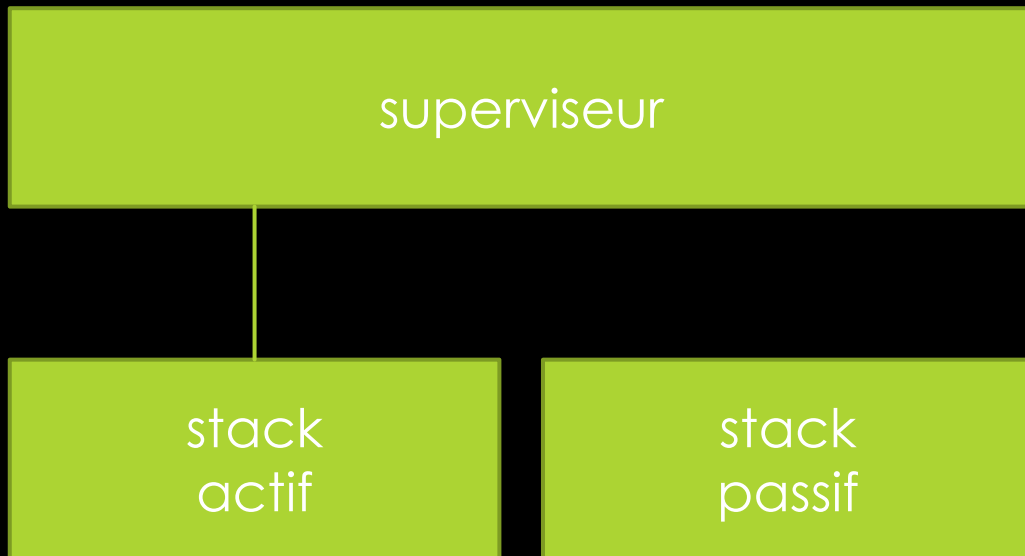
Confluens considère l'équipement de l'industriel comme un environnement de confiance.

Sécurité:

**L'industriel** est **responsable** de la **sécurité** de son équipement.

Nous recommandons l'utilisation des moyens de sécurité suivants:  
**firewall, chaine Secure Boot** et système de **mise à jour**.

logiciel confluens



### Sécurité:

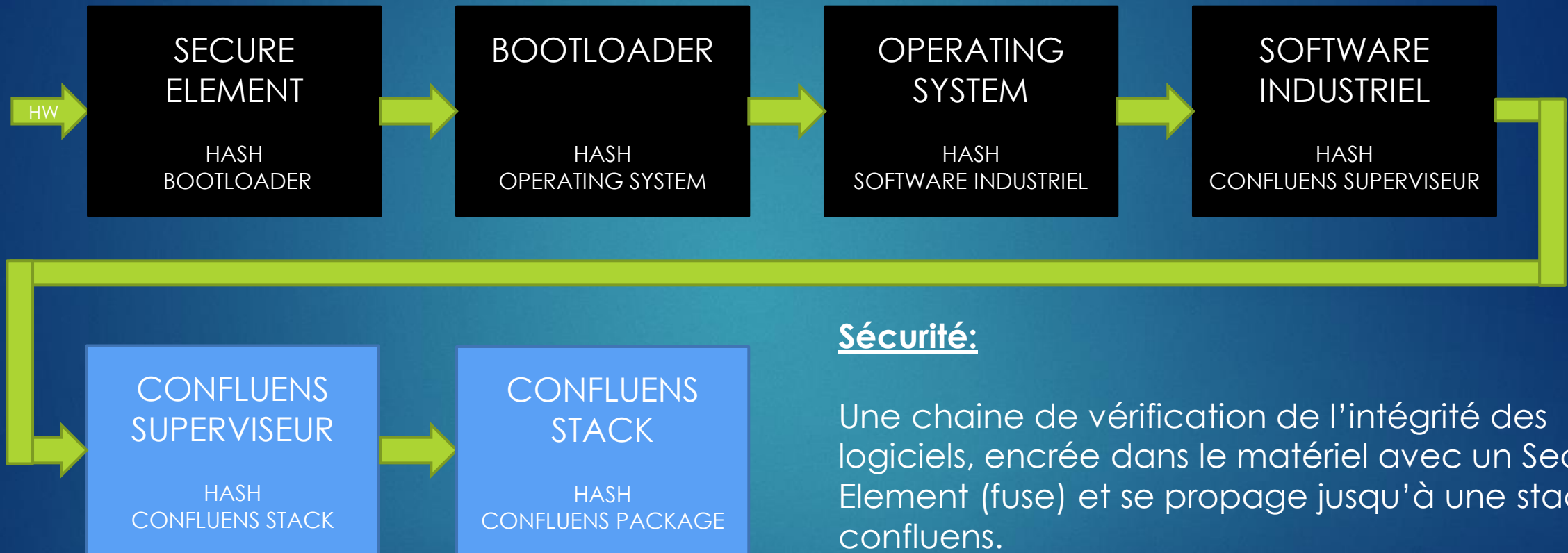
Afin de **prévenir** toute **corruption** ou tentative de **piratage** du logiciel confluens, le **superviseur** contrôle l'**intégrité** du logiciel actif avant de l'exécuter.

Si l'**intégrité** n'est **pas respectée**, le **logiciel actif** est considéré comme **invalide** et le prochain **logiciel passif** est **activé**.

(Rebouclage)

# logiciel

compatible chaine secure-boot



## Sécurité:

Une chaine de vérification de l'intégrité des logiciels, encrée dans le matériel avec un Secure Element (fuse) et se propage jusqu'à une stack confluens.

Le superviseur vérifie la stack puis l'exécute qui elle même vérifie l'ensemble des fichiers composants son package.

# logiciel

mise à jour



Cloud de sécurité  
Confluens

Le logiciel possède un service de **mise à jour** qui permet de **provisionner** jusqu'à **6 versions logicielles**.

A **chaque démarrage** et **plusieurs fois par semaine** l'Application Update du logiciel Actif **contacte** le **Cloud de Sécurité Confluens** pour demander si des **ordres** de mise à jour sont **disponibles**.

Le logiciel Actif **créé, supprime** ou **met à jour** les versions logicielles le nécessitant.

Chaque **version** logicielle forme un **package** dont l'**intégrité** et **authenticité** sont vérifiés.

VERSION  
1

VERSION  
5

VERSION  
2

### Sécurité:

Les **certificats** de sécurité sont **inclus** dans les **versions logicielles**.

La mise en œuvre de l'architecture est principalement basée sur les frameworks Confluens. L'ensemble des **frameworks Confluens** sont les briques élémentaires de la **portabilité**, de la **performance** et de la **sécurité**.

- ▶ Foundation => Types, Exceptions, Console, Atomic, Shared pointer, etc
- ▶ System => Threading, Streaming, Time, Multi-agent system, etc
- ▶ Storage => Buffer, File, Database, Encoding, Hash, etc
- ▶ Network => Addresses MAC/IPv4/IPV6, Sockets TCP/UDP/Multicast, Pipe, etc
- ▶ Cryptography => Certificate, Cipher, Key, Random, Signature, Socket TLS

- ▶ L'architecture multi-agent est mise en œuvre avec un pool de threads qui exécute une liste de Jobs portés par des Agents. Chaque job consiste en une commande à exécuter dans une unit avec une ou plusieurs ressources.  
**(Ex: Une personne fait une liste de courses et se rend chez chaque commerçant en faisant la queue pour acheter tous les éléments nécessaire)**
- ▶ Toutes les fonctionnalités sont implémentées dans des Units indépendantes. Une liste de job permet d'enchaîner un ensemble de commande afin de réaliser une fonctionnalité.



# LES SERVICES

# les services

## introduction

- ▶ Les **industriels** ou **tiers** opèrent les **services** du bâtiment intelligent en **partageant** des **messages** sur le **réseau Confluens** (**scénarios** et **données**).
- ▶ Les **équipements** se caractérisent par **un** ou **plusieurs profils métier**. Les **profils** sont composés de **messages obligatoires** et **optionnels**.
- ▶ Les **services** sont opérés en **échangeant** des **messages** caractérisés par le ou les **profils** de l'équipement.
- ▶ **Tous** les **messages** transitent à travers le **réseau Confluens** et sont donc **sécurisés**.

# les services

prédisposition aux services

life



energy



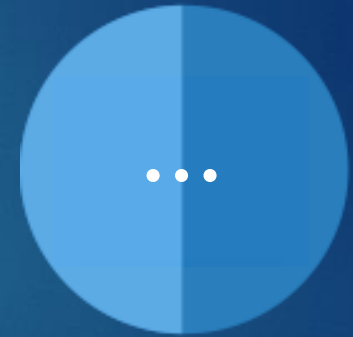
security



multimedia



...



# les services

## les profils métier

Un **profil** métier permet de décrire les **composantes** Confluens d'un **objet** métier.

- Gestionnaire d'énergie => Services Life + Energy
- HVAC => Services Life + Energy
- Ouvrants => Services Life + Energy + Security
- Contrôle d'accès => Services Life + Security
  
- Stockage => Service Energy
- Véhicule => Services Life + Security

Ex: Véhicule électrique (profils Véhicule + Stockage)

# les services

life

## ► confort

- vacances => éco super
- travail => éco on 1
- a la maison (jour) => éco off
- a la maison (nuit) => éco on 2
- je vais rentrer (10 min)
- je vais partir (10 min)

## ► user defined

- 1 à 10

# les services

energy

▶ **production**

- solaire
- géothermie
- éolien
- hydraulique
- ...

▶ **stockage**

- batterie
- véhicule électrique
- ...

▶ **consommation**

- chauffage
- eau chaude sanitaire
- refroidissement
- éclairage
- véhicule électrique
- ...

▶ **gestion**

- instantanée
- prévisionnelle
- paramétrage
- délestage
- ...

▶ **supervision**

- grids (pays, ville, quartier)
- auto-consommation
- ...



# les services

security

▶ **alarme**

- présence
- absence
- intrusion
- ...

▶ **contrôle d'accès**

- habitants
- véhicule
- intervenants récurrents
- intervenants occasionnels
- invités
- ...

▶ **vidéo-surveillance**

- caméras
- interphonie
- ...

# les services

multimedia

▶ **vidéo**

- affichage
- supervision
- vidéo-surveillance
- visiophone
- journalisation
- télévision

▶ **audio**

- annonces
- interphone
- musique
- radio

# LE DEMONSTRATEUR



**ILS NOUS ONT SOUTENUS**





VILLE DURABLE

EXEMPLES DE RÉALISATIONS CONCRÈTES

## CONFLUENS



Le projet CONFLUENS vise l'interopérabilité domotique via la constitution d'un métalangage qui s'intégrera dans les équipements domotiques neufs comme existants. Maquettage en 2015, déploiement en 2016, exportation en Europe en 2017. À l'initiative de Ignes, de la FIEEC, des entreprises CDVI, Delta Dore, Hager, Legrand, Schneider Electric et Somfy, la société Confluens a été créée pour développer la solution.

**Soutien public:** Soutien au Programme d'investissements d'avenir à hauteur de 1,80 M€ pour une assiette projet de 4,10 M€.

**Technologie clé:** Objets communicants.



# C*o*NFLUENS

smart-home digital network for services