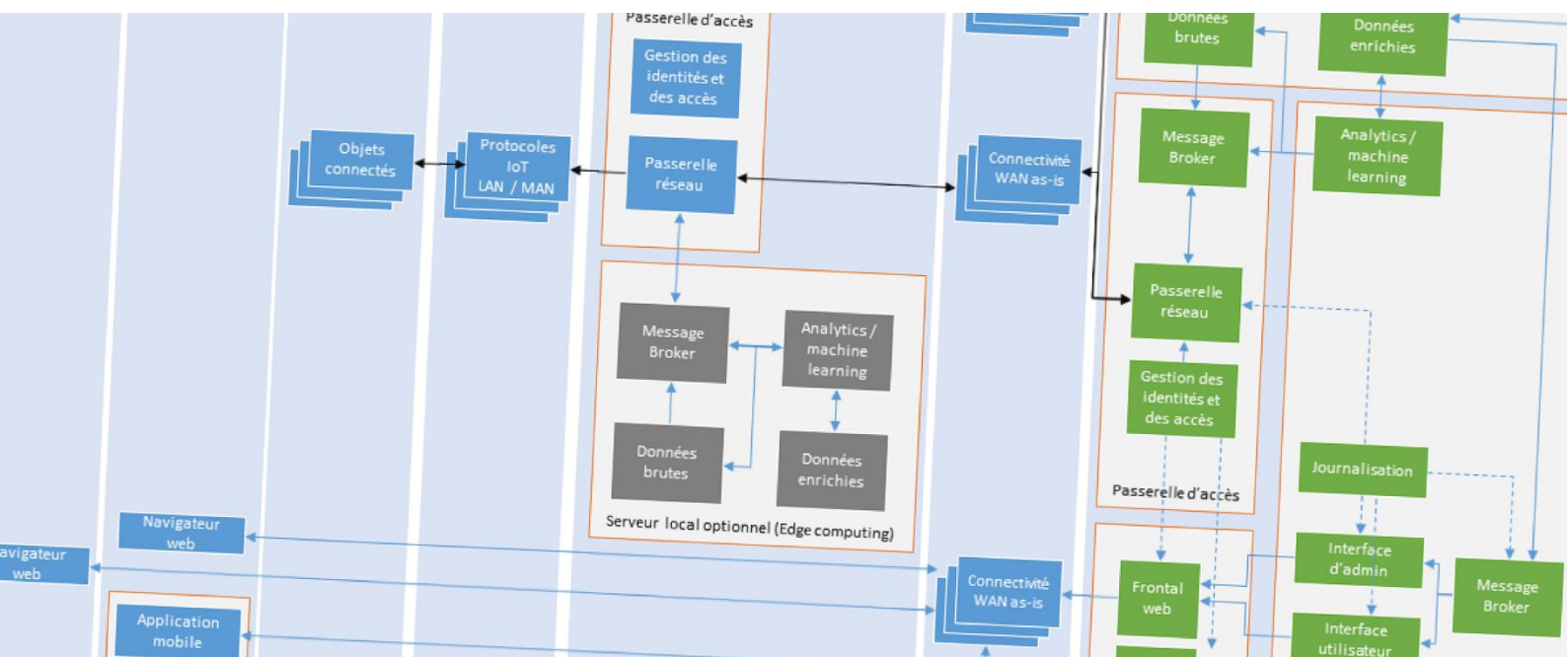


LES FICHES PRATIQUES du CLUSIF - IoT



QU'EST-CE QU'UN OBJET CONNECTÉ ?

Version 1.0

De nombreuses définitions ont été proposées au fil des années, démontrant l'évolution du concept ainsi que sa montée en maturité progressive. Au final, nous retenons la version suivante :

Un **objet connecté** peut être défini comme étant un « objet physique usuel pouvant interagir avec son environnement et enrichi de capacités de communication lui permettant d'être interrogé ou contrôlé à distance par l'intermédiaire d'un réseau privé ou d'Internet ». Il peut s'agir par exemple d'un capteur ou d'un actionneur connecté.

Par extension, un **système connecté** consiste en « un ou plusieurs objet(s) connecté(s) interagissant avec les autres composants du système selon certains principes

ou règles dans le but d'apporter de la valeur au système d'origine ». Exemple : voiture connectée, chaîne de fabrication connectée, système domotique, etc.

Un **écosystème connecté** représente « l'ensemble des ressources nécessaires au fonctionnement d'un système connecté et reposant généralement sur un ou plusieurs objets connectés, une passerelle de communication vers Internet et un service de type Cloud associé à une interface web ou/et mobile ».

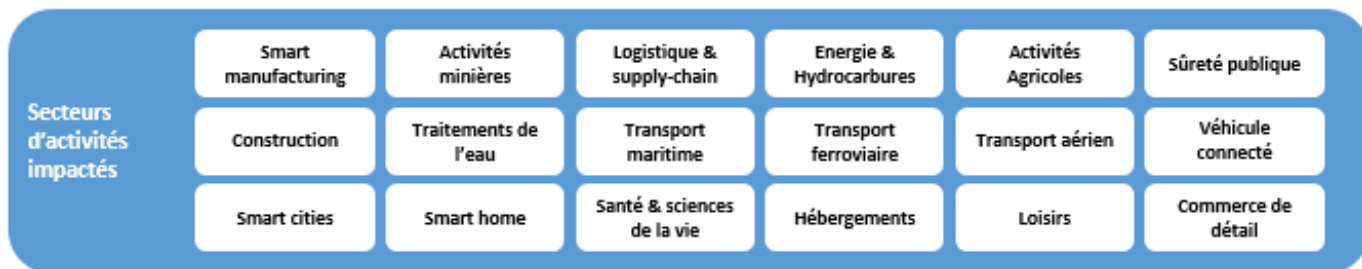
L'**Internet des objets** (Internet of Things - IoT) est un terme générique pouvant désigner un « ensemble de systèmes ou d'écosystèmes connectés pouvant être fédérés via Internet ».

1. PÉRIMÈTRE, USAGES ET ENJEUX

Les objets connectés accompagnent la transformation numérique des entreprises et organisations existantes. Ils enrichissent des systèmes en place, et traduisent la convergence des domaines des Systèmes d'Information de gestion¹ et des Systèmes d'Information industriels². Le périmètre fonctionnel couvre des secteurs d'activité très variés, tels que représentés ci-après.

¹ Les SI « gestion » reposent sur des actifs support de type IT (Information Technology).

² Les SI « industrie » reposent sur des actifs support de type OT (Operational Technology).

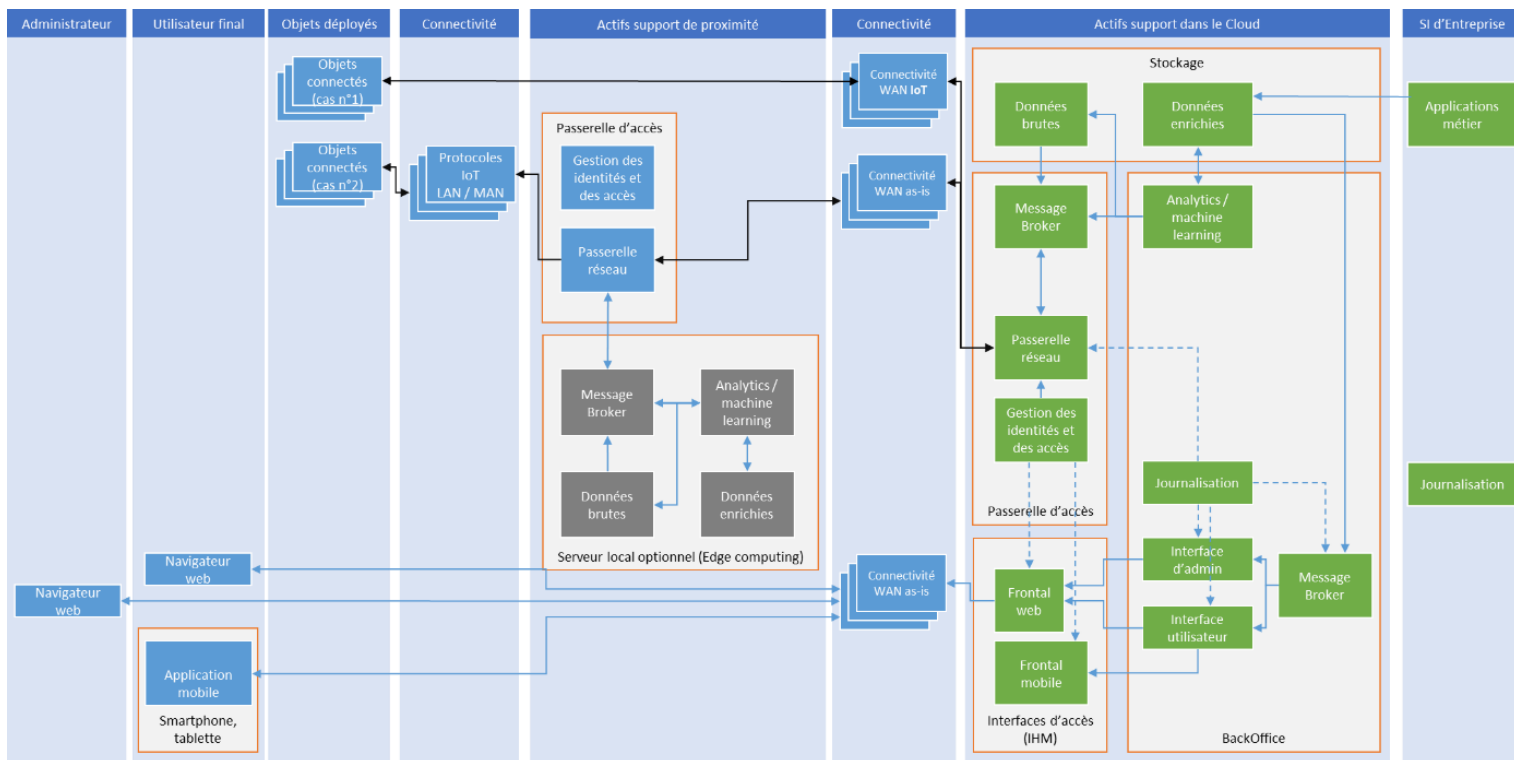


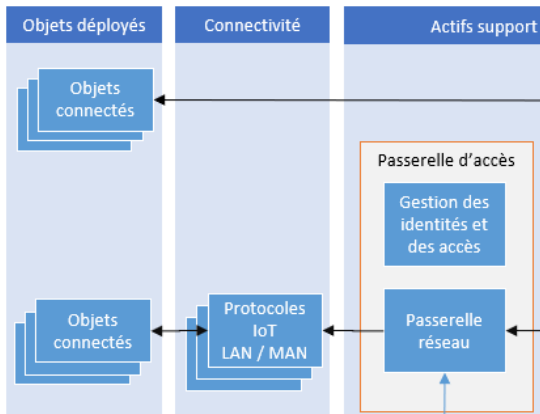
Précision : Le groupe de travail « Sécurité de l'IoT » du CLUSIF a cependant exclu de son champ d'investigation les applications industrielles (usines, infrastructures critiques, Industrial IoT, etc.), celles-ci étant déjà couvertes par le groupe de travail : « Sécurité des Systèmes Industriels ».

En termes d'usages métier, l'objectif consiste à « collecter, stocker, organiser et traiter l'information issue de ces objets en vue de créer une valeur ajoutée complémentaire ». Par exemple, cette valeur peut se traduire par des gains de temps, une simplification du quotidien ou la réalisation d'une maintenance prédictive.

2. ARCHITECTURE FONCTIONNELLE D'UN ÉCOSYSTÈME CONNECTÉ

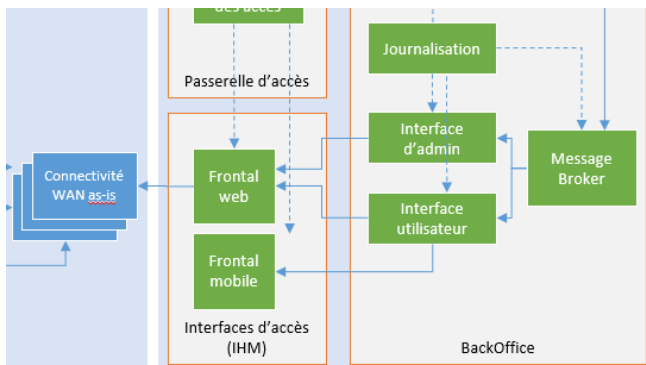
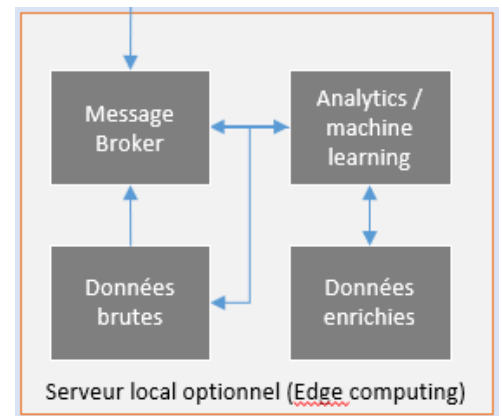
L'architecture fonctionnelle d'un écosystème connecté peut être synthétisée par le schéma suivant :





L'écosystème représenté intègre a minima un ou plusieurs objets connectés, pouvant être ou non de même nature, éventuellement une passerelle permettant de fédérer les objets entre eux.

Un écosystème plus complexe peut également intégrer un serveur local (Edge computing) permettant de répondre à des exigences temps-réel ou de latence. Une tablette ou un smartphone, ainsi qu'une application mobile peuvent compléter le dispositif pour permettre l'accès aux données.



Une application backoffice hébergée sur une infrastructure Cloud ainsi qu'une interface d'accès web complètent cette architecture.

Les protocoles IoT à utiliser dépendent des exigences fonctionnelles et techniques exprimées par le métier : il peut s'agir par exemple d'une exigence de portée du réseau (protocole de portée locale, régionale, nationale ou internationale) mais également d'une exigence de confidentialité des données à laquelle les concepteurs de la solution pourraient répondre en choisissant de mettre en œuvre un protocole intégrant une couche de chiffrement des données échangées.

Lors de l'utilisation d'une passerelle locale, la connectivité WAN « as-is » désigne les solutions de raccordement non spécifiques au monde IoT : 3G/4G/5G, ADSL, fibre, etc.

Par ailleurs, les brokers permettent non seulement de découpler les échanges entre deux environnements, renforçant ainsi leur résilience, mais également de réaliser des vérifications sur le contenu et le format des données échangées. Les vérifications sur le contenu assurent la cohérence des données échangées, renforçant ainsi le niveau de confiance associé (donnée médicale aberrante par exemple). Le contrôle sur la forme limite les effets de bord liés à des données incorrectement formatées.



Précisions et limites de l'architecture présentée :

À des fins de clarté, cette représentation volontairement simplifiée d'un écosystème connecté ne détaille pas les fonctions des objets connectés en eux-mêmes.

Celles-ci dépendent en effet de la nature de l'objet (déterminés lors de la phase de conception initiale) et des objectifs de sécurité associés (déterminés lors de l'analyse de risque).

D'autres simplifications ont également été opérées : L'interconnexion avec un système d'information tiers pour la remontée et le traitement des journaux d'événements n'a pas été représentée. Les flux d'administration du serveur local ont également été écartés même si certains cas d'usage peuvent les nécessiter (métro autonome par exemple) en regard des résultats de l'analyse de risques.

① Point de vue du RSSI

La conception, l'intégration et le déploiement d'objets, systèmes et écosystèmes connectés accompagnent la transformation numérique de l'ensemble des secteurs d'activités.

Ils permettent de collecter, stocker, organiser et traiter les données collectées et de réagir de manière prédéfinie ou dynamique à des événements du monde réel, que ce soit en interagissant avec leur environnement ou en permettant d'améliorer ou d'adapter les processus concernés.

Cette révolution peut être source de progrès mais également favoriser l'émergence de nouvelles menaces, en raison notamment de l'augmentation de la surface d'attaque des systèmes d'informations résultant de cette transformation. Les impacts peuvent être de nature humaine, sociale, environnementale, mais également financière et juridique.

LES FICHES PRATIQUES

L'intégralité de la FAQ IoT et la liste des membres qui ont contribué à son élaboration sont consultables sur le site du CLUSIF : www.clusif.fr/publications

