CONSTRUIRE UN TERRITOIRE DE CONFIANCE ET DE SÉCURITÉ

SBA
théma 4

La Commission SBA Safe City

Née du rapprochement de la SBA et de l'AN2V (Association nationale de la vidéoprotection) à l'hiver 2017, la commission Safe City s'est fixé comme objectif de porter le message que le développement de la Smart City et des Smart Territoires ne pourra se faire de manière pérenne sans y associer une dimension de sécurité et de sûreté.

Ses réunions de travail ont été l'occasion pour les contributeurs de tâcher de définir ce qu'est une Safe City, de rapprocher les acteurs de la chaîne de valeur de la Smart City à ceux de la sécurité et de la sûreté pour une prise en compte mutuelle des enjeux et impératifs de chacun, et enfin de rédiger le présent guide à l'attention des collectivités et des pouvoirs publics pour la construction de la Smart & Safe City de demain.

Remerciements

Ce livret, fruit de nombreux échanges riches et passionnés, n'aurait pu voir le jour sans la contribution des membres de la commission que nous remercions chaleureusement :

Eddy Benesteau, DIRECTION GÉNÉRALE DE LA GENDARMERIE NATIONALE ● Jean-René Bouzonie, SALTO SYSTEMS ● Frédéric Brûlefert, LORIAS ● Christian Carle, POLE STAR ● Lilian Caule, ANITEC ● Vincent de l'Estang du Rusquec, DIRECTION GÉNÉRALE DE LA GENDARMERIE NATIONALE ● Camille Dubedout, ANSSI ● Michaël Fumery, DIRECTION GÉNÉRALE DE LA GENDARMERIE NATIONALE ● Éric Hazane, ANSSI ● Patrick Lavergne, ILOGS FRANCE ● Rémy Nollet, DIRECTION GÉNÉRALE DE LA GENDARMERIE NATIONALE ● Jean-Yves Orsel, DOVOP ● Éric Roland, AZURSOFT ● Jacques Roujansky, CICS ● Stéphane Schmoll, DIDAXIS

Et plus particulièrement pour leur soutien et leur investissement :

Gendarmerie nationale

AN2V ASSOCIATION NATIONALE DE LA VIDÉOPROTECTION

ANITEC ALLIANCE NATIONALE DES ENTREPRISES DE TECHNOLOGIES CONNECTÉES, SÉCURISÉES ET PILOTÉES

Emmanuel François : Direction de la publication
Alain Kergoat : Direction des programmes
Florian Mercier : Direction éditoriale
Dominique Briquet : Coordination projet

Couverture et illustrations © Les 5 sur 5
Réalisation : DoYouMeanBlue

Imprimé en France. Dépôt légal : août 2019. ISBN 978-2-95601-757-8

CONSTRUIRE UN TERRITOIRE DE **CONFIANCE** ET DE **SÉCURITÉ**

Les territoires doivent générer et maintenir la confiance indispensable à leur attractivité et à leur efficience pérenne. Les usagers des bassins de vie (citoyens, entreprises, etc.) attendent des autorités un niveau d'engagement de service suffisamment élevé et constant, ou en progrès mesurable.

L'État a pour rôle de mettre en place des politiques publiques générales, d'adapter la législation et les réglementations aux solutions intelligentes et efficientes, d'encourager la standardisation et l'interopérabilité, et de participer le cas échéant à certains investissements.

Pour leur part, les Collectivités territoriales peuvent relayer ces politiques publiques en les adaptant à leurs spécificités géographiques, économiques et sociologiques, tout en définissant les meilleures solutions et en pilotant leur mise en œuvre. La participation active et impliquée de tous les acteurs locaux, y compris les citoyens eux-mêmes, est indispensable pour satisfaire l'exigence de niveau de service attendu. Si ces derniers ont des droits, ils ont aussi des devoirs vis-à-vis des collectivités et doivent s'inscrire dans cette démarche participative.

Ce guide n'a pour autre ambition que de sensibiliser les élus des collectivités territoriales à l'importance d'intégrer la dimension « Safe » dans leurs démarches de construction d'une Smart City ou d'un Smart Territoire. La convergence de ces deux concepts favorisera la transformation des territoires géographiques des collectivités en véritables Territoires de Confiance.

Force est de constater qu'il est plus aisé pour un élu de parler de Smart City à ses concitoyens plutôt que de Safe City : le sujet est plus clivant, plus risqué aussi dans la perception de ce qui sera fait… ou pas ! Et pourtant, le Smart et le Safe ne peuvent pas être dissociés, l'un n'allant jamais sans l'autre. Cependant, le côté *Safe* arrive plus bas dans la pyramide de Maslow (juste après le besoin de se nourrir), c'est une condition vitale afin de pouvoir profiter sereinement des niveaux plus haut de cette même pyramide : être dans le smart, c'est profiter pleinement de son environnement, de sa ville, du plaisir d'être avec les autres, avec des services nouveaux, avancés et pertinents.

C'est la raison pour laquelle nous avons œuvré dans ce guide à une tentative de description des fondamentaux de la Cité Safe et Smart. Dans un premier temps, en changeant ces deux anglicismes et en évoquant plutôt les « territoires de confiance » afin de réunir tous les concepts, au moins sur deux plans : Territoires, car toutes surfaces doivent être prises en compte, du centre-ville le plus dense à la commune rurale la plus isolée, et Confiance, car au-delà de la mise en sécurité, la confiance est ce à quoi nous aspirons tous.

Vivre dans un territoire apaisé et agréable, tel est notre vœu. Nous vous souhaitons une lecture attentive de ce condensé de toutes nos réflexions menées durant un an, de manière parfois très contradictoire mais toujours dans la bonne humeur, avec des profils de compétences très complémentaires. L'AN2V est fière d'avoir participé à tous ces travaux et nous remercions la SBA d'avoir eu l'initiative de créer ce groupe de travail.

Florian Mercier
Responsable Développement - SPIE CityNetworks
Président de la commission Safe City

Dominique Legrand
Président - AN2V
Coprésident de la commission Safe City

SOMMAIRE

ENJEUX & ATTENTES

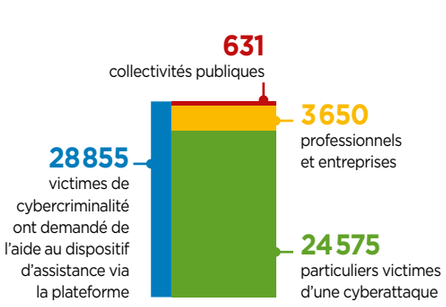
DONNÉES ET STATISTIQUES

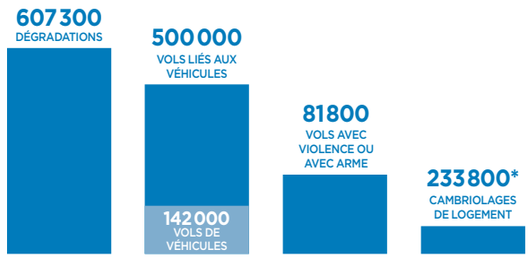
Les citoyens, pour leur ville, placent la sécurité en deuxième position (à 46%) de leurs préoccupations derrière le logement (54%). C'est peu dire que le sujet est d'importance et qu'il ne peut pas être traité de façon désordonnée. À cela s'ajoute l'impérieuse nécessité d'apporter la sécurité dans la vie «numérique» et connectée: 92% des français sont connectés à Internet, dont plus de 58% sont des utilisateurs actifs des réseaux sociaux, et 93% de la population est équipée de téléphones mobiles, dont 71% d'un smartphone. *(Source: Hootsuite.com)*

Cette tendance à être connecté de façon permanente est une tendance de fond, une révolution sociétale, avec son lot de menaces sur la sécurité, individuelle et collective. Le site www.cybermalveillance.gouv.fr lancé en 2017 permet de recenser les victimes et de dresser un panorama des risques.

Pour les citoyens et tous les usagers des territoires, leur sécurité doit être assurée de façon continue, dans l'espace privé et dans l'espace public, dans l'espace physique comme dans l'espace numérique.

EN 2018





* Tous les chiffres viennent du SSMSI.

L'ENGAGEMENT CITOYEN

La numérisation des services publics, des services marchands, des services de mobilité, etc, oblige à une attention et sensibilisation de tous par l'information et la formation, et entraine une responsabilité particulière des acteurs publics, des collectivités locales et territoriales.

Le village, la ville, l'agglomération «intelligente» pourraient se résumer à un ensemble de services mis à disposition des usagers, résidents, salariés ou visiteurs. Que ces services soient tangibles ou numériques, le besoin de sécurité est la base, la fondation. La sécurité: la notion de disponibilité, de qualité et de sécurité de service sont essentielles dans la perception qu'en auront les citoyens et les usagers.

Il est d'usage de dire que la sécurité est l'affaire de tous. C'est un fait, que les citoyens et les usagers de la ville en sont des acteurs essentiels par leur civisme et la sensibilisation qu'ils reçoivent. Chaque citoyen, chaque usager est un capteur mobile d'information qui, s'il est connecté, devient un maillon clé de la prévention des risques et à de la résolution des crises.

Le village, la ville, la métropole, pour être intelligent, doivent être pensés dans leur ensemble comme un territoire de confiance qui permettra de développer et mettre en œuvre des services aux usagers physiques et numériques, prêts à l'emploi, et sécurisés. Cela implique une dose de civisme, illustrée par la circularité du concept: éduquer, pour mieux prévenir et dissuader, pour mieux établir la confiance.

LES ENJEUX

On estime que dans les années à venir le pourcentage de la population vivant dans les territoires urbains et périurbains va croître de manière significative. La question de la sécurité va de ce fait devenir de plus en plus prégnante pour les autorités publiques qui devront mettre tout en œuvre pour garantir aux concitoyens un territoire de confiance sans couture: il ne doit pas y avoir de rupture du sentiment de sécurité.
Ce risque de rupture de confiance est un défi majeur qui est posé aux institutions et aux citoyens: il faut pour cela savoir réinventer la ville pour que celle-ci soit collaborative, vivante, et que tout le monde s'y sente bien. Réinventer la ville, en réinventant les liens de confiance, notamment à travers des programmes éducatifs et pédagogiques: montrer que les bénéfices dépassent les risques, tel est l'enjeu de la confiance.

Mais attention à trouver le bon dosage: le projet smart dans son ensemble permettra de réinventer le territoire, mais pourra aussi en accentuer la fracture; ce risque appelle à une très grande vigilance de la part des élus.

Une attention particulière devra être également prêtée à la sécurisation des dispositifs, notamment face aux failles liées au numérique (cyberattaques, comportements, bons usages, répartition de la sécurité numérique, compartimentation...): cet enjeu est encore bien trop peu appréhendé aujourd'hui.

LES ATTENTES

Le citoyen, usager des territoires, a une vision linéaire, descendante, des services de sécurité: la grande majorité se positionne en situation de «recevoir» les services, d'être destinataire des opérations de protection et de sécurité mises en œuvres par les forces publiques et privées.

Il est essentiel d'œuvrer à la transformation de cette vision, en faisant passer le citoyen d'une position linéaire à une position circulaire: le citoyen doit être le maillon qui s'insère dans la chaîne globale de la sécurité, étant tour à tour utilisateur et acteur. En effet, ne pas oublier que si le citoyen a des droits, il a aussi des devoirs envers la collectivité.

Au cœur de la confiance se trouvent l'adhésion et l'acceptation: pour construire un territoire de confiance, il est essentiel de faire adhérer l'ensemble des contributeurs, et notamment le citoyen. Positionné au cœur du dispositif, il légitimera toutes les actions entreprises par les pouvoirs publics.
Les élus doivent pouvoir proposer des politiques participatives permettant de répondre ainsi aux attentes suivantes:
- garantir la sécurité dans la mobilité, en tout lieu, y compris dans les bâtiments (indoor);
- garantir un territoire qui protège le citoyen;
- garantir un territoire de continuum de services;
- garantir un territoire inclusif;
- garantir la tranquillité publique;
- garantir le sentiment de bien être.

LES CLÉS

Le fait que le Citoyen soit un coproducteur de la sécurité sous-entend pour lui acceptabilité et engagement actif. Pour cela, il faudra être pédagogue. C'est là un des rôles majeurs des élus: obtenir l'adhésion en transmettant l'envie à travers la création d'espaces numériques citoyens permettant l'apprentissage et l'acquisition de réflexes liés à la sécurité.

Beaucoup de collectivités ont déjà un espace citoyen mais qui n'inclut pas forcément de volet incivilité, sécurité ou sûreté: ce point est à faire évoluer.
Afin d'assurer un service minimum de sécurité, les collectivités devront établir une charte pour donner de nouveaux rôles aux bénéficiaires, aux contributeurs, aux opérationnels. Le déploiement d'une boucle continue d'information, de dispositif technique bidirectionnel, d'infrastructure réseaux, améliora la prévention et la protection, et ce à moindre coût.

Enfin, il conviendra de garantir une qualité de service et de disponibilité quelles que soient les situations, normales ou de crise: résilience et interopérabilité sont des notions majeures pour assurer des services numériques disponibles, sécurisés, performants, et ce en tout instant et en tout lieu.

PRINCIPAUX **ACTEURS**

LES SERVICES DE L'ÉTAT

Toute approche de sécurité des territoires s'appuie sur les services de l'État qui ont des responsabilités, des prérogatives et des ressources uniques. Il s'agit de la Police nationale, de la Gendarmerie nationale, de la Justice, des services préfectoraux, et de la sécurité civile qui s'appuie sur les sapeurs-pompiers des services départementaux d'incendie et de secours, les renforts zonaux ou nationaux, les associations agréées ainsi que les services ambulanciers médicaux d'urgence.

Ces acteurs pour participer à une nouvelle approche doivent s'adapter pour mieux s'interfacer et échanger en toute fluidité avec les autres acteurs du territoire, de la même façon qu'ils s'interfacent entre eux, par exemple pour traiter les urgences dans le cadre du 112. Il faut assurer le *continuum* de la sécurité.

LES COLLECTIVITÉS TERRITORIALES

La commune est un échelon essentiel de la sécurité, car les prérogatives du maire restent fortes sur les infrastructures locales comme sur les aspects de prévention de la délinquance (conseil local de prévention de la délinquance, vidéoprotection, ...), opérationnels (police municipale, plan communal de sauvegarde, ...), ou exceptionnels (transports dans certains cas, gestion d'événements sur la voie publique...).

Les établissements publics de coopération intercommunale (de la communauté de communes à la métropole, en passant par les syndicats tournés vers l'équipement numérique ou énergétique), départements, régions, jouent un rôle moteur, renforcent la couverture avec leurs responsabilités directes ou déléguées sur les voiries et les réseaux, voire permettent des architectures élargies des dispositifs visés. Le dialogue entre toutes ces collectivités est nécessaire pour assurer une vision d'ensemble, la synergie et la cohérence, tout en s'adaptant à la réalité de mobilité des habitants. Les choix de gouvernance d'une approche territoriale élargie résultent de ce dialogue.

LA FILIÈRE DE LA SÉCURITÉ

La filière de sécurité apporte aux parties prenantes les solutions technologiques et services nécessaires à la conception, à la réalisation et aux opérations, des instruments de la confiance et de la sécurité des territoires. Elle intervient dès la conception des territoires intelligents pour assurer nativement la sécurité des équipements urbains, des infrastructures et services physiques, électroniques et numériques des territoires, et viser ab initio la synergie entre la sécurité et les autres finalités telles que mobilité, santé, inclusion, environnement.

Les professionnels des filières de sécurité privée et industrielle proposent des solutions sur les :
- segments capacitaires : observation, détection, analyse, décision, coordination, alerte, intervention, prévention, flux, etc.
- segments technologiques : protection physique, vidéoprotection intelligente, hypervision, big data, intelligence artificielle, réseaux, cloud, IoT, cybersécurité, protection des données, blockchain, etc.

Au cœur de la filière, les acteurs de confiance apportent des réponses nationales ou territoriales la protection et la souveraineté des données et des transactions.
Face à la complexité d'approches ambitieuses, il est nécessaire d'entretenir un dialogue générique constant entre les prescripteurs, les utilisateurs (régaliens, entreprises, collectivités) et l'industrie.

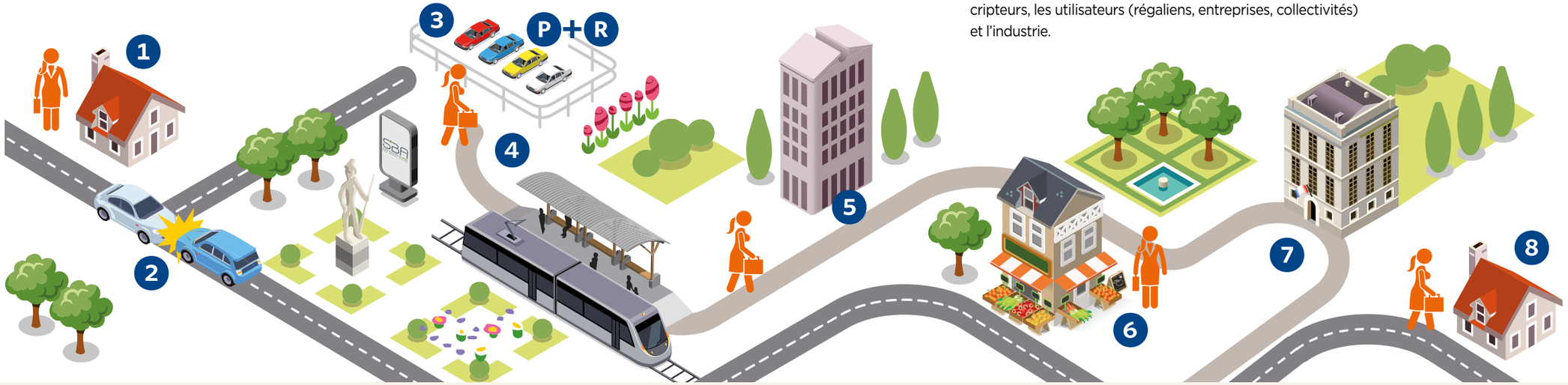
LES ACTEURS ÉCONOMIQUES

La sécurité des territoires ne s'arrête à l'espace public. L'activité s'exerce dans un espace où public et privé s'imbriquent : entreprises, magasins, lieux associatifs ou de culte, transports, espaces de loisirs, etc. La sécurité concerne aussi les opérateurs d'infrastructures sur le territoire : eau, énergie, communication, etc, nécessaire à l'activité économique et à la vie du territoire. Des approches collaboratives à l'interface de ces espaces et des processus sont indispensables pour définir des réponses d'ensemble efficaces.

LES USAGERS DES TERRITOIRES

L'usager (citoyen, touriste, voyageur, passager) n'est plus le simple bénéficiaire passif de la sécurité. Il est contributeur, élément actif du dispositif en cas d'événement, et source d'information de masse. Le numérique facilite les consultations, les orientations, voire la mesure des politiques de sécurité par les usagers, faisant ainsi croître l'implication des citoyens dans leur sécurité et dans sa gouvernance.

EXEMPLE DE JOURNÉE D'UN USAGER ET DÉTAIL DE SES RENCONTRES AVEC LES ACTEURS DU TERRITOIRE DE CONFIANCE ET DE SÉCURITÉ



1 Départ de la maison
2 Alerte accident
3 Parc relais
4 Transport en commun
5 Journée au bureau
6 Courses du soir
7 Participation citoyenne
8 Retour maison

SERVICES DE L'ÉTAT
- Forces de l'ordre
- Sécurité civile, santé

COLLECTIVITÉS TERRITORIALES
- Maire, Président d'EPCI
- Police municipale
- Pompiers

FILIÈRE DE LA SÉCURITÉ
- Téléopérateur
- Entreprise de sécurité

ACTEUR ÉCONOMIQUE
- Commerce

CONCEPTS & **MÉTHODOLOGIES**

SÉCURITÉ INTELLIGENTE : TROIS INSTANTS À DISSOCIER POUR TOUT ACTE DÉLICTUEUX

La dernière stratégie nationale de prévention de la délinquance, dans son programme d'actions pour améliorer la tranquillité publique, intégrait des approches de prévention , en particulier de vidéoprotection, et de présence humaine. À l'heure des territoires intelligents, il n'est pas question de remettre en question cette complémentarité des outils techniques et des moyens humains. Toutefois, ces vingt dernières années, les caméras étaient quasiment les seuls capteurs techniques déployés et les effets sur le terrain semblaient dépendre essentiellement de l'engagement des moyens humains.

Aujourd'hui, les territoires intelligents vont permettre à la fois de disposer et de croiser beaucoup plus de sources d'information (reporting citoyen, capteurs de mouvement, de son…) et d'agir de façon multiple, à la fois par une action humaine «augmentée», mais aussi par l'information du public, la mise en sécurité d'espaces ou d'itinéraires…

Ces évolutions technologiques ne changent pas pour autant la méthodologie qui doit continuer de s'appuyer sur des outils déjà éprouvés. Ainsi, les cycles temporels permettent d'analyser les besoins pour prévenir, intervenir, élucider, tandis que la gouvernance favorisant le partage de l'information doit désormais s'envisager aussi bien dans les structures de pilotage que dans les outils techniques.

La question de la réactivité de la protection intelligente en cas d'événement est une des principales réflexions à conduire.

AVANT : LA DISSUASION

Avant le passage à l'acte : l'objectif ultime, qu'il soit atteint grâce à des moyens technologique ou humains, n'est-il pas tout compte fait d'éviter le passage à l'acte ? La vidéoprotection et le contrôle d'accès peuvent créer un obstacle qui rendra le passage à l'acte plus difficile, plus risqué. En cela, les dispositifs techniques sont des moyens de prévention situationnelle. Nous pourrons parler ici de prévention technologique, ou de dissuasion technologique.

1. SÉCURITÉ DES PERSONNES
2. SÉCURITÉ DES BIENS
3. SÉCURITÉ DE L'ESPACE NUMÉRIQUE

Attention, si on ne prend en compte que l'objectif de dissuasion, la logique nous conduit à ne déployer que des dispositifs très visibles, imposants, voire inopérants (caisson vide ou caméra obsolète), pourquoi pas ? En effet, elles dissuadent ! Donc elles répondent à leur mission… Mais qui prendra le risque de faire croire qu'une caméra fonctionne alors qu'elle est défectueuse, qu'elle n'enregistre pas, ou mal, ou plus… L'efficience de dissuasion est bonne mais il sera impossible de produire des images sur événement grave, en temps réel ou en temps différé.

PENDANT : PROTECTION, INTERVENTION

Pendant le passage à l'acte (voir schéma ci-contre) : l'objectif est alors de repérer l'événement et de déclencher la réponse adaptée. Chaque seconde compte, de jour comme de nuit, un fait, un bien, ou une personne est en danger et il convient de tout mettre en œuvre pour que l'infraction cesse au plus vite, que les moyens humains appropriés puissent intervenir en toute connaissance de cause, de manière proportionnée et efficace, avec les bons outils (feu, cambriolage, rixe, perte de connaissance…). Encore faut-il pour cela que les dispositifs techniques et que l'organisation humaine soient aptes à réagir immédiatement, en temps réel !

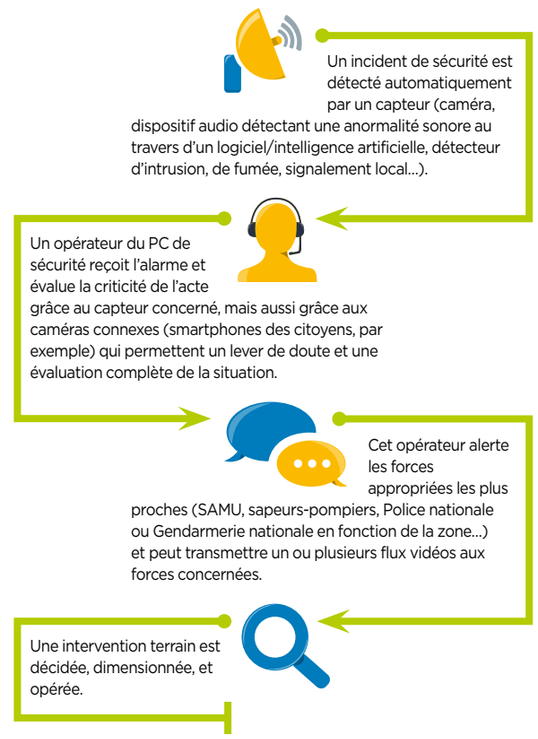
APRÈS : ÉLUCIDATION, INVESTIGATION, ENQUÊTE

Après le passage à l'acte : l'infraction a cessé. Le mal est fait !

Il est temps de comprendre le séquencement des actes : Qui a fait quoi ? Comment ? Pourquoi ? Pour cela, il est précieux de posséder les enregistrements d'une ou plusieurs séquences vidéo (plusieurs angles de vues) permettant de noter un visage, un vêtement, un comportement, une plaque minéralogique, un type de véhicule…

L'objectif est d'élucider, pour éviter la récidive d'une part, et d'autre part, pour que l'auteur soit confondu – au plus vite et à moindre coût – et assume les conséquences de ses actes. Il faut à cet égard rappeler ici que la vidéoprotection et les autres données enregistrées issues des divers capteurs apportent des éléments à charge mais également à décharge. Ces données permettent notamment de mettre au clair les conditions d'intervention de chacun.

ENCHAÎNEMENT DES TÂCHES



LES CLEFS DE LA DISSUASION

Les axes à développer pour mettre en œuvre la dissuasion sont :
- Prévention situationnelle
- Prévention sociale
- Intelligence des territoires
- Évaluation des risques
- Relations et aide
- Assistance éducative
- Police de sécurité du quotidien
- Prédictif

GOUVERNANCE

DÉCLOISONNEMENT

Le constat est partagé que la technologie avance de plus en plus rapidement, notamment avec la percée remarquée de l'intelligence artificielle ainsi que des investissements et des ressources financières et technologiques des GAFAMI[1] et BATX[2].

Toutefois, la capacité de déployer cette nouvelle offre technologique plafonne alors qu'il est pourtant indispensable d'être de plus en plus efficient, compte-tenu des contraintes de budget et des attentes citoyennes. Cela s'explique, à notre sens, par le fait que les projets demeurent traités « en silos », de manière cloisonnée au sein des organisations. De plus, l'environnement juridique reste souvent figé voire timoré, et tend à restreindre les nouvelles possibilités de déploiement.

UNE NÉCESSAIRE CONDUITE DE CHANGEMENT SUR LES SILOS

Il est regrettable que certains dossiers soient freinés par une trop faible prise en compte du facteur humain. Il parait essentiel de miser sur l'intelligence collective et d'intégrer une approche collaborative des projets comme un puissant levier d'accélération des transformations.

Il est donc indispensable d'ouvrir les champs de compétence de conduite du changement. Dans les organisations, la sécurité/sûreté est en effet l'affaire de tous les acteurs, mais associer leurs compétences individuelles ne suffit pas à relever le défi.

La solution est dans la mise en place d'un collectif inter services performant quelle que soit l'organisation publique ou privée dont il s'agit.
Nous pouvons par exemple noter les obstacles terrains suivants, à lever :
– le fait que l'organisation de l'établissement ne fonctionne pas en mode projet ;
– le manque de connaissances dans le domaine de la ville intelligente, dont tous n'ont de fait pas la même définition ;

1. GAFAMI : Google, Apple, Facebook, Amazon, Microsoft, IBM.
2. BATX : Baidu, Alibaba, Tencent, Xiaomi.

– le manque de clarté sur le sens et les priorités données aux différents projets lancés ;
– la faiblesse de la communication interne, là où une communication forte et structurée est nécessaire ;
– la fracture numérique au sein de l'établissement, certains agents n'étant pas à l'aise avec le numérique ; combinée à la faible disponibilité pour des temps de formation et d'appropriation ;
– le déploiement non généralisé dans les services de terminaux mobiles (smartphones ou tablettes) et de manière générale des outils numériques ;
– le manque de polyvalence et la très faible interconnexion des différents logiciels métiers ;
– la disparité des services au niveau de la gestion industrialisée et donc de la collecte de données.

Par ailleurs, il nous semble nécessaire au contraire de :
– développer la transversalité et le travail en mode projet – ce qui permettrait aux services de mieux se connaître et se comprendre ;
– revoir et améliorer l'organisation du travail dans les services, en s'inspirant par exemple des douze recommandations du R2S de la SBA ;
– remettre à plat et moderniser les systèmes d'information ;
– renforcer la communication interne, à tous les niveaux de l'établissement et également en externe.

LE CONTINUUM DE SÉCURITÉ

Le rapport parlementaire des députés Fauvergue et Thourot a récemment mis en lumière le concept de « continuum de sécurité » qui consacre la reconnaissance d'acteurs à part entière de la sécurité : les Polices municipales (PM) et intercommunales (21 000 agents) et la sécurité privée (170 000 personnels). Les propositions avancées feront l'objet d'une large concertation, incluant les élus, et seront étudiées à l'automne 2019 dans la perspective de la rédaction du livre blanc de la sécurité intérieure.

De nombreuses avancées au cours des dernières années (notamment : les conventions de coordination entre les Polices municipales (PM) et les Forces de sécurité de l'État (FSE), la mise en place de patrouilles conjointe Gendarmerie/SUGE (Surveillance générale dans la cadre de la sûreté ferroviaire), les conventions d'échange avec les bailleurs sociaux, l'évolution de l'armement des polices municipales, la création du CNAPS (Conseil national des activités privées de sécurité), le développement de l'interopérabilité radio entre FSE et PM, et la toute récente possibilité d'employer des agents de sécurité privée armés…) amènent à réfléchir sur la nécessaire mise en cohérence du rôle des acteurs non-régaliens avec l'action des forces étatiques, pour construire une « sécurité partagée ».

Par ailleurs, depuis la loi Notre, la prévention de la délinquance se décline localement au niveau :
– de la commune : la structure d'animation peut être le Conseil local de sécurité et de prévention de la délinquance (CLSPD) ; « le Maire anime et coordonne la politique de prévention de la délinquance et en coordonne la mise en œuvre » (L. 132-4 CSI) ;
– ou dans le cadre des regroupements de communes au sein d'un éventuel Conseil intercommunal de sécurité et de prévention de la délinquance (CISPD). La prévention de la délinquance relève ainsi obligatoirement de la structure intercommunale pour : les communautés d'agglomération (art. L. 5216-5 du Code général des collectivités territoriales), les communautés urbaines (article L. 5215-20 du CGCT), et les métropoles (art. L. 5217-2 du CGCT), à l'exception du Grand Paris.
C'est une compétence facultative pour les communautés de communes (art. L. 5214-16 du CGCT).

Les CISPD sont donc obligatoirement mis en œuvre au sein des métropoles (22), des communautés d'agglomération (222) et des communautés urbaines (11), mais facultatifs au sein des communautés de communes (1009). Pour autant, le Président du CISPD (Président d'EPCI ou adjoint) ne dispose pas des pouvoirs de police octroyés au Maire. Enfin, les CLSPD au sein de communes relevant de l'EPCI peuvent être maintenus (coexistence possible de CLSPD et CISPD).
Il convient de prendre en compte ce nouvel environnement de la gouvernance de la prévention de la délinquance afin d'en saisir les opportunités : un Centre de supervision urbain (CSU) peut ainsi être mutualisé au niveau intercommunal, gage d'une efficacité accrue pour de petites et moyennes communes en particulier.

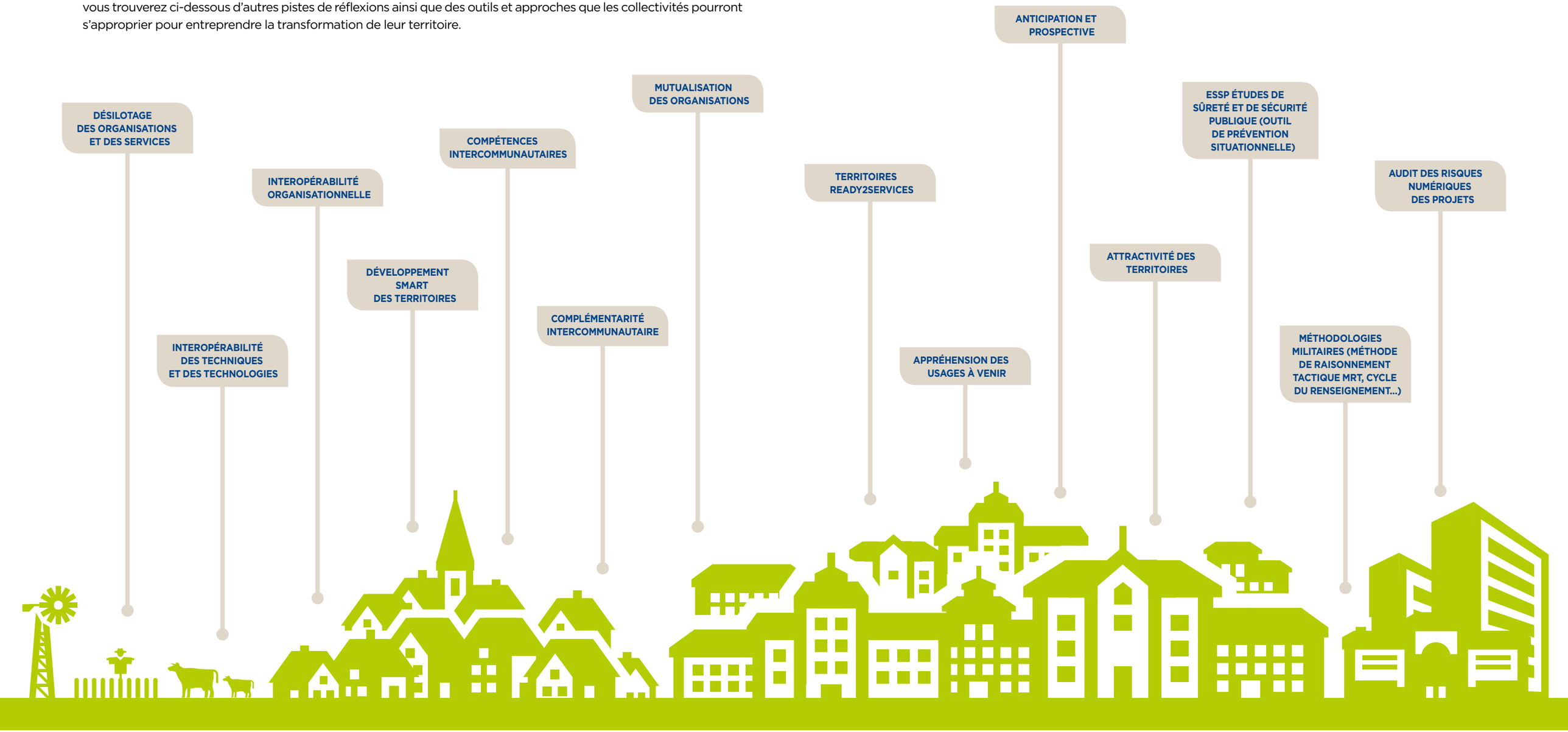
QUE DIT LE RAPPORT FAUVERGUE-THOUROT SUR LE SUJET DE LA VIDÉOPROTECTION ?

Dans son guide *PIXEL 2020*, notre partenaire AN2V (Association Nationale de la Vidéoprotection) défend quelques propositions destinées à faire bouger les lignes, comme notamment :
– élaborer des schémas départementaux de vidéoprotection (proposition 6) ;
– autoriser les bailleurs à mettre en place des systèmes de vidéosurveillance aux abords immédiats des immeubles (proposition 12) ;
– autoriser les communes à utiliser les lecteurs automatisés de plaques d'immatriculations (proposition 36).

Guide PIXEL 2020

AUTRES CONCEPTS & MÉTHODOLOGIES À APPRÉHENDER ET À INTÉGRER DANS LES DÉMARCHES DE CONSTRUCTION D'UN TERRITOIRE DE CONFIANCE ET DE SÉCURITÉ

Au-delà de l'approche temporelle et de la question de la gouvernance appréhendées dans les pages précédentes, vous trouverez ci-dessous d'autres pistes de réflexions ainsi que des outils et approches que les collectivités pourront s'approprier pour entreprendre la transformation de leur territoire.



MAÎTRISE DES RISQUES

PRINCIPE D'APPROCHE PAR L'ANALYSE DES BESOINS ET DES RISQUES

UNE APPROCHE PRAGMATIQUE

La nature protéiforme des services attendus, la multiplicité des solutions techniques susceptibles d'y répondre et leur inexorable obsolescence sont des écueils pouvant freiner les investissements d'une collectivité.

Une approche pragmatique peut cependant fournir des outils d'analyse favorisant la prise de décision et la conduite des projets sur une trajectoire vertueuse.
Il s'agit de trouver les solutions techniques en étudiant les besoins par le prisme d'une analyse des risques. Le préalable à cette analyse des risques est la qualification du besoin et la détermination du champ des usages afférents. Ensuite, une architecture de solutions émergera du berceau des technologies disponibles.

Je vise un effet à obtenir auprès d'une cible précise !

Quel est le besoin ?

Je mesure l'impact sur les services de la collectivité !

Quels sont les usages qui seront améliorés par la satisfaction du besoin ?

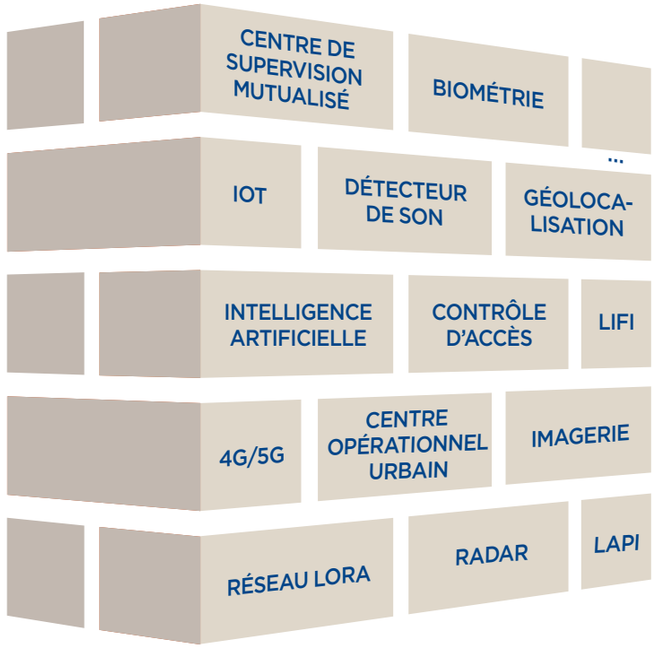
Je détermine à quels risques je réponds !

Quels sont les risques auxquels répondra le déploiement d'une solution ?

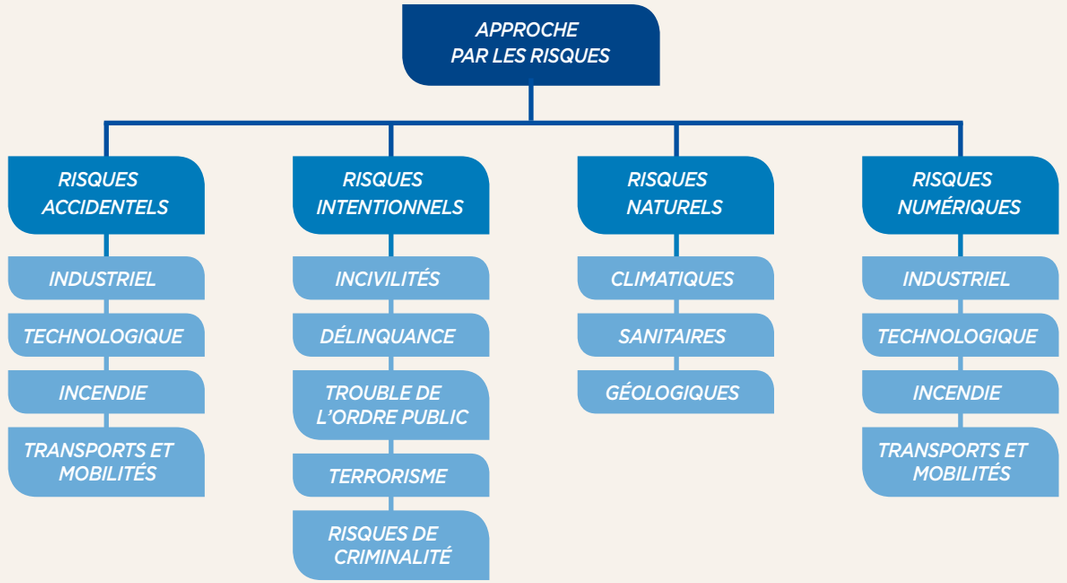
Je pense une architecture inclusive !

Quelles sont les technologies offrant un niveau de réponse ?

UN BERCEAU DE BRIQUES TECHNOLOGIQUES POUR APPORTER DES RÉPONSES AUX BESOINS ET AUX RISQUES



EXEMPLE DE MAPPING DES RISQUES



ÉTUDE À TRAVERS QUATRE CAS D'USAGES

PRÉSENTATION DES CAS D'USAGES

Dans les pages suivantes, nous proposons d'appréhender l'approche technique de la Safe City à travers l'étude des quatre cas d'usages suivants :
- éclairage public intelligent ;
- vidéoprotection intelligente ;
- mobilité intelligente ;
- bâtiment public intelligent.

Pour chacun des cas d'usage, un exemple concret d'application par une collectivité est présenté

MÉTHODOLOGIE DE L'ÉTUDE

L'approche par l'analyse des risques que nous proposons se penche sur la recherche pour chaque cas d'usage des thématiques suivantes :
- l'analyse de la prévention des **risques accidentels** : quels risques de nature accidentelle identifiés peuvent-ils être appréhendés et traités à travers la solution intelligente étudiée ?

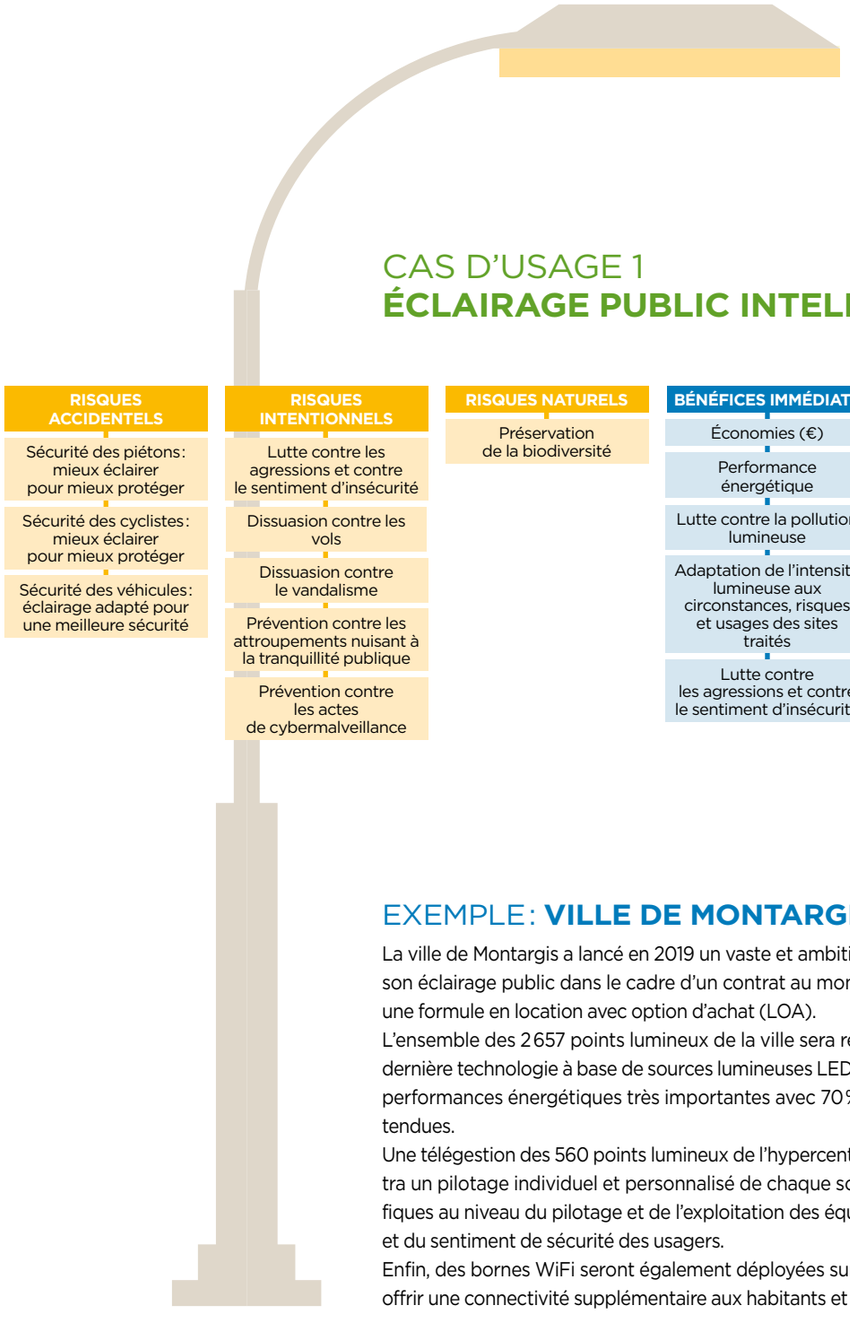
- l'analyse de la prévention des **risques intentionnels** : quels risques de nature intentionnelle identifiés peuvent-ils être appréhendés et traités à travers la solution intelligente étudiée ?

- l'analyse de la prévention des **risques naturels** : quels risques de nature naturelle identifiés peuvent-ils être appréhendés et traités à travers la solution intelligente étudiée ?

- les **bénéfices immédiats** : quels gains directs et immédiats la collectivité peut-elle trouver dans le déploiement de la solution intelligente étudiée ?

- les **solutions** et **technologies possibles** : quelles offres peuvent concrètement être déployées sur site ? À travers les solutions proposées, quelles technologies sont-elles mises en œuvre ?

En complément, chaque solution doit faire l'objet d'une étude de l'acceptabilité par le public et le cas échéant d'une communication adaptée.



CAS D'USAGE 1
ÉCLAIRAGE PUBLIC INTELLIGENT

RISQUES ACCIDENTELS
- Sécurité des piétons : mieux éclairer pour mieux protéger
- Sécurité des cyclistes : mieux éclairer pour mieux protéger
- Sécurité des véhicules : éclairage adapté pour une meilleure sécurité

RISQUES INTENTIONNELS
- Lutte contre les agressions et contre le sentiment d'insécurité
- Dissuasion contre les vols
- Dissuasion contre le vandalisme
- Prévention contre les attroupements nuisant à la tranquillité publique
- Prévention contre les actes de cybermalveillance

RISQUES NATURELS
- Préservation de la biodiversité

BÉNÉFICES IMMÉDIATS
- Économies (€)
- Performance énergétique
- Lutte contre la pollution lumineuse
- Adaptation de l'intensité lumineuse aux circonstances, risques et usages des sites traités
- Lutte contre les agressions et contre le sentiment d'insécurité

SOLUTIONS & TECHNOLOGIES POSSIBLES
- Sources LED
- Détection de présence
- Télégestion des points lumineux
- Abaissement/ augmentation de puissance
- Alimentation électrique de services connexes (caméras, capteurs…)
- Connectivité (WiFi, LiFi, IoT…)
- Intelligence artificielle
- Centre opérationnel urbain de pilotage

EXEMPLE : **VILLE DE MONTARGIS (45)**

La ville de Montargis a lancé en 2019 un vaste et ambitieux projet de rénovation de son éclairage public dans le cadre d'un contrat au montage financier reposant sur une formule en location avec option d'achat (LOA).
L'ensemble des 2 657 points lumineux de la ville sera rénové par des luminaires de dernière technologie à base de sources lumineuses LED, permettant d'atteindre des performances énergétiques très importantes avec 70 % d'économies d'énergie attendues.
Une télégestion des 560 points lumineux de l'hypercentre sera déployée et permettra un pilotage individuel et personnalisé de chaque source, avec des effets bénéfiques au niveau du pilotage et de l'exploitation des équipements, du confort visuel et du sentiment de sécurité des usagers.
Enfin, des bornes WiFi seront également déployées sur cinq mâts d'éclairage pour offrir une connectivité supplémentaire aux habitants et aux visiteurs occasionnels.

CAS D'USAGE 2
VIDÉOPROTECTION INTELLIGENTE

RISQUES ACCIDENTELS
- Détection d'accident de personne
- Détection d'accident routier
- Détection de mouvement de foule
- Protection de risques industriels
- Détection d'incendie

RISQUES INTENTIONNELS
- Prévention des atteintes aux personnes
- Prévention des atteintes aux biens
- Protection de zones utilisées par des publics sensibles
- Détection de dépôt d'objets
- Prévention des incivilités (dépôt sauvages, vandalisme, dégradations…)
- Prévention contre les actes de cybermalveillance

RISQUES NATURELS
- Surveillance des crues
- Surveillance des incendies de forêts

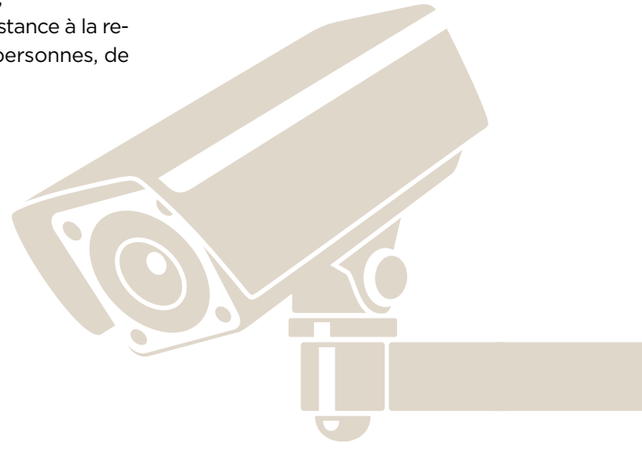
BÉNÉFICES IMMÉDIATS
- Augmentation du sentiment de sécurité
- Dissuasion
- Efficacité des investigations
- Protection de bâtiments et zones sensibles
- Pilotage des interventions de Police/ Gendarmerie
- Régulation du trafic routier
- Contrôle des zones à faible émission

SOLUTIONS & TECHNOLOGIES POSSIBLES
- Captation des anomalies sonores
- Vidéo-analytique (intelligence artificielle)
- Protection périmétrique, contrôle d'accès
- LAPI (Lecture automatique de plaque d'immatriculation) et VPI (Visualisation de plaque d'immatriculation
- Centre de supervision urbain (CSU) ergonomique
- Centre opérationnel urbain multiservices (VPU, Bornes, EP, Trafic…)

EXEMPLE : **VILLE DE CHAMBÉRY (73)**

La ville de Chambéry s'est équipée d'un dispositif de vidéoprotection urbain constitué de caméras fixes et mobiles et d'un centre de supervision urbain ergonomique et performant.

Les technologies déployées sont :
- caméras haute définition de dernières générations ;
- liens de transmission sécurisés ;
- vidéoverbalisation des infractions routières et des incivilités ;
- intégration progressive de l'intelligence artificielle pour assistance à la recherche et analyse dans l'image d'objets, de véhicules, de personnes, de comportements et d'intrusion ;
- postes d'exploitation ergonomiques ;
- mur d'image grands écrans à bords fins avec rétroéclairage.



CAS D'USAGE 3
MOBILITÉ INTELLIGENTE

RISQUES ACCIDENTELS	RISQUES INTENTIONNELS	RISQUES NATURELS	BÉNÉFICES IMMÉDIATS	SOLUTIONS & TECHNOLOGIES POSSIBLES
Prévention des risques routiers	Attaque avec véhicule bélier	Mobilité décarbonnée	Désengorgement des villes (optimisation des stationnements)	Mobilité électrique
Téléphone au volant	Prévention contre les actes de cybermalveillance	Réduction des déplacements générant des rejets de gaz à effet de serre	Fluidification des axes de circulation	Parking intelligent
Conduites addictives			Partage des espaces publics	Covoiturage et auto partage
Excès de vitesse			Sécurisation des déplacements et des temps de parcours	Mobilité douce
Franchissements			Intégration accessibilité PMR	Information usagers
Prise en compte des conditions météorologiques				Route connectée
				Véhicule autonome
				Radars (vitesses, feux, pédagogiques)
				Vidéosurveillance info trafic
				Régulation de trafic
				Lecture de plaques d'immatriculation
				Détection Automatique d'Anormalités
				Détection de présence de véhicules
				Données flottantes

EXEMPLE : **LE RÉSEAU EBORN POUR LA RECHARGE DE VÉHICULES ÉLECTRIQUES** (AUVERGNE-RHÔNE-ALPES ET PACA)

Ce réseau de 700 bornes de recharge pour la mobilité électrique propose sur cinq départements du sud-est de la France des services de localisation et de réservation de points de charge, de paiement et de gestion et de suivi de comptes abonnés.
Le réseau Eborn a délivré plus de 47 000 recharges (juillet 2019), soient 2,8 millions de kilomètres parcourus et 460 tonnes de CO^2 économisées.

Les technologies déployées sont :
- géolocalisation (bornes, véhicules) ;
- paiement électronique dématérialisé ;
- détection d'occupation et réservation de places ;
- calcul de temps de parcours et de recharge ;
- informations usagers ;
- services connexes ;
- expérimentations smart grid et alimentations autonomes.

CAS D'USAGE 4
BÂTIMENT PUBLIC INTELLIGENT

RISQUES ACCIDENTELS	RISQUES INTENTIONNELS	RISQUES NATURELS	BÉNÉFICES IMMÉDIATS	SOLUTIONS & TECHNOLOGIES POSSIBLES
Sécurité des usagers (personnel, visiteurs, équipes d'intervention)	Attaques aux personnes (terrorisme…)	Dégâts des eaux	Augmentation de la valorisation du bien immobilier (asset management)	Contrôle d'accès
Alertes et efficacité des interventions des secours	Cambriolages	Zones sismiques	Sécurisation du site	Sécurité incendie
	Piratage informatiques, cyberattaques	Empreinte carbone du bâtiment	Performance organisationnelle et opérationnelle des équipes	Vidéoprotection
			Accueil et services au public visiteur	PC de sécurité
				Éclairage intelligent
				Réseaux de communications internes performants
				Géolocalisation indoor

EXEMPLE : **PHILHARMONIE DE PARIS (75)**

Établissement culturel principalement consacré à la musique symphonique, la Philharmonie de Paris a engagé en 2010 un vaste programme de construction d'une salle de concerts et d'espaces musicaux permettant d'offrir des offres culturelles et de loisirs améliorés tout en garantissant une sécurité accrue aux visiteurs, au personnel et aux œuvres.

De très nombreux dispositifs techniques modernes ont été déployés (contrôle d'accès, interphonie, sécurité incendie, dispositifs malvoyants et malentendants, vidéoprotection…) et permettent aujourd'hui à la Philharmonie de Paris d'agir sur la diminution de la pollution lumineuse, le développement de l'activité commerciale et touristique, la sécurisation des accès au site, la réduction de la facture énergétique et de l'empreinte carbone.

CADRE DE CONFIANCE NUMÉRIQUE

Analyse et recommandations écrites avec le soutien de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

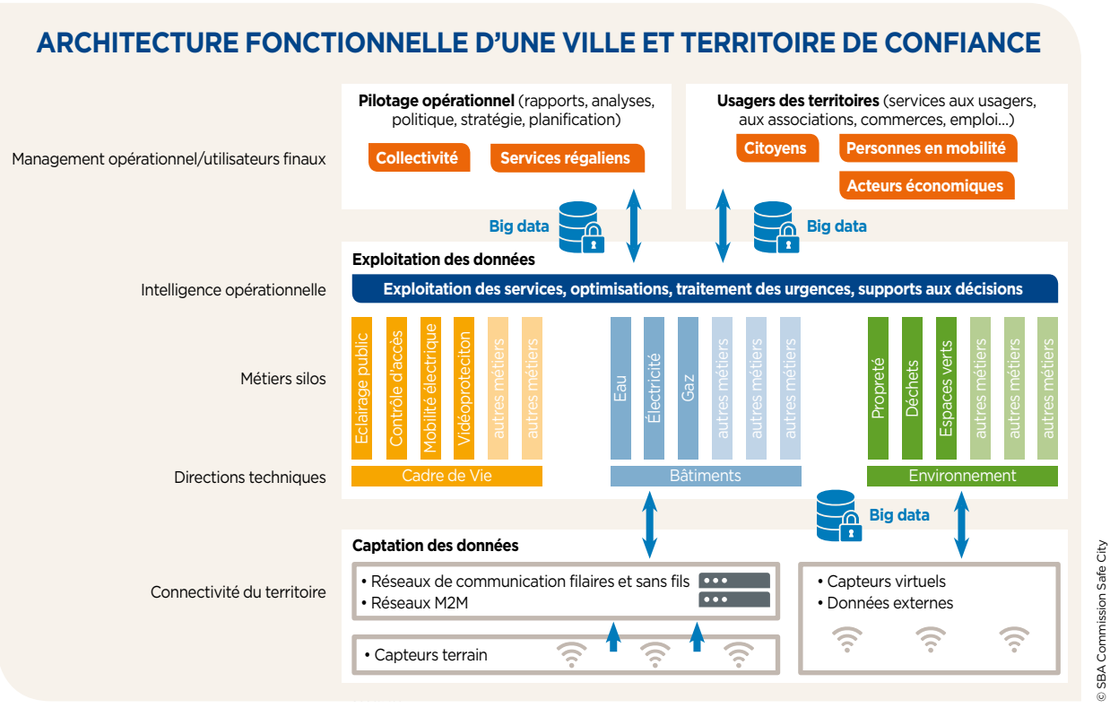
ENJEUX

Les enjeux liés au numérique sont multiples et complexes. S'ils sont porteurs de grandes opportunités - notamment économiques -, ils peuvent également être sources de risques, parfois difficiles à évaluer.
La difficulté d'appréhension de ces risques par les organisations réside notamment dans l'accroissement exponentiel de la surface d'exposition aux attaques. L'interconnexion des systèmes participe grandement à l'aggravation de ce risque comme l'illustre l'exemple de la voiture connectée où s'imbriquent plusieurs systèmes, tous interdépendants. Il en va de même pour certaines infrastructures dites critiques et parmi lesquelles on retrouve des opérateurs d'importance vitale (OIV), des points d'importance vitale (PIV) et des Opérateurs de services essentiels (OSE).

Le défi principal auquel sont confrontés les Villes et Territoires de Confiance est celui de la sécurisation de ces « systèmes de systèmes », alors même que les différentes parties prenantes peinent à garantir la sécurité des systèmes d'information pris unitairement.

L'incertitude demeure quant à la possibilité de « maîtriser » les risques numériques que drainent ces systèmes complexes et dont l'impact potentiel concerne désormais directement les équilibres économiques, la vie de la société et celle des citoyens.

ARCHITECTURE FONCTIONNELLE D'UNE VILLE ET TERRITOIRE DE CONFIANCE



© SBA Commission Safe City

MENACES ET RISQUES

ÉTAT DES LIEUX

Les motivations malveillantes auxquelles seront de plus en plus confrontées les Villes et Territoires de Confiance sur le plan numérique peuvent être différenciées en plusieurs catégories dont les effets potentiels peuvent varier de significatifs à catastrophiques :
- la cybercriminalité ;
- l'atteinte à l'image/la déstabilisation ;
- l'espionnage ;
- le sabotage.

Les menaces auxquelles font face les Villes et Territoires de Confiance sont de même nature que celles visant les systèmes d'information. Cependant, le contexte particulier des multiples interconnexions, de l'interopérabilité des systèmes et capteurs et de l'internet des objets (IoT), rend certaines de ces menaces plus prégnantes ou font peser un risque systémique sur l'ensemble des territoires connectés. Il peut s'agir :
- de prise de contrôle (de manière physique ou logique) d'installations publiques et/ou privées ;
- d'accès aux informations stockées ou échangées sur les serveurs ;
- de dysfonctionnement ;
- de manipulation ;
- d'atteinte à la vie privée.

RECOMMANDATIONS

L'approche rationnelle du cadre de confiance numérique est d'intégrer nativement la sécurité (*security by design*) à chaque nouveau projet Villes et Territoires de Confiance quelle qu'en soit l'échelle (application, équipement, bâtiment, blocs de bâtiments, zones/quartiers...). Cela passe notamment par l'application d'un ensemble de recommandations telles que :
- la désignation d'un référent sécurité numérique pour chaque projet ;
- l'intégration de la sécurité numérique sur l'ensemble du cycle de vie de chaque projet ;
- les principes de Maintien en conditions de sécurité (MCS) ;
- l'analyse des risques, par exemple, selon la méthode EBIOS Risk Manager ou la norme ISO 27005 ;
- le recours aux produits et services de confiance (voir le catalogue *Visas de sécurité* publié par l'ANSSI) ;
- la nécessaire sensibilisation/formation des différents utilisateurs, selon leurs profils ;
- l'application d'un processus de type « homologation de sécurité ».

EXEMPLES DE MENACES ET RISQUES

EXEMPLE 1

Menaces : atteinte à l'image, cybercriminalité - Signalement d'une compromission du site Internet d'une commune (source ANSSI, 2018)
En juin 2018, un particulier signale, par courriel, la compromission du site Internet d'une commune. Selon lui, des attaquants auraient installé des portes dérobées et téléchargé illégalement des fichiers sur le serveur. Une recherche effectuée par le CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques), indique effectivement la présence de fichiers et de pages Internet considérés comme malveillants. Contactée, la mairie confirme avoir reçu le signalement et pris attache avec son prestataire pour supprimer les fichiers en cause. Il est à noter que le site Internet de cette commune avait déjà été victime d'une défiguration en mai 2018. Ces éléments ont donc amené le CERT-FR à demander des précisions à la victime sur l'identification du vecteur de compromission et les actions de remédiation entreprises afin de réduire significativement le risque que survienne un nouvel incident.

EXEMPLE 2

La ville de Baltimore « prise en otage » par des cybercriminels (source : Le Point, 25 mai 2019).
Menaces : atteinte à l'image, cybercriminalité, sabotage - Conséquences : paralysie partielle des services municipaux, moindres rentrées fiscales, services administratifs perturbés.
Au printemps 2019, la ville de Baltimore (Maryland, États-Unis) est paralysée. Une attaque menée par des cybercriminels verrouille le système informatique municipal, raconte Radio Canada. Au total, près de 10 000

ordinateurs sont touchés. Malgré à la pression, le maire de la ville du nord-est des États-Unis refuse toujours de payer la rançon demandée. Les pirates informatiques ont bloqué des ordinateurs de la ville grâce à des logiciels malveillants. L'attaque se serait produite le 7 mai dernier. À présent, pour débloquer la situation, les hackeurs exigent le versement d'une rançon de 13 bitcoins, soit environ 140 000 dollars. Comme le décrit Radio Canada, la ville peut également payer une rançon de 3 bitcoins (environ 32 000 dollars) pour débloquer chaque fichier. Le FBI mène l'enquête concernant l'identité des pirates informatiques, mais, pour le moment, aucune information n'a filtré. Le site Internet précise que si la municipalité refuse de céder, elle devra alors refonder l'ensemble de son système informatique. Un travail qui prendra plusieurs mois. Pour le moment, la ville a déconnecté l'ensemble des ordinateurs d'Internet afin d'éviter une propagation de ces virus. Cette panne géante affecte les citoyens de la ville qui ne peuvent plus payer certaines factures via la plateforme en ligne. Pour tenter de contourner la paralysie, la ville a dû mettre en place une alternative manuelle permettant aux habitants de continuer à remplir leurs documents administratifs.

EXEMPLE 3

Menace : cybercriminalité - Risques : paralysie du trafic, accidents de masse

En novembre 2016, des pirates informatiques ont attaqué le réseau des transports en commun de San Francisco. Si le trafic de la cité n'a pas été perturbé (échec de la tentative), on peut frémir à l'idée d'une prise de contrôle de la signalisation routière dans une métropole.

Documents de références

Cahier IP5 CNIL « La plateforme d'une ville »

Action territoriale ANSSI

Bonnes pratiques ANSSI

CADRE RÉGLEMENTAIRE ET JURIDIQUE SUR LA PROTECTION DES SYSTÈMES D'INFORMATION

En tant qu'autorité administrative ou collectivité, il est obligatoire de se conformer à un cadre législatif et réglementaire exigeant ayant pour objectif :

- **Le Référentiel général de sécurité**, RGS (2010) impose la sécurisation des systèmes d'information lors de la mise en œuvre d'un télé-service aux usagers ;
- **La Politique de sécurité des systèmes d'information**, PSSIE (2014) assure la gouvernance et la sensibilisation des acteurs ;
- **Le règlement eIDAS** (2014) vise à établir un socle commun pour les interactions électroniques sécurisées ;
- **La Loi de programmation militaire**, LPM (2014-2019) concerne la sécurisation des systèmes « d'importance vitale » ;
- **La Directive *Network and Information Systems***, NIS (2018) s'adresse aux opérateurs publics ou privés qui se sont vus notifiés comme Opérateurs de services essentiels.

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

[RÈGLEMENT N° 2016/679, ABROGEANT LA DIRECTIVE 95/46/CE]

Le règlement général sur la protection des données à caractère personnel, RGPD (2018) a pour objectif de renforcer la protection des données à caractère personnel au sein de l'Union Européenne. L'enjeu pour les porteurs de projet réside dans leur capacité à mettre en œuvre des services respectueux des droits des personnes, quelle que soit la complexité des systèmes. Il est de l'intérêt des porteurs de projets d'effectuer une analyse d'impact sur la vie privée (Privacy Impact Assessment), dès lors que la mise en œuvre du service engendre un risque élevé pour les droits et les libertés des personnes physiques (article 27 du RGPD).

Ces textes imposent plusieurs mesures générales :

- la définition des objectifs de sécurité ;
- la réalisation d'une analyse de risque ;
- l'homologation de sécurité du système d'information ;
- le suivi opérationnel de la sécurité du système d'information.

LA GOUVERNANCE DES DONNÉES, DES IDENTITÉS ET DES SYSTÈMES D'INFORMATION

La question de la gouvernance de la donnée est au cœur d'une stratégie cruciale pour la réussite d'un projet. Elle doit donc être appréhendée de manière globale et faisant partie intégrante des traitements numériques du projet. Parmi toutes les définitions que l'on peut donner à la notion de gouvernance des données, la plus consensuelle et technique que nous pouvons vous proposer vient du cabinet de conseil Baseline Consulting, qui indique que la gouvernance est « un processus de supervision et de décision qui permet de hiérarchiser les différents investissements, d'allouer les ressources adéquates et un pilotage par les résultats, tout ceci pour s'assurer que les données utilisées au sein des projets sont valorisées et répondent aux enjeux et aux objectifs de l'organisation ».

La gouvernance des données doit pouvoir classifier les acteurs comme suit :

– Le propriétaire des données : il possède l'autorité nécessaire pour créer, définir, maintenir le niveau de protection de la donnée, que celle-ci soit dans le projet définie comme d'ordre géographique, sécuritaire, sociétale, gestion technique ou de toute nature.

– Le gestionnaire des données : il n'est pas propriétaire des données et ne doit pas en avoir le contrôle absolu. Il peut assurer sous mandat contractuel précis, l'architecture des systèmes de collecte et d'analyse, effectuer la maintenabilité simple ou poussée jusqu'à la résilience du projet installé, s'assurer que le projet respecte les règles de l'art pour ce qui concerne la protection des données, comme de l'ensemble du système (réseau, matériels, logiciels…).

Le gestionnaire des données doit disposer d'une frontière contractuelle claire et d'une qualification, une certification dédiée, d'un agrément ou d'un label reconnu par le propriétaire, afin que tous les intervenants répondent sur la totalité de la chaine à la conformité sur la protection des données.

CONSEILS POUR ASSURER LE CADRE DE CONFIANCE NUMÉRIQUE DES PROJETS

– Mettre en œuvre un cadre de gouvernance sous la direction des autorités compétentes de l'état et des collectivités territoriales prenant en compte le risque cyber, et portant une clarification des rôles et responsabilités des acteurs projet.

– Réaliser une analyse de risques en identifiant prioritairement tous les actifs sensibles (matériels ou immatériels) et assurer une veille continue sur les menaces, failles et vulnérabilités techniques applicables ainsi que sur les menaces émergentes.

– Porter une réflexion sur la conception d'un socle technique d'infrastructure urbaine selon une approche holistique et qui devra être nativement sécurisée.

– Porter une réflexion sur la formalisation des futurs standards de sécurisation en fonction des technologies installées et de leur niveau de sensibilité. Formuler les exigences fonctionnelles et veiller à leur déclinaison technique dans le respect des standards en vigueur.

– Contractualiser les engagements des fournisseurs et prestataires en matière de cybersécurité.

– Garantir le maintien en condition de sécurité des services et infrastructures critiques comme de télémaintenance (maintenance prédictive) ou de contrôle physique (maintenance curative et corrective).

– Assurer une surveillance permanente optimale et tracée de toute activité suspecte et autres signaux faibles dans le respect de la législation en vigueur et de façon déontologique et faire remonter dans un délai de 72 h auprès de l'autorité compétente qu'est la CNIL.

– Mise en œuvre d'un plan de gestion de crise et de revues de sécurité périodiques.

– Établir un plan de continuité en adhésion avec les plans de gestion de crise pour chacun des services et infrastructures critiques déjà existant, planifier des tests de résilience réguliers pour en vérifier l'efficacité.

– Établir un plan de réponse à incident majeur toujours en correspondance avec les plans de gestion de crise de la collectivité, planifier des exercices de simulation réguliers à partir de scénarios préétablis pour en vérifier la pertinence.

– Sensibiliser régulièrement, tous les acteurs porteurs du projet et les usagers sur les règles élémentaires et les bonnes pratiques en matière de cybersécurité en s'appuyant sur un réseau de correspondants formés (référents sûreté de la Police ou de la Gendarmerie nationale par exemple).

– Faire réaliser des audits de sécurité externes par un tiers de confiance neutre.

– Piloter la mise en conformité des écarts identifiés en priorisant par criticité (penser à la nomination d'un DPO).

BUDGETS & MODÈLES CONTRACTUELS

RETOUR SUR INVESTISSEMENT (RSI)

RSI DIRECT : DÉFINITION

Le Retour sur investissement direct permet un bénéfice immédiat d'une action d'investissement.
Un premier bénéfice constaté est une économie directe liée à un effet de récurrence annuelle : tout gain obtenu sur un fonctionnement se répercutera tous les ans.
Un second bénéfice concerne l'optimisation des services qui pourra en être fait, soit par optimisation voire suppression des tâches associées, soit par réorganisation liée directement à l'usage fait de l'investissement.
Enfin, un troisième bénéfice peut résulter de la production de recettes liées à l'exploitation de l'investissement, au titre d'un nouveau service facturé à son utilisateur ou générant des économies.
Il est commun également de constater que les gains réalisés dans les coûts de fonctionnement permettent de dégager des capacités d'investissement dans la ville : l'inscription dans ce cercle vertueux permet de contribuer au financement du territoire de confiance et de sécurité.

Quelques exemples :
– vidéoverbalisation : recettes directes perçues par la commune (contre-sens, stationnements gênants, voies réservées, feux, stops…) ; de manière concrète, à l'aide d'un véhicule de vidéoverbalisation semi-automatique, une commune d'Île-de-France a réalisé 1 M € de recettes complémentaires ;
– une ville du centre de la France : coût d'assurance du parc de bâtiments de la ville diminué de 800 K €/an à 50 K €/an en dix ans, suite à une politique sécurité municipale de long terme plus forte et plus dynamique qui a fait chuter un grand nombre de vandalismes sur les bâtiments.

RSI INDIRECT : DÉFINITION

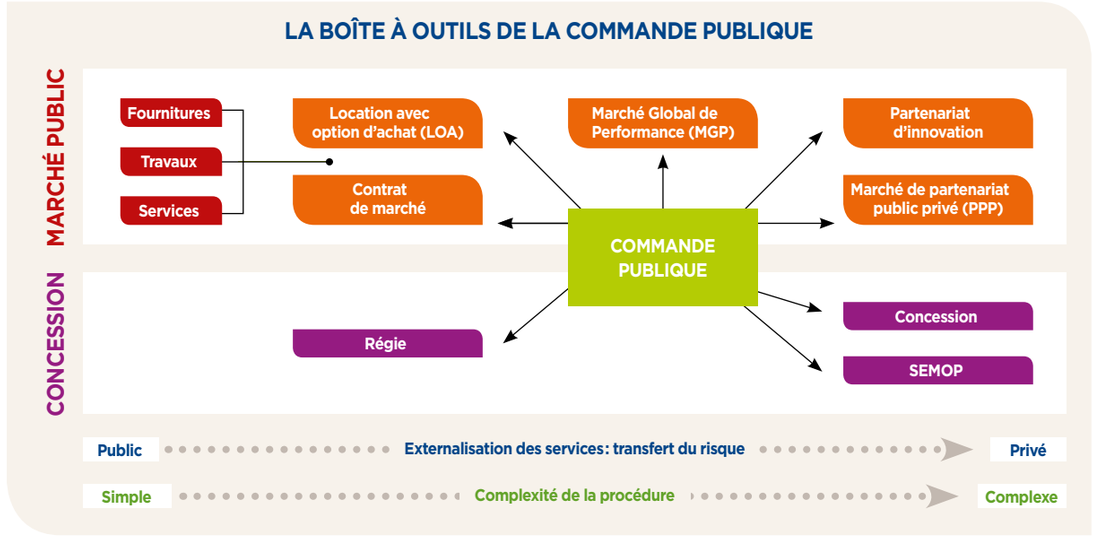
Le Retour sur investissement indirect permet un bénéfice dont on ne mesure pas immédiatement le gain, ou qui engendre un processus de transformation dans un domaine collatéral.

Parmi ces bénéfices, on peut trouver par exemple la notion d'attractivité qui est induite par la transformation de multiples actionneurs. Résultante d'actions combinées multiples, l'attractivité est influencée par tous les éléments de la chaîne de valeur sur un territoire et peut se retrouver renforcée (ou fragilisée !) par des investissements influençant directement ou indirectement le cadre de vie. Autres bénéfices possibles : tous les services générant des données partagées, ouvrant ainsi à d'autres développements, d'autres applications, d'autres fonctionnalités pour les usagers du territoire.
Quelques exemples :
– en Suisse : il est possible de faire financer des systèmes d'alerte des pompiers par les assurances, ces dernières y trouvant leur intérêt suite à la baisse des risques ;
– une ville du sud-ouest de la France : utilisation des images filmées par la vidéoprotection urbaine pour détecter la formation de flaques d'eau à proximité des arrosages automatiques de pelouse, exemple d'alerte par rapport au réseau de distribution d'eau potable.
– une déchetterie de nouvelle génération peut permettre un RSI à 6 mois pour :
• la lutte contre les vols de métaux ;
• le contrôle du poids des déchets ;
• l'optimisation de la rotation des bennes ;
• le respect des engagements contractuels avec les exploitants de déchetteries ;
• le développement de l'écoresponsabilité.

COMMENT FINANCER ?

CONSTRUIRE UN SCHÉMA DIRECTEUR

Pour développer un projet de Territoire de Confiance, il est nécessaire de construire un schéma directeur. À ce titre, il est impératif de déterminer au préalable une stratégie de sécurité, pour ensuite fixer le cap.
La construction pourra ensuite se faire selon plusieurs phases, par étapes, c'est-à-dire en réalisant des investissements successifs et complémentaires. Mais pour que cela se réalise en



harmonie, il est impératif d'avoir défini une vision globale au préalable.
C'est par cette approche par anticipation et planification de la cible à atteindre que se dégage une réelle capacité de retour sur investissement : les solutions développées pour construire une « Smart City » permettent d'en financer sa dimension « Safe ».

PISTES POUR L'INVESTISSEMENT

– La recherche de subventions : départementales, régionales, FIPD, DETR (fonds ruraux), dotation de soutien à l'investissement local (DSIL), dotation de solidarité en faveur de l'équipement des collectivités territoriales et de leurs groupements touchés par des événements climatiques ou géologiques, travaux divers d'intérêt local (TDIL)…

PISTES POUR LE FONCTIONNEMENT

– bien travailler le sujet de la maintenance ;
– être attentif à la portabilité et la réversibilité ;
– ressources humaines adaptées ;
– favoriser la mutualisation ;
– attention à la promesse des propositions « … As A Service » : bien mesurer les avantages et les inconvénients de chacune.
– La mutualisation : gains à trouver à travers le processus de réalisations mutualisées entre collectivités ou EPCI
– Une approche R2S Territoire (Territoire Ready2Service) inspirée des travaux de la SBA, notamment du point n° 9 (composante Smart) pour des projets conséquents ou à connotation centralisatrice.

POINTS DE VIGILANCE

« Quand c'est gratuit, c'est vous le produit »
Attention à la tentation du produit gratuit ou anormalement bas. Sans rejeter impérativement toutes ces propositions, il convient néanmoins de s'interroger sur le véritable modèle économique d'une proposition alléchante où l'investissement semble pris en charge par un tiers. Le gratuit peut cacher une stratégie qui fragilise les intérêts de l'utilisateur.

Attention à la problématique Cyber
Derrière une proposition gratuite ou pas chère, peut aussi se cacher une problématique de cybersécurité, intentionnelle ou non, malveillante.
Ça paraît moins cher, mais probablement parce qu'il y a une problématique cyber qui se cache derrière cette attractivité financière.

TRAVAUX **SBA**

Les transitions énergétiques, environnementales, technologiques, démographiques et urbaines constituent autant de défis que d'opportunités d'actions pour les acteurs des villes de demain. Ces enjeux font état de l'importance de développer des systèmes urbains intelligents qui permettront d'opérer en toute confiance le passage à la ville intelligente et durable.

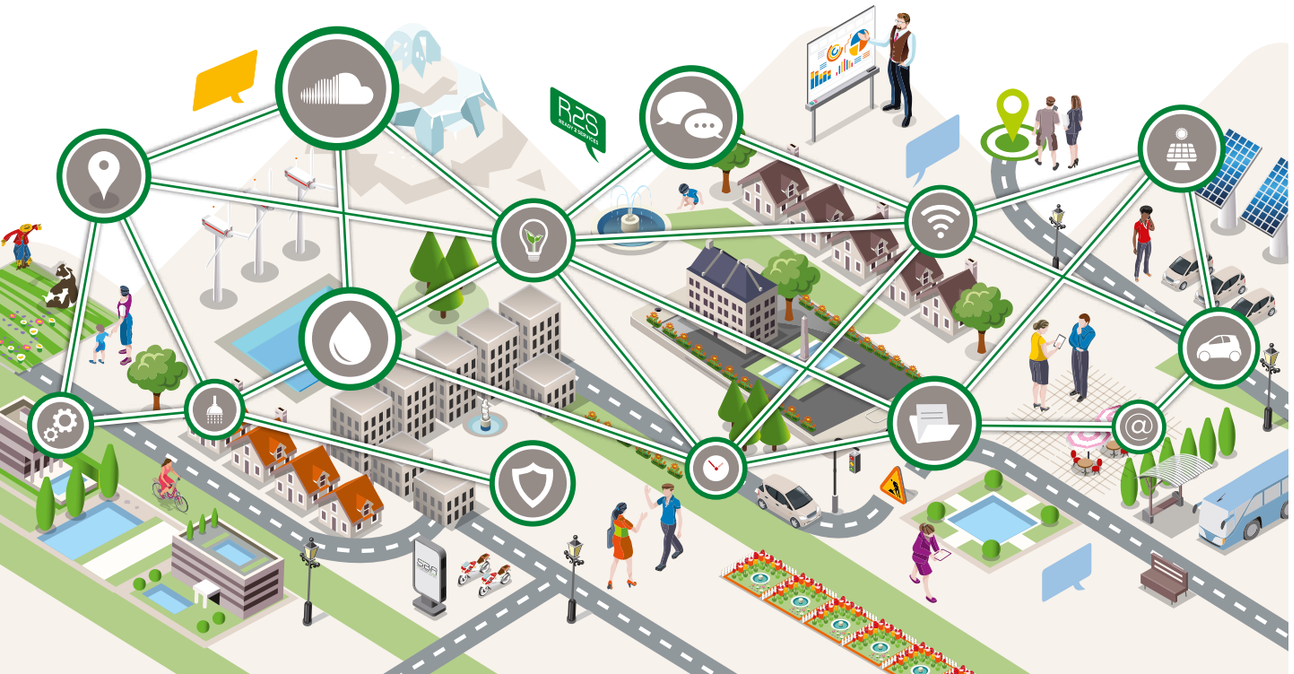
Créée en 2012, la SBA (Smart Buildings Alliance) est unique en son genre de par sa transversalité et la diversité de ses membres. Elle dépasse les approches traditionnelles en silo et fédère l'ensemble des corps de métiers liés au bâtiment et au territoire, elle réfléchit aux impacts sur le tissu urbain et ses usages des transitions environnementales et numériques, investigue de nouvelles voies et propose des solutions pour relever les défis de notre société à l'aune de ces deux transitions majeures.

Dans cette perspective la SBA bâtit des cadres de référence permettant d'accompagner la transformation des pratiques, améliorer l'efficience des projets, accroître l'attractivité des bâtiments et des territoires, en valorisant les services et développant les nouveaux usages. Le cadre de référence R2S (Ready2Services) étant le socle sur lequel repose cette démarche.

LE TERRITOIRE R2S

Partant du bâtiment R2S (Ready2Services), il est déclinable de l'échelle du bâtiment (tertiaire et résidentiel) à l'échelle des territoires. « Confrontés à de nombreux défis (économiques environnementaux, sociaux et sociétaux), les territoires sont contraints d'entrer en transition(s) ». Transition numérique mais, aussi, énergétique, c'est en alliant la puissance de ces deux transitions majeures que s'ouvre un formidable terrain de progrès et c'est là où se situe le cœur de l'action de la SBA.

L'approche R2S pour le territoire repose sur quatre grands axes répartis en douze principes comme explicités sur le schéma ci-contre.



12 POINTS CLÉS POUR BÂTIR UN TERRITOIRE « READY2SERVICES » : R2S

CITOYENNETÉ

1. Un territoire **par et pour le citoyen** : concertation et engagement citoyen au cœur du dispositif, e-administration simplifiée, réduction de la fracture numérique.

2. Un territoire **durable** : préservation des ressources, politique énergétique, réduction des pollutions.

3. Un territoire qui **protège les citoyens** : sécurité des espaces publics, protection des données personnelles, cybersécurité.

GOUVERNANCE

4. Une **stratégie territoriale numérique** : inscrite dans les plans et documents de programmation du territoire.

5. Une **gouvernance numérique** : inclusive des acteurs publics et parapublics, des entreprises et des citoyens.

6. Un territoire **transparent** dans sa gestion : partageant avec tous ses actions et ses résultats.

DONNÉES

7. Un **langage commun** : établissement de standards (esperanto numérique) pour que les données soient compréhensibles et utilisables par tous.

8. Généralisation du BIM et du CIM : des référentiels 3D, Building et City Information Modeling partagés.

9. Un **Iot Smart** dans chaque contrat public : exigence de publication des données aux standards territoriaux, nationaux ou internationaux contribuant aux référentiels 3D communs.

INFRASTRUCTURES

10. Un **territoire connecté** : réseaux télécom fixes et mobiles de qualité, déploiement du très haut débit, couverture d'un ou plusieurs réseaux IoT.

11. Des **infrastructures publiques R2S** : réseaux de transport Ready2Mobility as a Service ; réseaux d'eaux et d'énergies Ready2Grids (R2G).

12. Des **bâtiments publics R2S** : bâtiments R2S (Ready2Services) ouverts et connectés au territoire.

LA SBA ACCOMPAGNE LE SECTEUR DU BÂTIMENT POUR L'AIDER À ACCÉLÉRER SA MUTATION FACE AUX ÉVOLUTIONS LIÉES À L'ARRIVÉE EN MASSE DU NUMÉRIQUE DANS LE SMART BUILDING ET LA SMART CITY. ELLE PROPOSE UNE VISION GLOBALE S'APPUYANT SUR DES INFRASTRUCTURES MUTUALISÉES POUR LA PROMOTION DE NOUVEAUX SERVICES, AUTOUR DES USAGES, GÉNÉRATEURS D'EFFICIENCE ET D'UNE MEILLEURE COHÉSION SOCIALE.

Les actions de la SBA

RENCONTRES

Fédérer la filière dans un esprit de transversalité

Évènements SBA, pour le partage d'expérience et la veille autour des thématiques du bâtiment intelligent dans la ville durable.

PUBLICATIONS

Partager notre vision et nos recommandations

Manifeste du Bâtiment Intelligent pour des Territoires Durables. Guide du bâtiment et du territoire R2S (Ready2Services), e-SBA (news bimestrielle), Théma SBA Territoires, Logement social, Circulation dans la ville.

COMMISSIONS

Réflexions sur l'évolution du bâtiment dans la ville intelligente

Commissions «experts» pour définir un cadre commun pour des bâtiments connectés et ouverts.

RELATION INSTITUTIONS

Sensibiliser les décideurs publics

Ministères, institutions publiques, collectivités locales, syndicats professionnels...

COOPÉRATION INTERNATIONALE

Rayonner au-delà des frontières

Échanges avec les organisations internationales.

Devenez membre de la SBA au côté des leaders et experts du Smart Buildings et de la Smart City pour :

- En comprendre les enjeux et les défis
- Participer à la définition et la mise en place des socles référentiels
- Vous informer et suivre les innovations du secteur
- Développer votre réseau et échanger avec vos pairs
- Rencontrer des experts des métiers connexes au vôtre

LA SMART BUILDINGS ALLIANCE EST FAITE POUR VOUS, CONTACTEZ-NOUS :
CONTACT@SMARTBUILDINGSALLIANCE.ORG

WWW.SMARTBUILDINGSALLIANCE.ORG

LES MEMBRES

ABB ● ACCENTA ● ACCOR INVEST ● ACOME ● ACR ● ACS2I ● ACTIWATT ● ADEUNIS RF ● ADISCOM ● AFPA-TOULOUSE ● AIRELIOR FACILITY MANAGEMENT ● AIRRIA ● ALACAZA ● ALCANTE ● ALGECO ● ALLIANZ REAL ESTATE FRANCE ● ALPHA RLH ● ALTAREA COGEDIM ● ALTECON ● ALTERNET ● AN2V ● ANITEC ● APAVE SUDEUROPE ● APILOG AUTOMATION ● APOGEE ● ARC INFORMATIQUE ● ARCHIMEN ● ARCOM ● ARISTOTE ● ARKHENSPACES ● ARP ASTRANCE ● ARTELIA ● ARTETRIS ● ARXIT ● ASCAUDIT ● ASSOCIATION FRANCAISE DE L'ECLAIRAGE ● ASSOCIATION HQE ● ASSOCIATION PROJET LORIAS ● ASSUR & SENS ● ASSYSTEM ● ATC FRANCE ● AURI ZONE ● AUTOMATION BUILDING INTELLIGENCE ● AUTOMATIQUE ET INDUSTRIE ● AVELTYS ● AXIANS ● AXXONE SYSTEM ● AZUR SOFT ● B.tib ● BAALBEK MANAGEMENT ● BACNET FRANCE ● BARBANEL ● BCM ENERGY ● BEEBRYTE ● BET DELTA ● BG INGENIEURS CONSEILS ● BIA ● BIRDZ ● BNP PARIBAS REAL ESTATE ● BORDEAUX METROPOLE ● BOUYGUES CONSTRUCTION ● BOUYGUES ENERGIES & SERVICES ● BOUYGUES IMMOBILIER ● BOUYGUES TELECOM ENTREPRISES ● CABA ● CAE GROUPE ● CAILLOU VERT CONSEIL ● CAPENERGIES ● CCF ● CCI NICE COTE D'AZUR ● CDU IMMOBILIER ● CELEC ● CERTIVEA ● CIDECO ● CINOV ● CISCO ● CIT RED ● CLUSTER HBI ● CMT ● CNAM ● CNOA ● CONNEK+ CONSEIL ● CONSEIL DE DEVELOPPEMENT METROPOLE DE LYON ● COSTIC ● COTHERM ● COVIVIO ● CR SYSTEM ● CSTB ● CUST'HOME ● CYMBI.O ● CYRISEA ● DALKIA ● GROUPE EDF ● DALKIA SMART BUILDING ● DASSAULT SYSTEMES ● DATA SOLUCE ● DECAYEUX ● DECELECT ● DEERNS FRANCE ● DELTA DORE ● DEMATHIEU & BARD ● DIS INGENIERIE ● DISRUPTIVES TECHNOLOGIES RESEARCH ● DISTECH CONTROLS ● DOVOP DEVELOPPEMENT ● ECONOCOM ● EDF ● EFFICACITY ● EFFIPILOT ● eG4U ● EGF BTP ● EGIS CONSEIL BATIMENTS ● EIFFAGE ENERGIE ● ELICHENS ● ELITHIS ● EMBIX ● EN ACT ARCHITECTURE ● ENERBEE ● ENERGIE IP ● ENERGISME ● E'NERGYS ● ENGIE AXIMA ● ENGIE INEO ● ENLESS WIRELESS ● ENLIGHTED ● ENOCEAN ● ENSI POITIERS ● EUROPEAN SLEEP CENTER ● F2A SYSTEMES ● FAYAT ENERGIE SERVICES ● FEDENE ● FFDomotique ● FFIE ● FIFTHPLAY ● FLOW ● FORMAPELEC ● FSIF ● GA SMART BUILDING ● GA2B ● GADS ● GARCIA INGENIERIE ● GBMP ● GCC ● GETEO ● GETRALINE ● GIESPER ● GIZMO ● GLI ● GROUPE EKIUM ● GRAND PARIS HABITAT ● GRDF ● GREENFLEX ● GROUPE BETOM ● IDEAM SOLUTIONS ● GROUPE VIVALYS ● HABITAT76 ● HAGER ● HAVR ● HBF ● HENT CONSULTING ● HERVE THERMIQUE ● HESTIA INNOV ● HONEYWELL ● HSBC ● HXPERIENCE ● HYDRELIS ● IBM ● ICADE ● ICONICS ● IDEX ● IDTIQUE ● ILOGS FRANCE ● IMMOBILIERE 3F ● IMPERIHOME ● INGEROP ● INGETEL BET ● INNOVATION PLASTURGIE COMPOSITES ● INSITEO ● INTENT TECHNOLOGIES ● IPORTA ● ISTA ● JIP CORPORATION ● JOOXTER ● JVD ● KALIMA DB ● KARDHAM CONNECT ● KEO FLUIDES ● KEYCLIC ● KIPSUM ● KLDOM ● KNX FRANCE ● KOONTOO ● KORUS ● LD EXPERTISE ● LE RÉSIDENTIEL NUMÉRIQUE ● LED LEASE FINANCE ● LEGRAND ● LEON GROSSE ● LES COMPAGNONS DU DEVOIR ● LEXCITY ● L'IMMOBILIERE IDF ● LITED ● LM INGENIERIE ● LOGISTA HOMETECH ● LONMARK FRANCE ● LUTRON ELECTRONICS ● LUXENDI ● LVMH MOET HENNESSY ● LYNRED ● MARSH ● MBA INGENIERIE ● MCS SOLUTIONS ● MEANWHILE ● MEDIACONSTRUCT ● MICROSENS ● MIOS ● MOFFI ● MONBUILDING ● MOZAIQ ● NEOBUILD ● NETISSE ● NETSEENERGY ● NETSYSTEM ● NEXITY ● NOBATEK ● NODON ● OCCITALINE ● OGGA ● OKEENEA DIGITAL ● ONEPOINT ● OPENFIELD ● OPNA ● ORANGE ● OTI FRANCE ● OVERKIZ ● OZE ENERGIES ● PARKING MAP ● PARTAGER LA VILLE ● PICHET ● PLACE DES ENERGIES ● PLAN BATIMENT DURABLE ● POLE FIBRES ● ENERGIVIE ● POLE TES ● POLESTAR ● POSTE IMMO ● PREMIUM CONSEIL ● PRESTANTENNES ● PRESTATERRE ● PRIVA ● PROLOGIS ● PROMOTELEC SERVICES ● PROXISERVE ● PULS ● QARNOT COMPUTING ● QOS SOLUTIONS ● QUALICONSULT ● QUALITEL ● QUANIM ● QUINTEA ● RABOT DUTILLEUL ● NACARAT ● REALITES HUB 5 ● RELAIS D'ENTREPRISES ● RESO ● RESOLVING ● REXEL ● ROBEAU ● S2E2 ● S2T INGENIERIE ● SAINT GOBAIN ● SAS MEDISAT ● SAUTER REGULATION SAS ● SCHNEIDER ELECTRIC ● SE3M ● SELUO ● SEMTECH ● SENSINOV ● SERCE ● SERELEC ● SETEC BATIMENT ● SFEL ● SFR ● SIA PARTNERS ● SIBCO ● SIEL 42 ● SIEMENS ● SIGNIFY ● SIRLAN ● SISA FRANCE ● SLAT ● SMART USE ● SMARTENON ● SMARTHAB ● SMARTHOME FRANCE ● SNACG ● SNEF Connect ● SOCOMEC ● SOMFY ● SONY ● SPIE ● SPIE BATIGNOLLES ● SPINALCOM ● SPL LYON CONFLUENCE ● SUPPLINNOV ● SXD ● SYLFEN ● SYNTEC INGENIERIE ● SYPEMI ● SYSELIA ● SYSTECHMAR ● TACTIS ● TECHNAL ● TECHNILOG ● TECXTEAM ● TEVOLYS ● THYSSENKRUPP ASCENSEURS ● TRACTEBEL ● TRIDONIC ● TRIO2SYS ● TT GEOMETRES EXPERTS ● UBIANT ● UNIBAIL-RODAMCO ● UNIGRID SOLUTIONS ● UNIVERSITE DE RENNES 1 ● URBAN PRACTICES ● URMET FRANCE ● VALLOGIS ● VERTBATIM ● VERTUOZ by ENGIE ● VILOGIA ● VINCI ENERGIES France ● VINCI FACILITIES ● VISIOGLOBE ● VIVERIES TECHNOLOGIES ● WAGO ● WAVESTONE ● WICONA ● WISEBIM ● WIT ● WITTI ● WORKTOO ● WSP FRANCE ● Wx ● YNCREA HAUTS DE FRANCE ● YOUSE ● Z#BRE ● ZEPLUG

LES MEMBRES **D'HONNEUR DE LA SBA**

Prix public 19 €
ISBN 978-2-95601-757-8
9 782956 017578

www.smartbuildingsalliance.org

SBA
SMART BUILDINGS ALLIANCE
FOR SMART CITIES