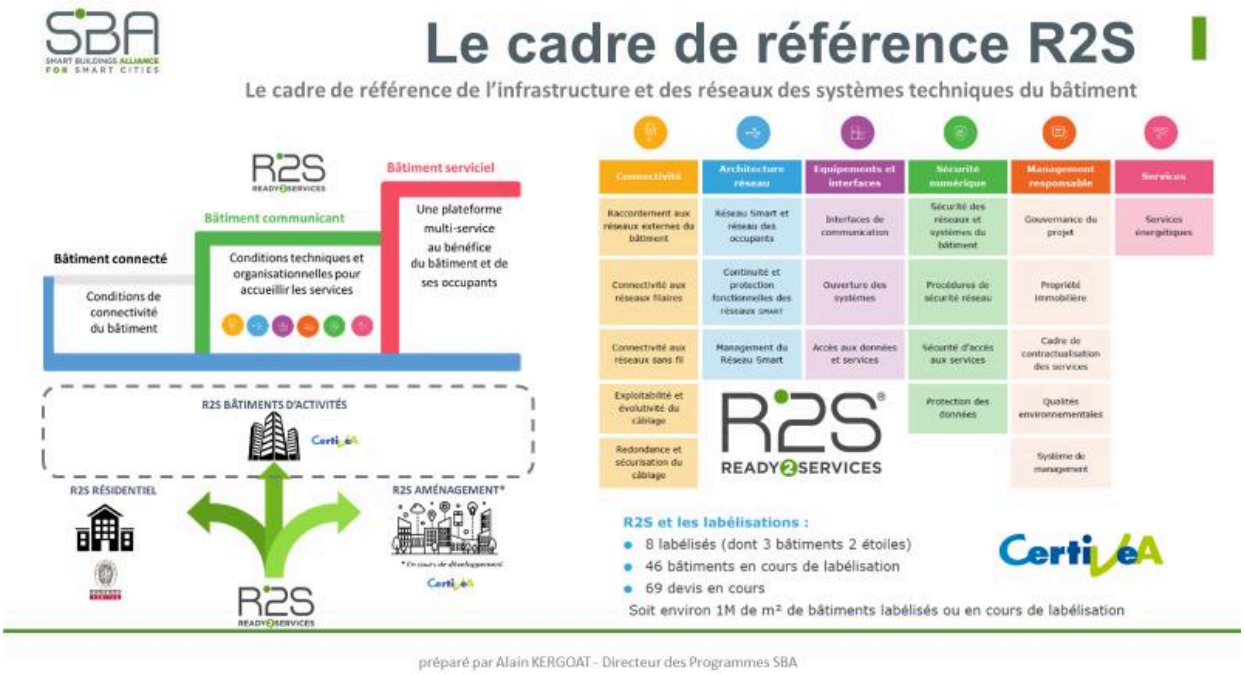
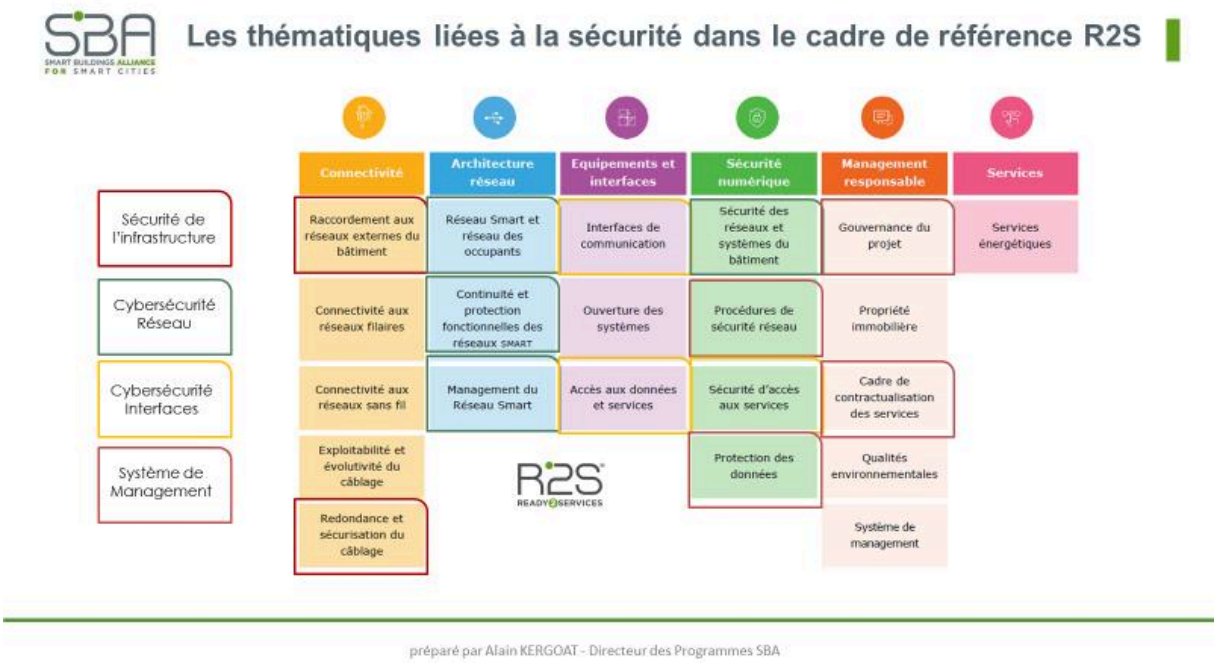
Compte Rendu de la réunion du mardi 10 novembre 2020

Participants:

Virgile Auge	AN2V
Dominique Legrand	AN2V
Nathalie Labeys	CNPP
Nesrine Mokrani	Engie
Gilles Courtes	Engie Solutions
Noémie Douénat	Ingetel
Pascal Zerates	Khardam
Solenne Lefranc	Orange
Ronan McFarlane	SIA Partners
Jean Christophe Denis	Wallix
Didier Cohen	Wallix
Henri Morawes	
Emmanuel François	SBA
Patrice de Carné	SBA
Alain Kergoat	SBA

Après un tour de table et la présentation des participants, la démarche R2S a été resituée. R2S constitue en effet un socle sur lequel une approche plus spécifique de la cybersécurité pourrait s'appuyer. Il a été rappelé que R2S lancé en juin 2018 par Certivea dans sa version destinée aux bâtiments d'activité, que ce soit en développement neuf ou en rénovation-réhabilitation, posait déjà les bases d'un certain nombre de thématiques liées aux questions de cybersécurité.





A titre indicatif ci-dessous une liste des critères existant dans R2S et qui peuvent être liés à la cybersécurité

Critères Cybersécurité R2S	Critères
Sécurité de l'infrastructure	5
CO1.1 Prédisposition du bâtiment au rattachement à tout type de liaison filaire externe	
CO1.2 Redondance de rattachement du bâtiment à tout type de liaison filaire externe	
CO5.1 Capacité de redondance des câblages du bâtiment	
CO5.2 Alimentation électrique de l'infrastructure	
CO5.3 Contrôle des accès et protection des infrastructures	
Sécurité Réseau	10
RE1.1 Réseau Smart dédié aux services généraux du bâtiment	
RE2.1 Capacité de résilience du Réseau Smart du bâtiment	
RE2.2 Détection d'anomalies et protection du Réseau Smart	
RE3.1 Administration des réseaux et de leurs équipements	
SN1.1 Mécanismes d'authentification d'accès au Réseau Smart	
SN1.2 Mécanismes de routage conditionnel du Réseau Smart	
SN1.3 Support des VLAN	
SN1.4 Mécanismes de surveillance des trafics et de protection contre les logiciels malveillants	
SN1.5 Chiffrement des communications	
SN2.1 Suivi des flux et des configurations du Réseau Smart	
Sécurité des Interfaces	3
IN1.1 Intégration des équipements au Réseau Smart du bâtiment	
IN3.3 Stabilité des services	
SN3.1 Sécurisation de l'accès aux applications	
API Terrain (R2S Connect)	
API Centrale (R2S Connect)	
Système de Management de la Sécurité	6
MA1.2 Administration du Réseau Smart	
MA3.1 Contrats de services (SLA) avec les fournisseurs	
SN2.2 Traitement des incidents et chaîne d'alerte	
SN2.3 Mises à jour logicielles des équipements	
SN3.2 Prévention et gestion des risques	
SN4.1 Conformité au Règlement Général sur la Protection des Données	

Un premier travail de la commission R2S-Cybersécurité pourrait consister à faire une première relecture de ces critères afin de valider le fait qu'ils correspondent au niveau d'attente en matière de cybersécurité, et les compléter si besoin.

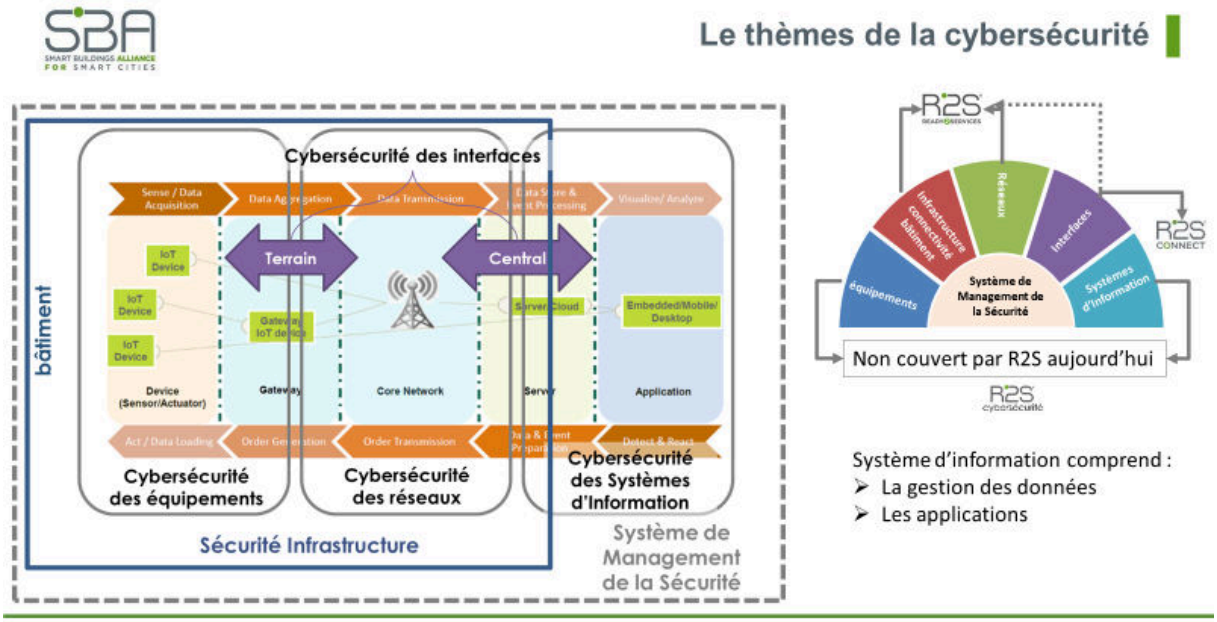
Parmi les premières pistes discutées :

Sur la Cybersécurité réseaux :
- Switches
- Câblages …

La liste semble bonne mais attention de bien intégrer les switches physiques et virtuels

Sur la sécurité d'accès des équipements
- Sécurisation des IoT : investiguer l'initiative IPBLIS
- Question du chiffrement des communications de bout en bout => parfois compliqué sur certains équipements ne disposant de la puissance de traitement nécessaire

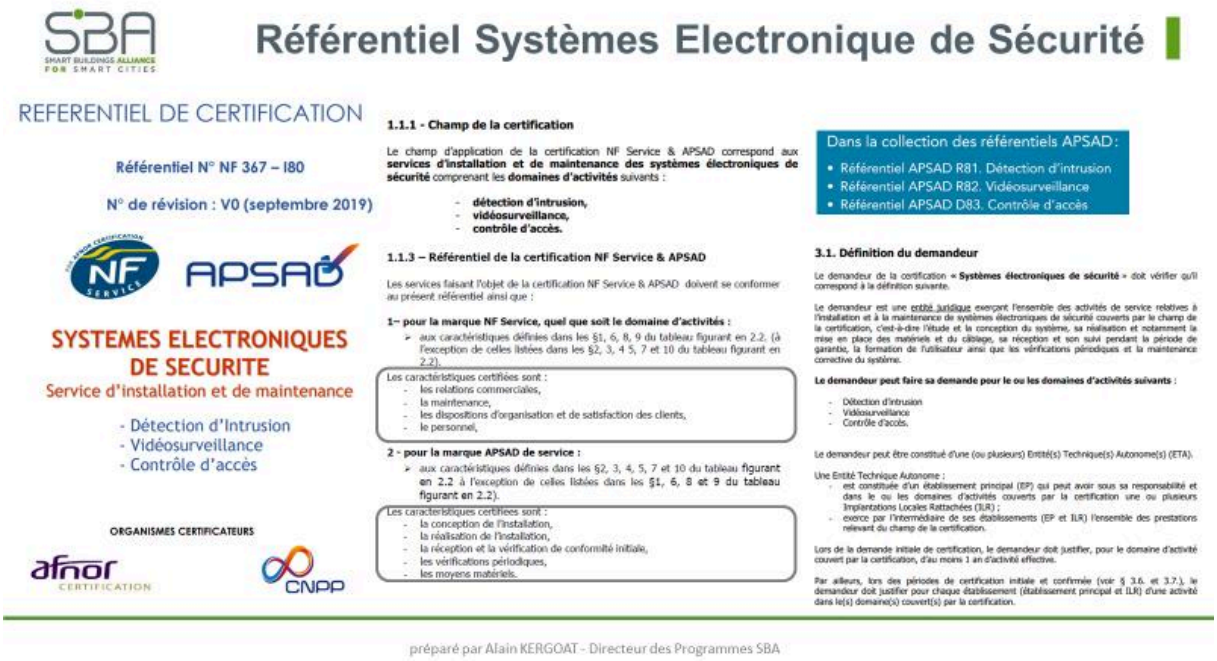
Au-delà de ce 1er travail de révision du cadre existant, il semble acquis, qu'en l'état actuel le cadre de référence R2S ne couvre pas l'ensemble des thématiques attendues d'une approche complète de la cybersécurité. En effet on peut considérer qu'une approche de la cybersécurité doit couvrir à minima les 6 thèmes suivants : les équipements – les infrastructure de connectivité – le réseaux – les interfaces – le système d'information – le système de management. Or 2 de ces thèmes : les équipements – le système d'information ne sont pas du tout couvert actuellement dans R2S, et d'autres doivent certainement être renforcés : Interfaces – Système de management de la sécurité notamment.



Partant de ces constats un 2ème focus de la commission R2S – Cybersécurité pourrait être d'approfondir et construire la trame pour les chainons manquants.

Pour les équipements :

En se référant aux normes existantes par exemple les référentiels des systèmes électroniques de sécurité (APSAD et CNPP)



Cependant ces référentiels ne couvrent que quelques segments métiers du bâtiment et ne s'appliquent pas à tous, comme par exemple la GTB, pourtant l'un des systèmes techniques centraux du bâtiment.
De plus au-delà des certifications de services (intégration – installation …) telle que présentée ci-dessus il ne faut pas oublier les certifications produits (à détailler lesquelles …)

Il conviendrait donc de voir dans quelle mesure ces certifications pourraient être étendus à l'ensemble des systèmes techniques du bâtiments

Pour les systèmes d'information :

Il est fait observer qu'il y a 2 univers différents : Les applications et les données

Sur la thématique des données plusieurs questions sont débattues :

- La sécurisation des données tout au long de leur flux.
- La gestion des logs. Cette question étant également abordée dans al commission juridique de la SBA.
- Le stockage des données (et les logs) de manière sécurisée pour y avoir accès en cas d'incident, en spécifiant spécifié comment on y accède, combien de temps ces données doivent être stockées, etc…
- La diversité des données qui doivent être normalisées afin de pouvoir les analyser.

Sur la thématique des applications & services plusieurs points sont évoqués :

- Etudier la matrice établie par Wallix /Kardham
- Intégrer les notions de : préventif / curatif / secured by design
- L'accès aux applications doit être sécurisée

Il est proposé de constituer des groupes de travail afin d'approfondir les thèmes vus lors de cette réunion. 3 groupes sont proposés :

GT Equipements (contributeurs) :

- Solenn Lefranc (Orange)
- Gilles Courtes (Engie)
- Nathalie Labeys (CNPP)
- Y adjoindre un acteur de la GTB …

GT Données (contributeurs) :

- Didier Cohen (Wallix) voir aussi avec JC Denis (Wallix)
- Virgile Auges (AN2V)
- Y associer IBM ou Aruba …

GT Système d'Information/Application (contributeurs) :

- Pascal Zeratès (Khardam)
- Didier Cohen (Wallix) voir aussi avec JC Denis (Wallix)
- Ronan McFarlane (SIA Partners)

<u>Questions & remarques générales :</u>

Profil de la cible de R2S-Cybersécurity (quel niveau de technicité) ? On s'adresse à 2 cibles :

- ⇨ Au responsable d'un projet bâtimentaire qui a une culture générale du bâtiment
- ⇨ Qui doit s'appuyer sur des BE spécialisés.

L'objectif étant de construire un cadre de référence technique qui doit être assez précis pour la labélisation.

Faire appel au département Cyber de la gendarmerie nationale : Cl Nollet
Inviter des acteurs de l'infra IT. : Aruba / Cisco / IBM
Faire venir un acteur des assurances

Noémie Douénat (Ingetel) se propose de coanimer les travaux de la commission Cybersécurité.

<u>Prochaines étapes :</u>

- ⇨ Constituer ces 3 groupes de travail tels que vu plus haut
- ⇨ Charge à ces GT de définir leur agenda (structuration de leur thèmes et calendrier)