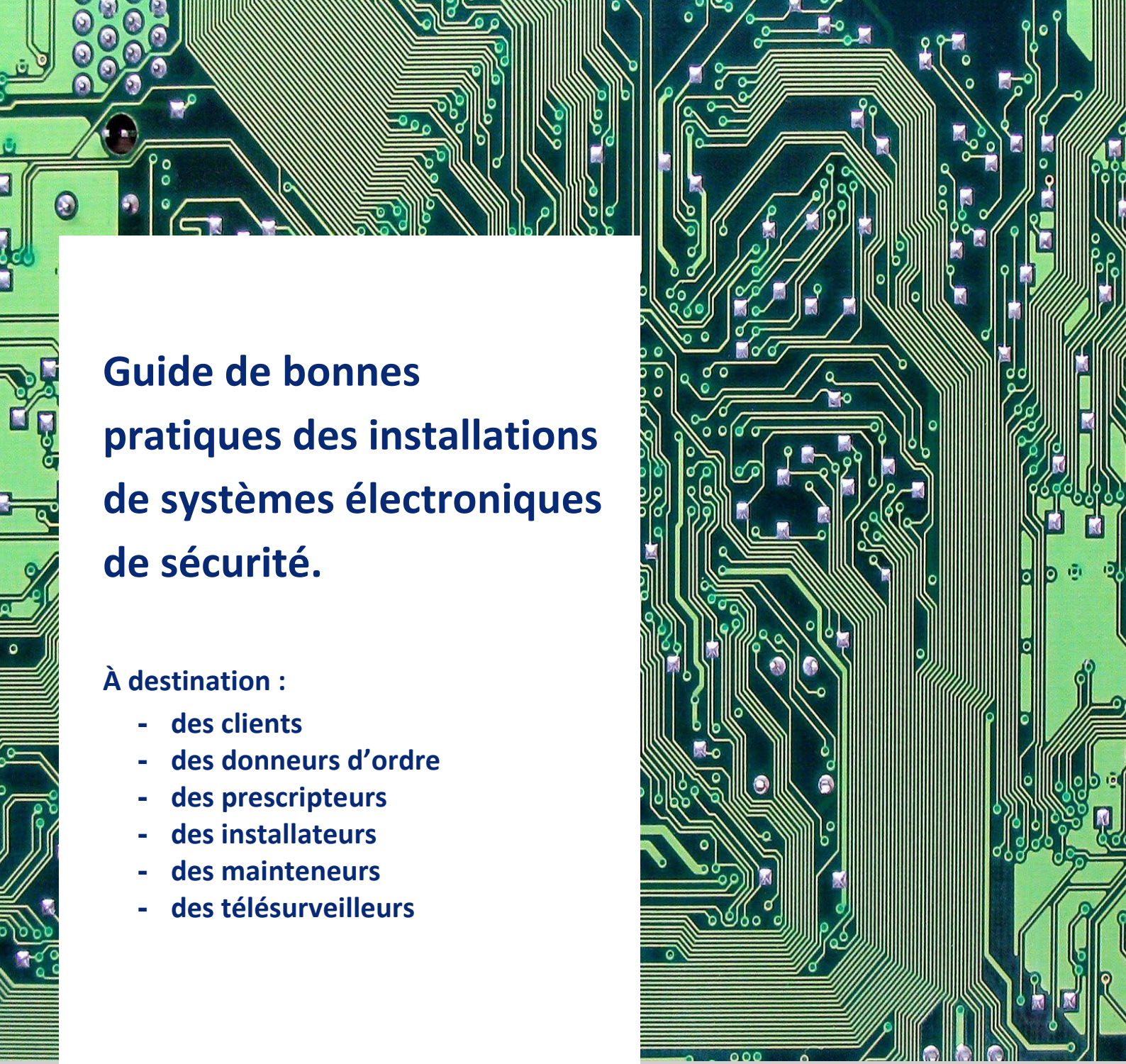


Guide de bonnes pratiques des installations de systèmes électroniques de sécurité.

À destination :

- des clients
- des donneurs d'ordre
- des prescripteurs
- des installateurs
- des mainteneurs
- des télésurveilleurs

Guide réalisé par :

CNPP

ADMS

Édition Mars 2021

Table des matières

Préambule 3

Les bonnes pratiques 3

1. Juridique 4
2. Techniques 7

Transmissions d'alarme 8

1. Niveaux de transmission suivant le référentiel APSAD R31 Télésurveillance de septembre 2017 9
2. L'arrêt du RTC 10
3. Impacts sur la transmission des alarmes 10

Les caractéristiques du raccordement classique et répandu 10

Transmission des signaux 11

L'indépendance par rapport à l'alimentation électrique 12

La détection de défaut de ligne 12

Les fonctions d'écoute/interpellation 12

Les garanties contractuelles de service 13

La rémunération du service 13

Le monde du "Tout IP" 13

Conclusions 13

Les modes de transmission 14

1. Le RTC 14
2. GSM (canal de communication voix) 15
3. DATA MOBILE (GPRS 3G 4G 5G) 17
4. VoIP / ADSL ou câble 19
5. IP / ADSL (ou câble/ fibre) 21
6. Balises VHF 23
7. Low-Power WAN (IoT) 25
8. RTC + secours GSM (canal de communication voix) 27
9. VoIP + secours GSM (canal de communication voix) 29
10. IP + secours VoIP 32
11. IP + secours data mobile (GPRS / 3G/4G/5G) 35

Annexes 37

Annexe 1 : Glossaire général 37

Annexe 2 : Plaques arrêtées par France Télécom 40

Annexe 3 : Zones Blanches 40

Annexe 4 : Risque de foudre - Zones kérauniques 40

Remerciements

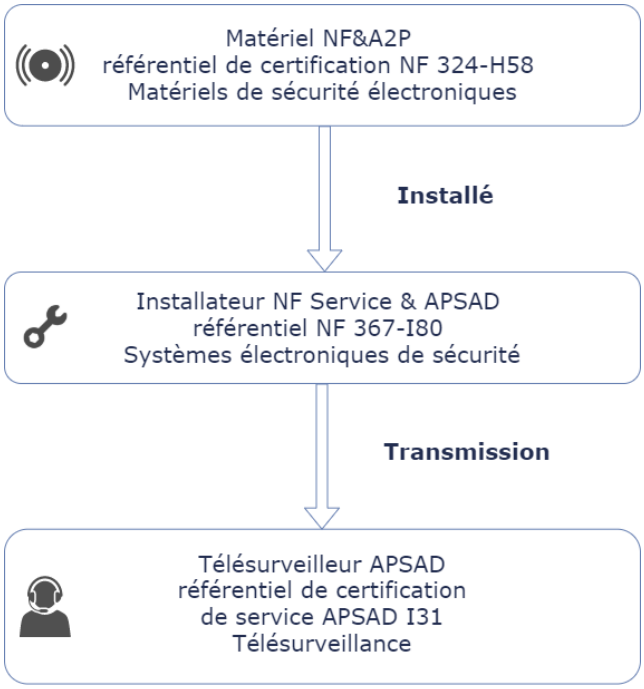
L'ADMS et le CNPP remercient la Fédération Française de l'Assurance d'avoir pu utiliser comme base de travail l'étude : « Situation actuelle et perspectives sur la transmission des informations d'alarmes aux entreprises de télésurveillance » rapport initialement commandé par la FFA au CNPP.

Préambule

Ce guide a pour but de rappeler les bonnes pratiques des installations de systèmes électroniques de sécurité.
Il est à destination des clients, des donneurs d'ordre, des prescripteurs, des installateurs, des mainteneurs, des télésurveilleurs.
Un rappel global des bonnes pratiques sera fait que ce soit d'un point de vue technique mais aussi contractuel.
Nous verrons aussi l'incidence que peut avoir l'arrêt du RTC dans la chaine globale de sécurité. Nous listerons tous les modes de transmission entre une installation de sécurité électronique et une station de télésurveillance.

Les bonnes pratiques

Un système électronique de sécurité a pour fonction de protéger les biens et les personnes.
Il est préconisé qu'une installation soit raccordée à une station de télésurveillance afin que les consignes clients soient respectées et que si nécessaire une intervention des forces de l'ordre soit lancée.



Toute la chaine de sécurité peut être certifiée par le CNPP et des référentiels APSAD encadrent l'ensemble de la chaine.
Seule la transmission reste le maillon « faible », car aucune norme n'existe sur ce point. La transmission dépend de sociétés externes du type opérateur de téléphonie fixe, mobile, détendeur de licence radio, ….
Il est donc important de connaitre les bons usages pour de bonnes transmissions des informations délivrées par les installations surveillées et transmises par des dispositifs électroniques.

L'installation d'un système électronique de sécurité doit répondre à un certain nombre d'exigences afin d'être conforme à la réglementation et aux règles de l'art.
Voici les différentes étapes que cela doit suivre :
- Etude technique avec une analyse de risque
- Validation commerciale de l'offre
- Contractualisation
- Conception
- Réalisation
- Mise en service (test de l'installation)
- Réception
- Maintenance préventive
- Maintenance curative

Les préconisations techniques et juridiques ci-dessous sont obligatoires et doivent être respectées. Elles doivent être prise en compte quel que soit le mode de transmission.

1. Juridique

CADRE GENERAL

La protection par systèmes électroniques peut comporter trois sortes de prestations complémentaires, qui sont :
- L'installation et la maintenance du système.
- La télésurveillance.
- L'intervention (ou levée de doute).

L'analyse des obligations qui résultent de chacune de ces prestations est rendue d'autant plus délicate que, selon les cas, elles seront exécutées par un seul prestataire ou par plusieurs.
Ainsi, il est fréquent qu'un prestataire ait installé le système, tandis qu'un autre assumera la télésécurité, dénomination par laquelle il convient d'entendre une mission de télésurveillance, doublée d'une intervention sur les lieux.
Dans un souci de clarté, ces obligations seront examinées séparément, sans qu'il faille pour autant occulter l'éventualité de leur cumul.

JURISPRUDENCE

La jurisprudence résulte de l'ensemble des décisions prises par une juridiction sur une matière, en tant qu'elles constituent une source de droit.
Il s'agit donc de l'interprétation que font les juges des textes de loi, au fil des évolutions de la société, des mœurs, des usages, etc….
Les notions d'obligations de moyens, de résultat, de renseignement, ainsi que le devoir de conseil, résultent de la jurisprudence.
Ces notions sont définies ci-après :

L'OBLIGATION DE MOYENS

L'obligation de moyens consiste à s'engager simplement à employer les moyens appropriés, dans une tâche à accomplir.
Partant, il n'est pas anormal qu'une diligence appropriée n'aboutisse pas au résultat recherché. Le résultat est aléatoire, et ne peut faire l'objet même de l'obligation, celui-ci étant la diligence, le comportement.
Le succès, c'est-à-dire le résultat, dans cette hypothèse, ne dépend pas seulement de l'attitude du prestataire, mais aussi d'autres facteurs sur lesquels il n'a pas de prise.
Dès lors, il y a toujours un risque assez grand d'échec : c'est l'aléa.

L'OBLIGATION DE RESULTAT

Ici le prestataire promet à son client de lui procurer coûte que coûte un résultat déterminé et précis.
Le client n'accepte pas que le doute puisse exister sur la certitude du résultat attendu. Le contenu de l'obligation parait donc être le résultat lui-même.
Certes, pour l'atteindre, le prestataire devra mettre en œuvre des moyens, mais ceux-ci ne sont pas pris en considération.
Le principe d'une obligation de résultat ne peut se concevoir que si l'exécution de cette obligation est normalement possible : le résultat promis apparait suffisamment certain pour constituer l'objet même de l'obligation, de sorte que la non-obtention du résultat permet de présumer de la responsabilité du prestataire.
L'obligation est de résultat, dans la mesure où ce dernier n'est pas aléatoire.

L'OBLIGATION D'INFORMATION

Cette notion impose au prestataire, non seulement d'exécuter la prestation comme convenu, mais encore :
- de fournir tous les renseignements indispensables à l'usage des matériels installés et/ou vendus.

Il s'agit pour le prestataire de s'informer des besoins du client, de lui apporter tout renseignement qui pourrait lui être utile concernant le matériel et/ou la prestation à livrer.
Le prestataire indiquera au client, les caractéristiques des produits, les conditions d'utilisation, l'adéquation de l'environnement, le contenu des contrats envisagés, les coûts, les garanties, sans oublier de l'informer et le mettre en garde de toutes les éventuelles limitations de la solution proposée.
Cette obligation d'information s'applique dès l'établissement du devis et perdure durant toute la période d'exécution du contrat.

L'OBLIGATION DE CONSEIL

Cette obligation impose au professionnel, d'intervenir en amont de l'installation du système, en sa qualité de "sachant", pour préconiser au client, les moyens adéquats, permettant d'aboutir et de répondre au souci de protection exprimé par ce dernier.

Dans le cadre de cette obligation, le professionnel est tenu d'informer le client sur les risques susceptibles de voir compromettre sérieusement l'efficacité du système proposé.
De fait, le professionnel est tenu de proposer des solutions pour optimiser l'efficacité du système.
A titre d'exemple, il devra entre autres, proposer des solutions pour pallier aux risques de coupures du ou des supports de communications dans le cas d'un système d'alarmes relié à un PC de télésurveillance.
Cette obligation perdure pendant toute la durée du contrat.

Le devoir de conseil pose à l'évidence un problème : celui de la conservation de la preuve.

Pour dégager sa responsabilité en cas de sinistre, le professionnel devra en effet, prouver qu'il a correctement conseillé son client et que ce dernier, en connaissance de cause, avait décidé de ne pas suivre les préconisations présentées.

Synthèse :
Pour les raisons évoquées ci-dessus, il est donc impératif de confirmer, lors de la formalisation de vos engagements dans le contrat de prestations, la traduction écrite de vos préconisations, conseils et informations et ce dans l'optique de devoir répondre et prouver que vous n'avez pas failli à vos obligations en tant que professionnel.
Tantôt effectuée par des électriciens (qui ne sont généralement pas assurés correctement), tantôt par des installateurs de métier, il n'en demeure pas moins que la pose de systèmes d'alarmes (intrusion, incendie, gestion technique, etc.…) confère au professionnel, de véritables obligations vis-à-vis de son client, lesquelles peuvent se traduire en terme de responsabilité le jour d'un sinistre.

Ces obligations sont multiples et se décomposent comme suit :

FOCUS sur les installateurs de systèmes de détection

Obligation de résultat :
L'analyse des nombreux arrêts de la Cour de cassation permet de confirmer, que le fournisseur d'un système d'alarme est tenu vis-à-vis de son client, d'une obligation de résultat.
Cette obligation qui pèse sur le professionnel, consiste à garantir au client final, que le système posé, fonctionnera correctement le jour de la réalisation d'un événement (tentative d'effraction, par exemple).
Pour être très précis et clair sur la notion de "fonctionnement du système d'alarme", le système d'alarme doit déclencher.
Si ce n'est pas le cas, le professionnel devra, pour dégager sa responsabilité, prouver que la défaillance du système, provient d'une cause étrangère qui ne peut lui être imputée (détecteurs masqués par une plante, configuration des lieux modifiée, défaillance intrinsèque du système, etc…).
Dans le cas contraire, les conséquences financières en cas de vol, resteront à la charge du prestataire ou de son assureur, s'il est garanti pour cette activité.
A cela s'ajouteront les obligations d'informations et de conseil, vues ci-dessus.

FOCUS sur les télésurveilleurs

Obligation de moyens :
La télésurveillance constitue un maillon intermédiaire dans la chaîne de sécurité, positionnée entre l'installation qui détecte l'événement et l'intervention qui permet d'en vérifier la réalité et de prendre les mesures utiles.
La responsabilité intrinsèque du télésurveilleur se situe donc dans un périmètre somme tout limité : relever les messages transmis par l'installation et appliquer les consignes propres à ces messages.
A ce titre, attention, on parlera alors concernant l'application des consignes, d'une obligation de résultat.
A ces obligations, s'ajouteront les obligations d'informations et de conseil, vues ci-dessus.

DANS LE CADRE DE L'ARRET DU RTC……

Il appartient donc au prestataire qui a un contrat en cours avec son client (d'installation, de maintenance ou de télésurveillance) d'informer ce dernier de l'arrêt programmé du RTC et de ses conséquences.
A ce titre, il devra donc proposer au client, les solutions de substitution, mettant en exergue les avantages et inconvénients (limites) et préconiser en sa qualité de sachant, la ou les solutions optimales au regard des caractéristiques du système de son client.
Pour remplir parfaitement son obligation de conseil, l'ensemble des informations et préconisations devront être réalisées par écrit et obtenir l'aval du client pour validation.

Des contrats types sont disponibles auprès de l'ADMS.

2. Techniques

Risques	Contraintes	Conformité R31
Foudre sur l'arrivée électrique	Destruction de l'installation et de l'ensemble des périphériques	Mise en place de parasurtenseurs
Coupure secteur centrale	Coupure alimentation centrale d'alarme	Secours par une batterie Autonomie définie dans les référentiels
Coupure secteur boitiers hors alarme (box, transmetteur,…)	Plus de transmission	Prévoir un onduleur et contrat de maintenance préconisé pour ce type d'équipement
Arrachement câblage		Autoprotection des boites de raccordement Protection mécanique des arrivées
Câblage		Les câbles doivent être d'un seul tenant. Les barrettes de raccordement intermédiaires et les épissures sont interdites
Risque Cyber sur le site	Prise en main du système et malveillance	Choix d'un matériel certifié @ par le CNPP Pas de bidirectionnalité du système d'alarme. Les informations ne peuvent que sortir mais pas rentrer
Risque Cyber du télésurveilleur	Mise hors service de la station de télésurveillance	Choix d'une station de télésurveillance avec une certification à minima APSAD P3
Risque Cyber fournisseur transmission	Plus de transmission possible sur le vecteur de communication	Voir les conditions générales de l'opérateur avec les temps de rétablissement et les taux de disponibilité réseaux garantie
Essais de transmission télésurveillance partiels ou non conformes	Risque de message inconnu ou non reconnu lors de tests	

Afin de répondre aux différentes réglementations et normes voici la liste des référentiels utilisés :

Installation et Maintenance de Systèmes Electroniques de Sécurité :
Référentiel de certification NF 367 – I80 Systèmes Electroniques de Sécurité

Service d'installation et de maintenance :
Détection d'intrusion / Vidéosurveillance / Contrôle d'accès.
Référentiel APSAD R81 Détection d'intrusion – Règle d'installation.
Référentiel APSAD R82 Vidéosurveillance – Règle d'installation.
Référentiel APSAD D83 Contrôle d'accès – Document technique pour la conception et l'installation.

Station de Télésurveillance :
Référentiel de certification de service APSAD I31 – Télésurveillance.
Référentiel APSAD R31 Télésurveillance – Règle de prescription.

Cybersécurité :
Référentiel APSAD D32 Cybersécurité – Document technique pour l'installation de systèmes de sécurité ou de sûreté sur un réseau informatique.

L'ensemble des documents sont disponibles sur le site du CNPP à l'adresse suivante :
https://cybel.cnpp.com/

Transmissions d'alarme

Pour la partie transmission des informations nous allons vous détailler les moyens de communications utilisables.
Il est rappelé que l'utilisation d'une seule liaison de transmission (filaire ou hertzienne) rend l'installation vulnérable.
Il est préférable de coupler 2 liaisons de transmission distinctes (filaire et/ou hertzienne) et de choisir si possible des opérateurs différents.
Il est possible d'utiliser comme support de communication pour les liaisons de transmission le GSM, le RTC, le GPRS ….
Vous trouverez les fiches x à y qui correspondent à des exemples de transmissions avec secours du support de communication de la liaison de transmission.
Ce ne sont que quelques exemples, d'autres possibilités sont possibles et le nombre de support de communication peut ne pas se limiter à 2.

La télésurveillance est un service permettant la surveillance à distance par des systèmes électroniques de sécurité. Cette surveillance peut s'appliquer à des dispositifs fixes ou mobiles.

La transmission des alarmes répond généralement au schéma suivant :

- ⇨ Les signaux d'alarme sont codés à l'émission, différents protocoles existent.
- ⇨ La liaison de transmission sert également en réception (retour d'acquittement, et télémaintenance).

La liaison de transmission peut utiliser un support de communication dédié (balise radio, ligne privée) ou un réseau qui présente l'avantage d'être partagé entre plusieurs utilisateurs, et d'offrir un niveau de redondance interne.
Pour améliorer la disponibilité, la liaison de transmission peut utiliser deux supports de communication, voire plus. La tolérance aux pannes est ainsi accrue.
Les fiches « moyens de transmission » en annexe donnent des exemples de réalisation.

1. Niveaux de transmission suivant le référentiel APSAD R31 Télésurveillance de septembre 2017

Le référentiel R31 de septembre 2017 décrit les 4 niveaux de transmission que vous retrouverez ci-dessous et qui doivent être respectés.

Niveau	Délai de mise à disposition de l'information *	Surveillance du support de communication de la liaison de transmission principale	Surveillance du support de communication de la liaison de transmission secondaire	Remarques
I	180 s	La détection et la signalisation d'une défaillance de la liaison de transmission principale apparaissent à la station de télésurveillance en moins de 3 min	La détection et la signalisation d'une défaillance de la liaison de transmission secondaire apparaissent à la station en moins de 10 min	Deux liaisons de transmission distinctes (filaire et/ou hertzienne) La surveillance de liaison de transmission peut être assurée par un système de supervision
II	10 mn	La détection et la signalisation d'une défaillance de la liaison de transmission principale apparaissent à la station de télésurveillance en moins de 10 min	La détection et la signalisation d'une défaillance de la liaison de transmission secondaire apparaissent à la station de télésurveillance en moins de 24 h	
III	Pas de disponibilité sur défaut du support de communication	La détection et la signalisation d'une défaillance de la liaison de transmission apparaissent à la station de télésurveillance en moins de 10 min	S/O	Exemples de supports utilisés : RTC, RNIS, GSM, GPRS, IP sous ADSL, etc…
IV	Pas de disponibilité sur défaut du support de communication	La détection et la signalisation d'une défaillance de la liaison de transmission apparaissent à la station de télésurveillance en moins de 24 h	S/O	

* Le délai de mise à disposition de l'information est le temps maximal de mise à disposition de l'information sur le module de traitement à partir de la présentation de l'information au transmetteur du site surveillé. Ce temps est mesuré en présence d'un défaut sur un des supports de communication. Il intègre les délais de réacheminement de la communication.

=> Exemples :

Niveau I

Support IP (3mn) et secours GPRS (10mn) est de niveau I.

Niveau II

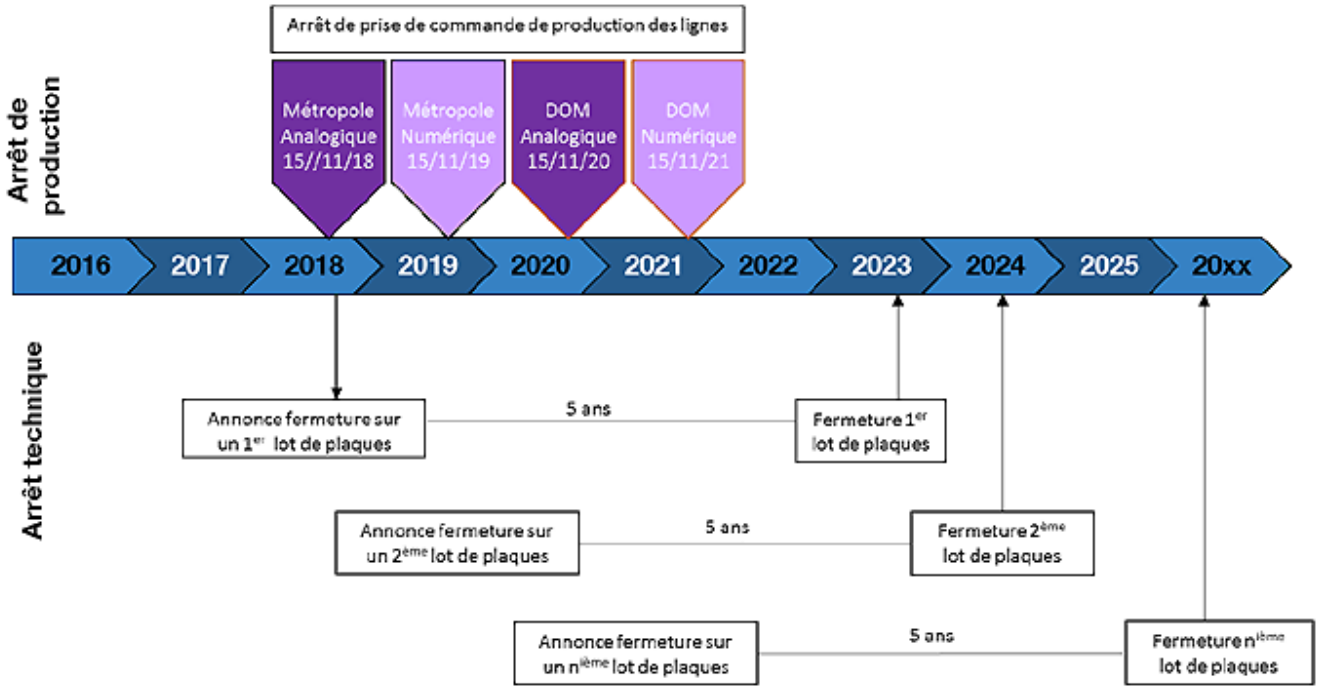
Support IP (10mn) et secours GPRS (24h) est de niveau II.
Support IP (10mn) et secours RTC (24h) est de niveau II.
Support GPRS (10mn) et secours RTC (24h) est de niveau II.

Niveau III

Support ADSL avec transmission IP (3mn ou 10 mn) et le secours RTC sur le même support physique est de niveau III.

2. L'arrêt du RTC

Le 26 octobre 2018, l'opérateur historique Orange a confirmé le plan d'abandon du Réseau Téléphonique Commuté (ou téléphone analogique) par « plaques » géographiques, en définissant les premières zones concernées (Charente-Maritime, Haute-Garonne, Haute-Loire, Morbihan, Nord, Seine-et-Marne, Vendée).
Le planning diffusé jusqu'ici doit être à recaler en application du délai d'annonce de 5 ans : fin 2023 pour la première plaque.



(Source arcep.fr)

Les dates d'arrêt de production sont toutefois maintenues :

- Depuis le 15 novembre 2018, il n'est plus possible d'ouvrir une nouvelle ligne fixe analogique. Les nouvelles lignes seront en technologie IP.
- Le 15 novembre 2019, les lignes RNIS (Numeris) ne seront plus commercialisées. Ceci concerne les accès T0 explicitement. Rien n'est annoncé concernant les accès primaires (ou T2). Il n'est pas annoncé non plus de fermeture des accès existants. L'impact en serait limité puisqu'il existe dans le commerce des passerelles au standard d'interconnexion SIP/IP.

NOTA : la fin du RTC ne veut pas dire la fin du cuivre. Les solutions IP actuellement distribuées sur le réseau cuivre vont bien subsister (ADSL, SDSL, lignes voix sur IP, …), sans qu'il soit nécessaire de les migrer sur fibre.
L'alternative future proposée à la téléphonie analogique est la VoIP (Voice Over Internet Protocol), technologie permettant de délivrer des communications vocales ou multimédia (vidéo par exemple) via le réseau Internet.
L'offre est déployée depuis de nombreuses années sur les box internet.
L'interconnexion des réseaux permet à l'utilisateur d'appeler n'importe quel abonné, qu'il soit raccordé en RTC ou en VoIP.

Pour les usages du RTC en transmission de données pure (anciens modems 56k, etc), les solutions de remplacement existent et donnent satisfaction (IP sur ADSL, GPRS).

3. Impacts sur la transmission des alarmes

Les caractéristiques du raccordement classique et répandu

Pour des raisons historiques, la plus grande partie des sites sous alarme est raccordée en RTC.
Les banques sont aujourd'hui raccordées en IP (souvent secouru par une ligne RTC).
Les nouvelles installations de particuliers se font maintenant en IP.

Ces parcs professionnels et particuliers ont des temps de renouvellement respectifs de 10 ans et de plus de 20 ans.

Les matériels développés ont exploité dès l'origine les particularités de la liaison analogique.

- Elle fonctionne sans avoir besoin d'une alimentation locale. Seul le modem interne à la centrale doit être alimenté.
- La coupure de ligne est détectée localement à moindre frais, simplement par l'absence de 48V.
- Elle est naturellement adaptée à la levée de doute audio et à l'interpellation. (Cette application tend à s'effacer avec la montée en puissance de la levée de doute vidéo via l'ADSL.)
- Elle est bien caractérisée pour le transport des codes en fréquences vocales. Les modems réutilisent le codage DTMF (Dual Tone Multi Frequency) et les composants spécifiques associés, initialement développés pour la numérotation.

Mémo : Principe de la communication RTC sur modem avec démodulation fréquence DTMF

Les technologies actuelles de transmissions de Télésurveillance utilisent les lignes téléphoniques, et plus particulièrement les fréquences DTMF (Dual Tone Multi-Frequency).

Cela signifie que lorsqu'un transmetteur émet une trame, il génère des sons dans la gamme de fréquence 300Hz à 3,4 GHz.

Alors, les cartes de démodulation multiprotocole en réception traduisent ces signaux en code au format Hexadécimal (0 à 9, A à D, et * #).

Le transport de ces signaux entre le site surveillé et le site de réception est supporté par les réseaux cuivre, en cours de remplacement par des réseaux fibre. Aussi, ce transport de bande s'effectue de 2 façons pour les nouveaux modes VoIP :

- en tonalités audio dans le flux vocal,
- ou en paquets séparés du flux vocal, mais sur le même canal que le flux vocal.

Suivant ces nouveaux modes de transmissions, et malgré les utilisations du Codec Spécifique G711, certaines fréquences ne sont pas jouées par les FAI (les lettres A à D qui sont essentiellement utilisées dans l'armée), de plus les FAI compressent les silences entre les bruits.

Ceci a pour incidence la perte potentielle de morceau de trame suivant le taux de compression des lignes, et donc une mauvaise traduction lors de la démodulation.

Ainsi, tant que les FAI n'auront pas terminé leurs travaux en cours, consistant à améliorer ces traitements, toutes les installations RTC sont exposées à quelques dysfonctionnements ponctuels.

Exemple :
L'appui sur la touche 5 produit une tonalité composite, de fréquences 770 Hz et 1336 Hz.

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Mais à la différence d'un utilisateur manipulant les touches, les modems accélèrent la cadence de succession des codes.

Transmission des signaux

Il est déconseillé de raccorder un transmetteur d'alarme classique à une box VoIP d'opérateur, car par défaut ces dernières sont optimisées pour la numérotation et les services interactifs pilotés manuellement. Pour une meilleure fiabilité, les fréquences sont décodées, converties en données dans un canal distinct, puis resynthétisées à l'interface de destination. Les paramètres du filtrage ainsi opéré ne conviennent pas aux signaux DTMF rapides, qui peuvent subir des altérations. Il en résulte des taux d'erreur inacceptables, à moins de désactiver cette conversion et de transmettre les signaux sans traitement (mode « in-band »).

Pour ne pas avoir à installer deux box distinctes (l'une dédiée à la téléphonie, l'autre dédiée aux automates (alarme intrusion, appareil de téléassistance, etc)) chez les utilisateurs, il est possible de commuter le mode approprié en fonction du destinataire des communications :

- « telephone event » s'il s'agit d'un serveur vocal,
- « in-band » s'il s'agit d'une station de télésurveillance.

Cela fonctionne si toute la chaine est en VoIP, chaque opérateur de la chaine gérant la signalisation SIP.

Mais pendant la phase transitoire, tous n'auront pas basculé en IP en même temps en fonction de leur situation géographique.

A minima, tous les télésurveilleurs devront proposer, dès la fermeture de la première plaque, un frontal VoIP ou une passerelle VoIP/RNIS capable de télécommander le mode « in band » à la box terminale.

Il a été déterminé que les conditions favorables sont les suivantes :

- Codage audio G711 sélectionné,
- « telephone event » désactivé (voir ci-dessus).

Des essais (ouverts notamment aux télésurveilleurs) sont en cours avec les opérateurs SFR et Orange, afin de vérifier la bonne transmission de tous les protocoles de bout en bout.

L'indépendance par rapport à l'alimentation électrique

L'alimentation centrale à 48V des lignes téléphoniques est un héritage des premières solutions techniques remontant à Graham Bell, et ne doit rien à des contraintes réglementaires.

La box d'interconnexion est un boitier supplémentaire, nécessitant une alimentation. Pour des raisons économiques, les constructeurs excluent d'y incorporer une batterie.

- Les chiffres qui ont circulé (autonomie de 8 heures) sont alignés sur le marché américain, et restent très éloignés des besoins exprimés dans le référentiel APSAD R81 Détection d'intrusion – Règle d'installation (12 heures en habitation, 36 heures minimum pour des locaux professionnels).
- La consommation électrique des box multiplay, intégrant éventuellement un disque dur et divers accessoires, est prohibitive. L'onduleur adapté serait plus gros que la box.

En revanche, une box spécialisée VoIP pourrait se contenter de quelques Watts en 12V, puissance compatible avec des chargeurs de type téléphone portable, ou avec le système d'alimentation secourue des centrales existantes.

Nota : ce serait hors référentiel de certification NF 324-H58 Matériels de sécurité électroniques (NF&A2P). Aucun produit n'est certifié à ce jour, et les centrales concernées n'ont jamais été testées avec cette connexion supplémentaire.

La détection de défaut de ligne

La méthode pratique de détection de coupure est le contrôle de présence de la tension de ligne (48V). Moyennant une temporisation (de 30 s à 1 min en général), l'alerte peut être renvoyée au télésurveilleur via une liaison secondaire. Cette possibilité est exploitée lorsqu'une disponibilité améliorée de la transmission est exigée. C'est en particulier le cas, suivant le référentiel APSAD R81 Détection d'intrusion – Règle d'installation, de tous les sites de catégorie C.

Pour continuer à fonctionner suivant ce schéma, il faut que la box VoIP :

- coupe sa polarisation de ligne lorsque le statut VoIP passe à NOK.
- ou bien délivre un signal défaut sur une sortie supplémentaire, qui active le transmetteur secondaire. Ce n'est pas à l'ordre du jour des fabricants.

Sinon, il faudrait recourir à une supervision de la partie IP du réseau, et transmettre au télésurveilleur l'identité des terminaux non accessibles. La faisabilité de cette solution reste à documenter.

Les fonctions d'écoute/interpellation

Dès lors que la signalisation par codes DTMF fonctionne, les commutations nécessaires devraient s'effectuer normalement dans les anciennes centrales. Il n'y a pas d'impact à prévoir.

Les garanties contractuelles de service

L'opérateur en charge du Service Universel doit se fixer un objectif de délai de réparation d'une défaillance inférieure à 48 heures calendaires pour 85% des demandes traitées le plus rapidement (source ARCEP). Cela s'applique au service sur RTC.

Sur les autres services, il n'existe aucune garantie, sauf contrat spécifique (ex : Orange Business propose aux professionnels une Garantie de Temps de Rétablissement inférieur à 4 heures). Les conditions contractuelles d'un opérateur de VoIP concurrent sont à étudier de près sur ce point.

Il convient d'autre part de rappeler que dans ses Conditions Générales de Vente, Orange déclare la connexion fibre incompatible avec les services de téléalarme ou de télésurveillance.

La rémunération du service

La fin du RTC signifie aussi la fin des services à valeur ajoutée (via les numéros 08) par lesquels une partie du service de télésurveillance était rétribuée et qui servaient aussi à la bascule des transmetteurs d'une station à l'autre en cas de panne.

Le monde du "Tout IP"

Une technologie disparait, avec ses équipements spécifiques et ses logiques d'interconnexion caractéristiques.
Ces derniers et dernières permettaient assez facilement d'identifier la séparation des réseaux (même si les supports physiques peuvent être partagés, ex : lignes dégroupées). Ce ne sera plus le cas.
L'avantage des réseaux IP, c'est la possibilité d'une redondance interne (ou « transparente », ce qui veut dire qu'elle ne se voit pas sans outils de diagnostic).
Le critère à utiliser dans le choix d'un contrat de service de télécommunication, quel que soit le prestataire, devient la disponibilité propre du réseau, et non plus la multiplication des réseaux, censée améliorer la disponibilité globale. En clair, il ne sert à rien d'avoir une liaison principale chez un opérateur lourd, et une liaison de secours chez un opérateur « virtuel » ou « alternatif » qui partagerait une partie des mêmes infrastructures matérielles.

Conclusions

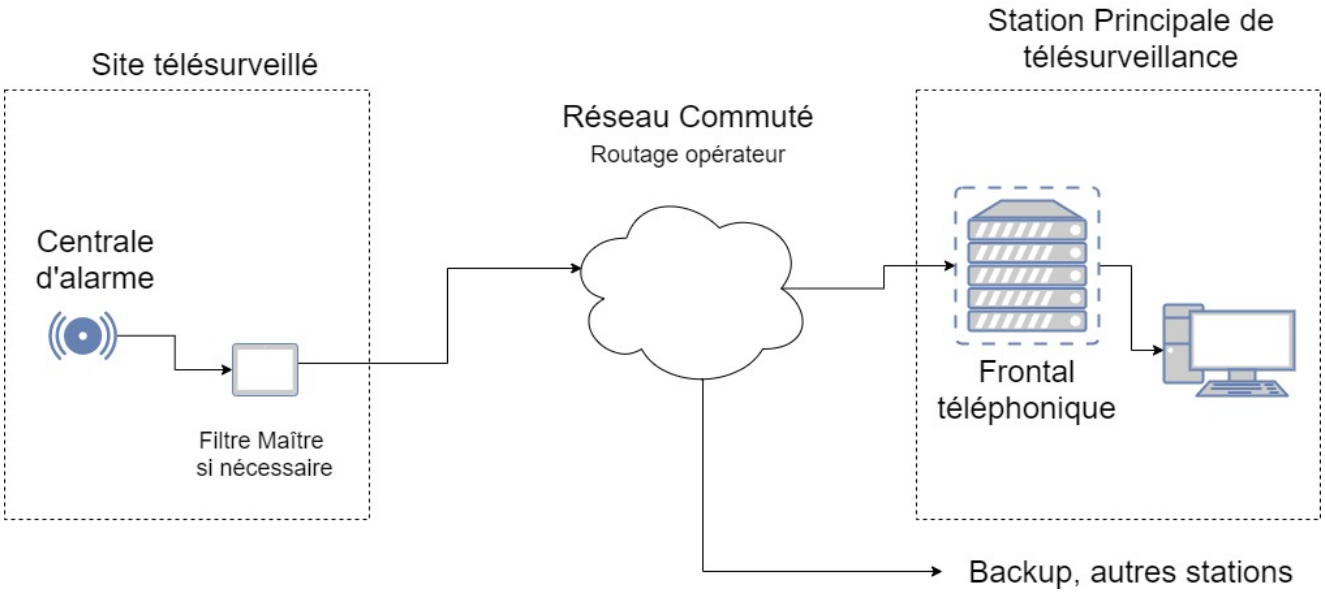
A ce jour, des difficultés subsistent :

- Dans la migration vers la VoIP des liaisons simples RTC (niveau de transmission IV) : il reste à valider la bonne transmission des différents protocoles utilisés, et à trouver sur le marché des mini-convertisseurs ou mini-box à basse consommation.
- Dans la migration des liaisons de niveau II intégrant le RTC, pour les mêmes raisons.
- Dans la création de nouvelles liaisons de niveau II intégrant la VoIP, tant que les box ou mini-box ne fourniront pas un diagnostic local exploitable.
- Dans la mise en place de liaisons IP directes sur des sites ne disposant pas d'une alimentation secourue. C'est le cas des particuliers, petits commerces, agences bancaires, etc... très rarement équipés d'un groupe électrogène pour leur informatique.

Dans l'immédiat, les solutions GPRS ou GSM (ou leurs combinaisons) restent applicables sans modification. Il convient bien entendu d'utiliser des transmetteurs satisfaisants aux critères d'autonomie. Cela doit être vérifié dans les spécifications du constructeur, et l'installateur doit respecter les dispositions de montage.
D'autre part, il convient d'évaluer en permanence la redondance interne des réseaux d'opérateurs disponibles.

Les modes de transmission

1. Le RTC



Paramètres fonctionnels du système de transmission

Tc : période du test cyclique

1h (en pratique) < Tc < 24h

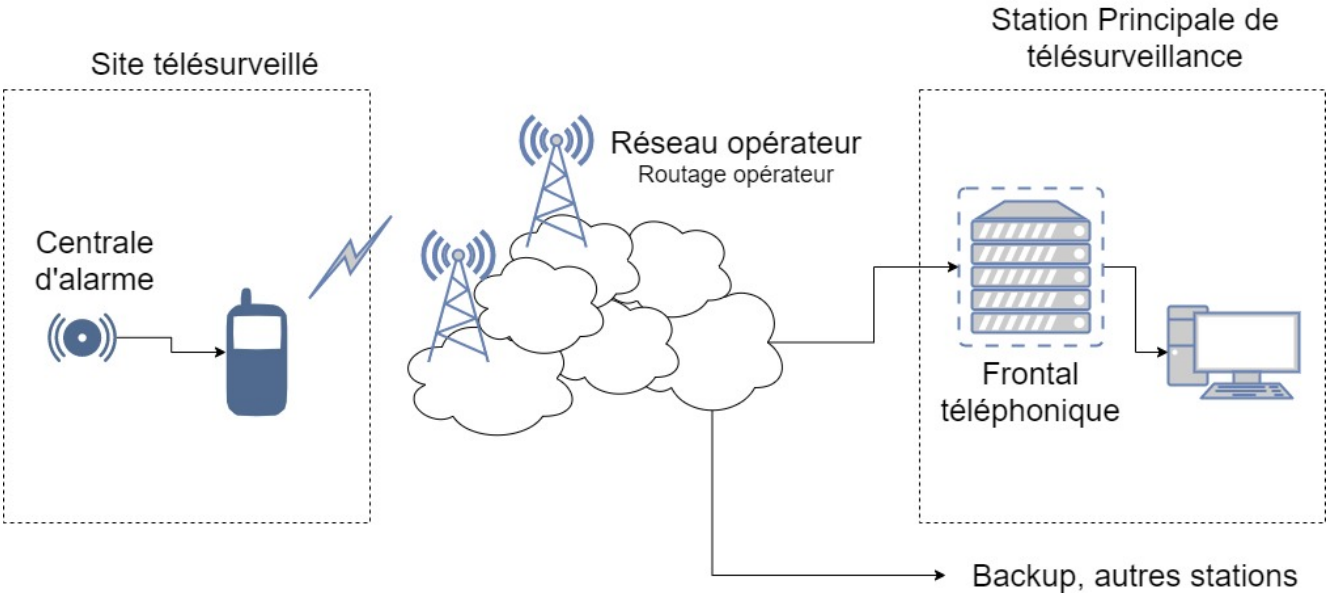
CARACTERISTIQUES

Contrôles	Contraintes	Conformité R31
Ligne téléphonique active et abonnement Connexion sur un autocom à proscrire Câblage maitre (prioritaire sur terminal de paiement, etc.) Programmation du n° d'appel Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station	Câblage filaire Fermeture en 2023 du réseau commuté Orange (plus de nouvelles installations depuis le 15 novembre 2018) Débit utile limité	Défaillance du support de transmission = indisponible *La détection et la signalisation de la défaillance apparaissent à la station de télésurveillance en moins de 24 heures* Période Tc<24h : niveau IV Période Tc>24h : hors niveau

ANALYSE DE RISQUE DU MODE DE TRANSMISSION

Évènements perturbateurs	Conséquences	Contre-mesures
Foudre	Destruction du transmetteur	Installation de parafoudres
Défaillance du réseau de l'opérateur	Indisponibilité, signalée dans un délai < période du test cyclique	Garantie de rétablissement 8h (service Orange Pro) Obligation du service universel (?)
Connexion frauduleuse	Neutralisation des fonctions d'alarmes	Protection contre les appels entrants (contre-appel)

2. GSM (canal de communication voix)



Paramètres fonctionnels du système de transmission

Tc : période du test cyclique

3h (en pratique) <Tc < 24h pour des raisons de coût.

CARACTERISTIQUES

Contrôles	Contraintes	Conformité R31
Abonnement auprès d'un opérateur acceptant ce type d'usage Qualité de transmission vocal suffisante Programmation du n° d'appel Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station CGV autorisent mise en place carte sim dans alarme CGV autorisent utilisation de numéro SVA	Compatibilité du protocole de transmission Couverture dépendante de l'opérateur (zones blanches) Débit utile limité (~10 kb/s) Support lié à l'opérateur et doit être changer en cas de changement d'opérateur Le support est un consommable qui peut tomber en panne	Défaillance du support de transmission = indisponible *La détection et la signalisation de la défaillance apparaissent à la station de télésurveillance en moins de 24 heures* Période Tc<24h : niveau IV Période Tc>24 : hors niveau

ANALYSE DE RISQUE DU MODE DE TRANSMISSION

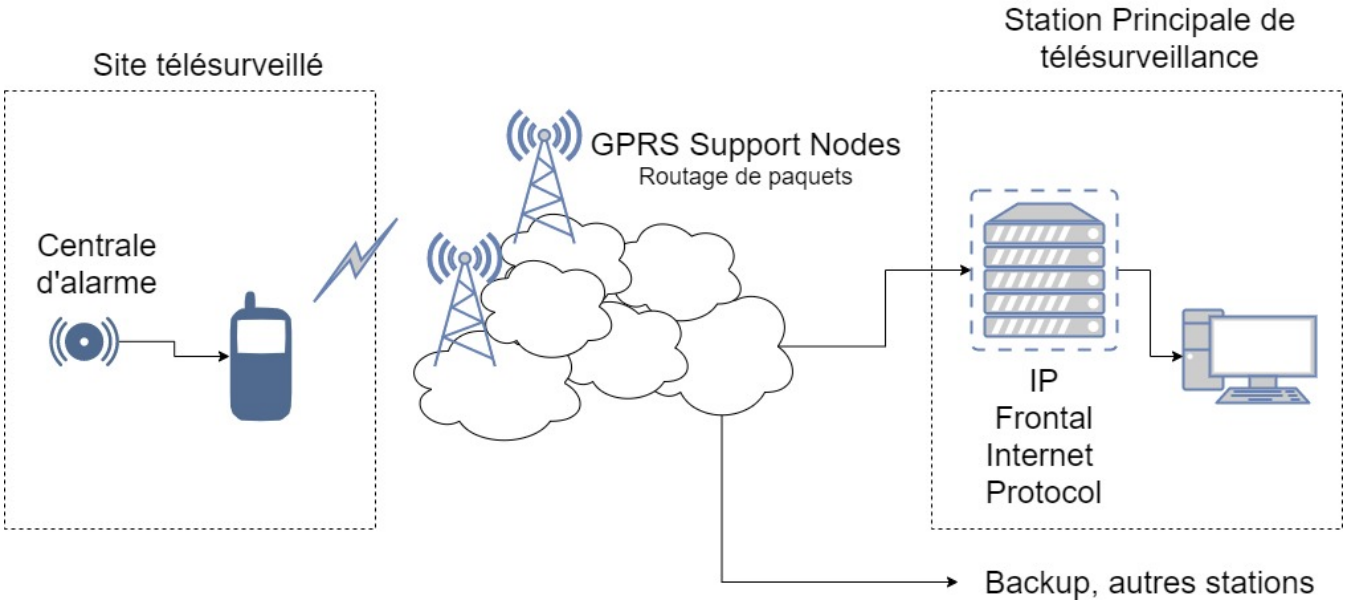
Évènements perturbateurs	Conséquences	Contre-mesures
Foudre	Destruction des antennes-relais	Antenne intérieure si possible Protections des antennes-relais + redondance de cellules
Défaillance ou surcharge du réseau de l'opérateur	Indisponibilité, signalée dans un délai < période Tc	Garantie contractuelle de rétablissement (sauf force majeure)
Perturbations électro-magnétiques, brouillage radio	Indisponibilité totale (signalée dans un délai < période du test cyclique) ou intermittente (incertain)	Néant
Usurpation de réseau (La carte SIM n'authentifie pas le réseau)	Indisponibilité, signalée dans un délai < période du test cyclique	Surveillance possible sur les réseaux 4G et 5G (pas en 3G)
Attaque cyber, connexion frauduleuse	Neutralisation des fonctions d'alarme (prise de contrôle de la centrale)	Protection contre les appels entrants, contre-appel
Forfait suffisant pour la typologie de transmission Ex 1 minute de voix pas suffisant	Blocage des transmissions par manque de crédit ou hors forfait	Etudier les conditions générales et ajuster son forfait a ses besoins

Les centrales d'alarme peuvent :

- Soit être équipées nativement (par exemple les produits radio destinés aux particuliers),
- Soit recevoir une carte interface,
- Soit piloter une passerelle externe, pour les modèles qui ont conservé leur interface RTC.

Les télésurveilleurs connus de CNPP et certifiés sont au niveau, pour gérer cette configutation.

3. DATA MOBILE (GPRS 3G 4G 5G)



Paramètres fonctionnels du système de transmission

Ts : période des paquets de surveillance. 10s <Ts < 300s.

N : nombre max d'échecs successifs. (De 2 à 5)

CARACTERISTIQUES

Contrôles	Contraintes	Conformité R31
Abonnement auprès d'un opérateur Qualité de service suffisante (QoS) Adressage des interfaces Paramétrage des paquets de surveillance Sécurité du terminal Choix du mode de transmission et voir la limite de vie de la technologie auprès de l'ARCEP et la FFT	Couverture hertzienne dépendante de l'opérateur (zones blanches) Débit utile 9,05 kb/s (mode CS-1) Incertitude dès 2016 sur la pérennité de la norme du service (évolutions annoncées dans le contexte UMTS) Support lié à l'opérateur et doit être changé en cas de changement d'opérateur Peut tomber en panne	Défaillance du support de transmission = indisponible *La détection et la signalisation de la défaillance apparaissent à la station de télésurveillance en moins de 10 minutes* N * Ts < 10 min : niveau III N * Ts > 10 min : niveau IV ou hors niveau si > 24h

ANALYSE DE RISQUE DU MODE DE TRANSMISSION

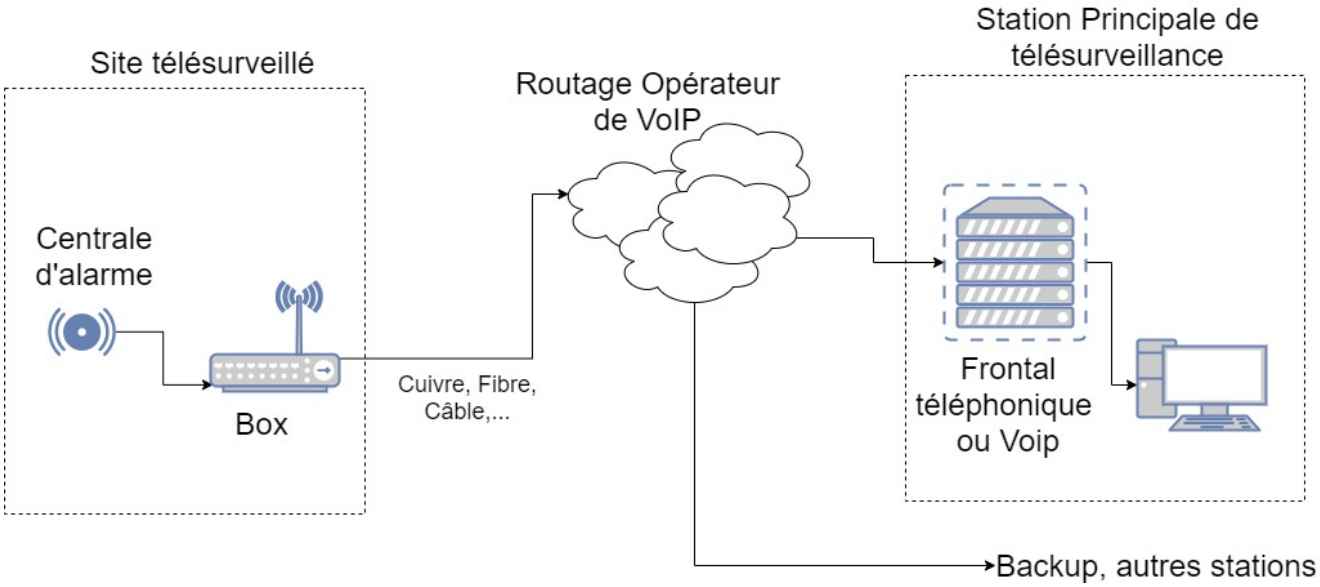
Évènements perturbateurs	Conséquences	Contre-mesures
Foudre	Destruction du transmetteur Destruction des antennes-relais	Antenne intérieure si possible Protections des antennes-relais + redondance de cellules
Défaillance, surcharge ou attaque du réseau de l'opérateur	Indisponibilité, signalée dans un délai < N * Ts	Garantie contractuelle de rétablissement
Perturbations électro-magnétiques, brouillage radio	Indisponibilité signalée dans un délai < N * Ts	Néant
Usurpation d'adresse (La carte SIM n'authentifie pas le réseau)	Indisponibilité, signalée dans un délai < N * Ts	Surveillance possible sur les réseaux 4G et 5G (pas en 3G)
Attaque cyber	Neutralisation des fonctions d'alarmes Prise de contrôle de la centrale	Activation des contrôles (vérification de l'appelant) Utilisation d'une centrale ou d'un transmetteur certifié NF&A2P@

Les centrales d'alarme peuvent :

- Soit être équipées nativement (par exemple les produits radio destinés aux particuliers),
- Soit recevoir une carte interface,
- Soit piloter une passerelle externe, pour les modèles qui ont conservé leur interface RTC.

Les télésurveilleurs connus de CNPP et certifiés sont au niveau, pour gérer cette configuration.

4. VoIP / ADSL ou câble



Paramètres fonctionnels du système de transmission

Tc : période du test cyclique

1h (pratique à vérifier) <Tc < 24h

CARACTERISTIQUES

Contrôles	Contraintes	Conformité R31
Abonnement auprès d'un opérateur Programmation du n° d'appel Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station	Câblage filaire, box éventuellement éloignée Eligibilité ADSL (suivant support) Box compatible DTMF sur VoIP Alimentation de la box externe Bande passante suffisante pour de la voix sur IP Utilise le codec G711 Compatible DTMF RAPIDE Dispositif vulnérable si non protégé Sécurisation de la connectique	Défaillance du support de transmission = indisponible *La détection et la signalisation de la défaillance apparaissent à la station de télésurveillance en moins de 24 heures* Tc < 24h : niveau IV Tc > 24h : hors niveau

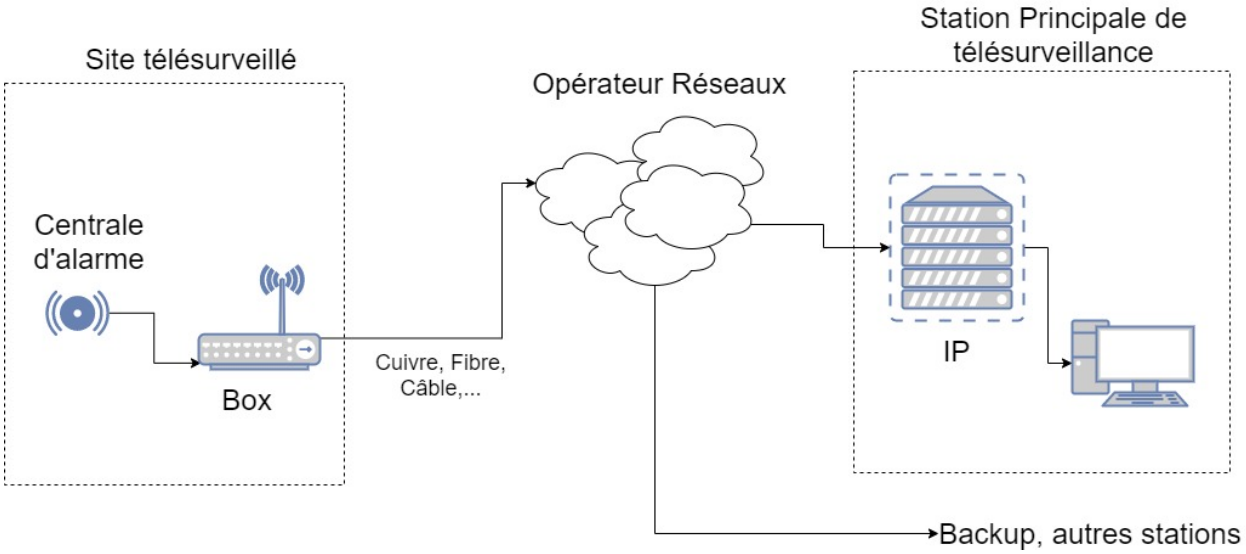
ANALYSE DE RISQUE DU MODE DE TRANSMISSION

Évènements perturbateurs	Conséquences	Contre-mesures
Foudre	Destruction de la box (sauf fibre)	Installation de parafoudres
Coupure du support physique sortant	Indisponibilité, signalée dans un délai < Tc	Dissimulation, protections mécaniques
Coupure secteur sur le site surveillé	Arrêt de la box, indisponibilité signalée dans un délai < Tc	Batterie de secours si la box est de faible consommation Attention aux autonomies
Défaillance, surcharge ou attaque des réseaux	Indisponibilité, signalée dans un délai < Tc	Garantie de rétablissement contractuelle ?
Perturbations électro-magnétiques	Echecs de transmission	Respect des recommandations du constructeur et des règles de l'art concernant l'implantation et le câblage
Connexion frauduleuse Attaque cyber	Prise de contrôle de la centrale Neutralisation des fonctions d'alarmes	Protection contre les appels entrants, contre appel Activation de pare-feu sur la box, proxy inverse
Intervention Operateur mise à jour	Perte de transmission durant la mise à jour et parfois redémarrage	Prévoir un secours

Cette configuration est la plus rapide à mettre en œuvre :

- En raison de la disponibilité, acquise sur le site, d'au moins une ligne dégroupée ou dégroupable.
- Avec la disponibilité annoncée de box compatibles.
- Sans intervention dans la centrale. Seule est à prévoir une alimentation complémentaire.
- Sans autre contrainte pour le télésurveilleur que de présenter une vraie interface VoIP.

5. IP / ADSL (ou câble/ fibre)



Paramètres fonctionnels du système de transmission

Ts : période des tests cycliques. 10s <Ts < 300s.

N : nombre max d'échecs successifs. (De 2 à 5 en pratique)

CARACTERISTIQUES

Contrôles	Contraintes	Conformité R31
Abonnement auprès d'un opérateur Mise en place de l'adressage Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station Paramétrage des accès autorisés	Câblage filaire Eligibilité ADSL (suivant support) Alimentation de la box Bande passante suffisante pour une transmission IP en fonction du protocole ou de la quantité de données nécessaire à transmettre Dispositif vulnérable si non protégé Sécurisation de la connectique	Défaillance du support de transmission = indisponible *La détection et la signalisation de la défaillance apparaissent à la station de télésurveillance en moins de 10 minutes* N * Ts < 10 min : niveau III N * Ts > 10 min : niveau IV ou hors niveau si > 24h

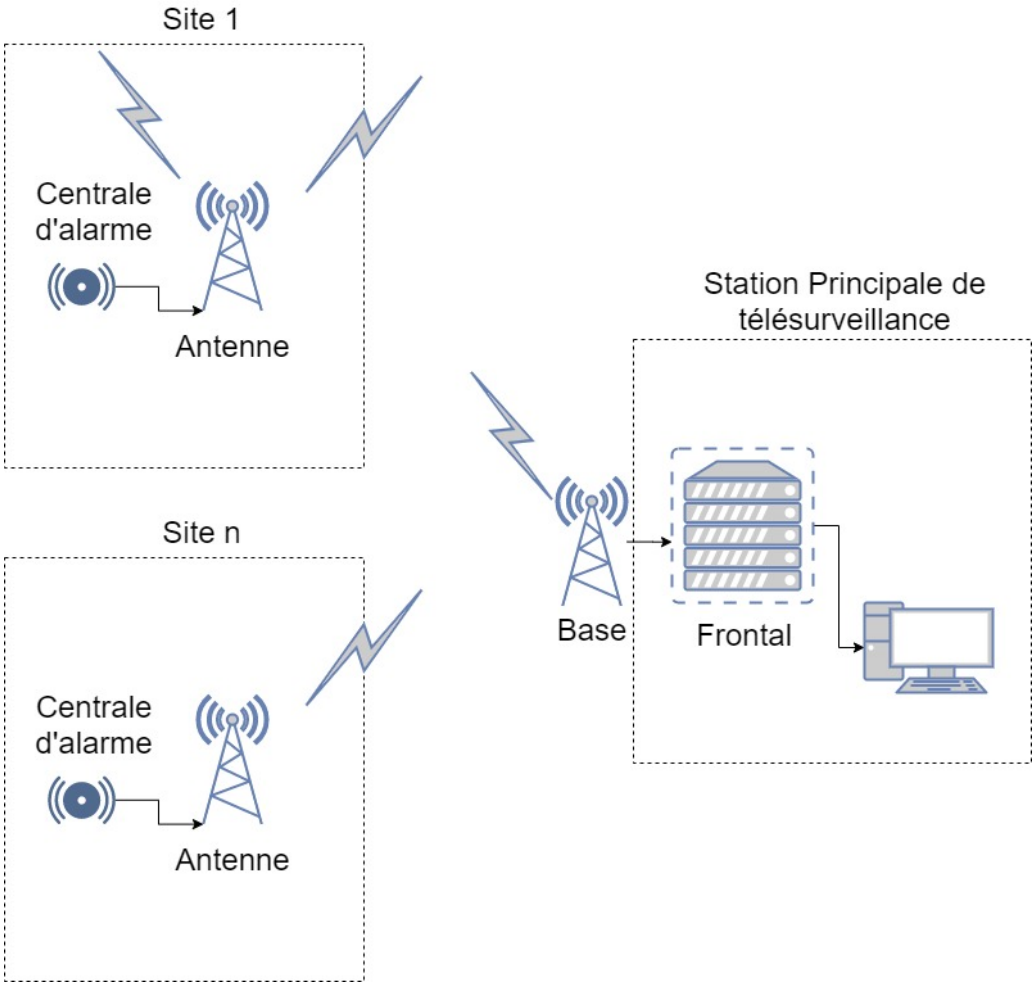
ANALYSE DE RISQUE DU MODE DE TRANSMISSION

Évènements perturbateurs	Conséquences	Contre-mesures
Foudre	Destruction de la box (sauf fibre)	Installation de parafoudres
Coupure du support physique sortant	Indisponibilité, signalée dans un délai < N * Ts	Dissimulation, protections mécaniques
Coupure secteur sur le site surveillé	Arrêt de la box, indisponibilité signalée dans un délai < N*Ts	Batterie de secours si la box est de faible consommation
Coupure secteur dans l'infrastructure réseau	Néant pendant la durée de l'autonomie (> délai réparation)	S/O
Défaillance, surcharge ou attaque des réseaux	Indisponibilité, signalée dans un délai < N * Ts	Garantie de rétablissement contractuelle
Perturbations électro-magnétiques, brouillage radio	Néant	S/O
Attaque cyber	Neutralisation des fonctions d'alarme	Activation de pare-feu sur la box, proxy inverse
Intervention Operateur mise à jour	Perte de transmission durant la mise à jour et parfois redémarrage	Prévoir un secours

Cette fiche s'applique également aux connexions IP sur réseau privé, en écartant ce qui concerne la box et la boucle locale.
Nota : Orange exclut les services de télésurveillance dans les Conditions Générales de ses contrats fibre.

La plupart des centrales d'alarme d'aujourd'hui sont nativement équipées d'une interface IP.
Tous les télésurveilleurs généralistes (connus de, et certifiés par CNPP) sont équipés des frontaux adaptés.
La diffusion de l'ADSL ou de sa version fibre par de nombreux opérateurs permet le raccordement de 100% des sites urbains et périurbains.

6. Balises VHF



Paramètres fonctionnels du système de transmission

Tc : période des tests cycliques.

CARACTERISTIQUES

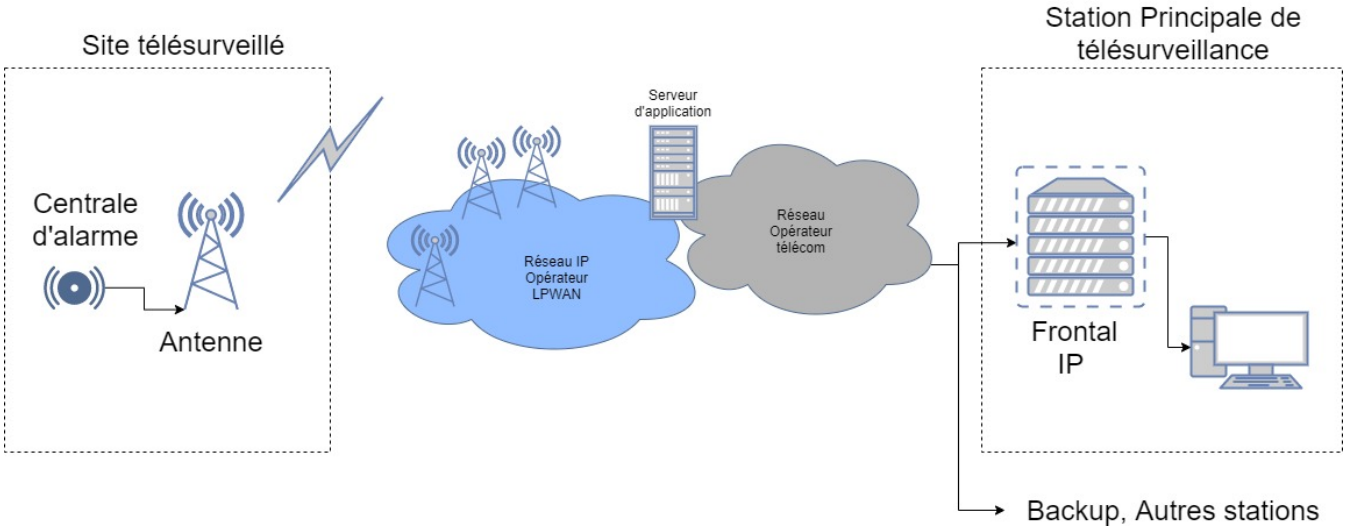
Contrôles	Contraintes	Conformité R31
Programmation des canaux d'appel Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station	Nécessite une licence pour la bande de fréquences Portée d'émission suivant puissance (jusqu'à 10W) Nombre de points très limité	Défaillance du support de transmission = indisponible *La détection et la signalisation de la défaillance apparaissent à la station de télésurveillance en moins de 24 heures* Période Tc<24h : niveau IV Période Tc>24 : hors niveau

ANALYSE DE RISQUE DU MODE DE TRANSMISSION

Évènements perturbateurs	Conséquences	Contre-mesures
Foudre	Destruction des transmetteurs	Antenne intérieure si possible Protection de la station réceptrice
Défaillance d'un relais	Indisponibilité de x balises, signalée dans un délai < Tc	Option de secours GSM ou GPRS
Perturbations électro-magnétiques, brouillage radio	Indisponibilité totale (signalée dans un délai < Tc) ou intermittente (incertain)	Néant
Usurpation de fréquence, substitution	Indisponibilité	- Surveillance par les tests cycliques - Option bi-bande UHF/VHF

Nota : Solution citée pour mémoire ; elle peut rendre service en zone montagneuse ou désertique.

7. Low-Power WAN (IoT)



Paramètres fonctionnels du système de transmission

Tc : période des tests cycliques.

N : nombre max d'échecs successifs

CARACTERISTIQUES

Contrôles	Contraintes	Conformité R31
Abonnement auprès d'un opérateur (cas de SigFox) Volumétrie de message journalier et horaire Programmation du n° d'appel Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station	Zone de couverture (portée d'émission 3 à 15 km) Débit utile faible : 100 b/s (Sigfox) à 1 kb/s (LoraWan) Débit descendant réduit Conçu pour une fréquence d'utilisation basse	Défaillance du support de transmission = indisponible *La détection et la signalisation de la défaillance apparaissent à la station de télésurveillance en moins de 24 heures* Période Tc<24h : niveau IV Période Tc>24 : hors niveau

ANALYSE DE RISQUE DU MODE DE TRANSMISSION

Évènements perturbateurs	Conséquences	Contre-mesures
Défaillance ou surcharge des réseaux	Indisponibilité, signalée dans un délai < période Tc	Garantie de rétablissement
Perturbations électro-magnétiques, brouillage radio	En fonction de la technologie IOT Indisponibilité totale (signalée dans un délai < Tc) ou intermittente (incertain)	Voir CGV et les outils de supervisions proposés par les différents opérateurs
Usurpation de réseau non détectée	Pas d'alarme locale Indisponibilité, signalée dans un délai < Tc	Néant
Attaque cyber au niveau des relais	Pas au niveau du site Au niveau de l'opérateur et de l'infra Indisponibilité, signalée dans un délai < Tc	Stratégies de protection et de récupération Cryptage des communications radio (à rajouter pour Sigfox)

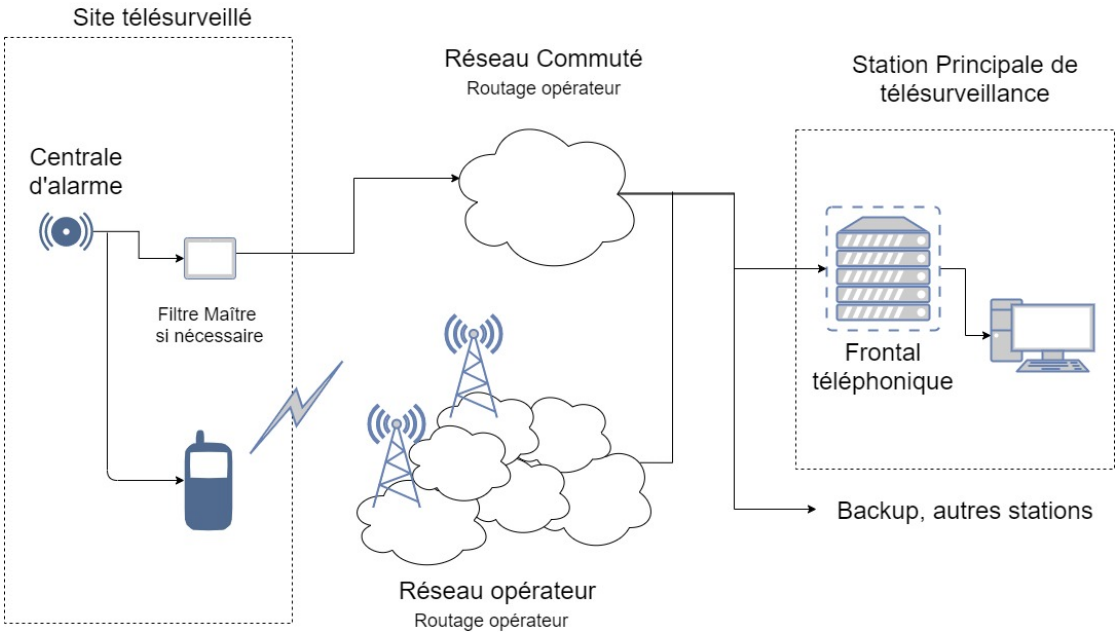
Nota : Cette fiche s'applique à SigFox ou à LoraWan, avec des caractéristiques voisines.

Les réseaux existent depuis plusieurs années, et n'en sont plus au stade expérimental. Les composants de base sont en production industrielle.
Des produits sont à l'étude coté terminal d'alarme, mais la commercialisation n'est pas annoncée.
L'interface banalisée IP n'impose pas de nouvel équipement aux télésurveilleurs, tout au plus auront-ils à s'adapter à de nouveaux protocoles.

Nota : par leur philosophie, ces réseaux confinent les transmissions :

- Dans le niveau IV.
- Sans services complémentaires gourmands en bande passante telles que photo ou vidéo.

8. RTC + secours GSM (canal de communication voix)



Paramètres fonctionnels du système de transmission

Tc1 : période du test cyclique RTC (1h < Tc1 < 24h)
Tc2 : Période du test cyclique GSM (3h < Tc2 <24h)
Tt : temporisation de la détection de défaut (1 à 5 min)
Td : délai de mise à disposition de l'information (R31 Ann. 6)
N : nombre limite de tentatives d'appels sur RTC

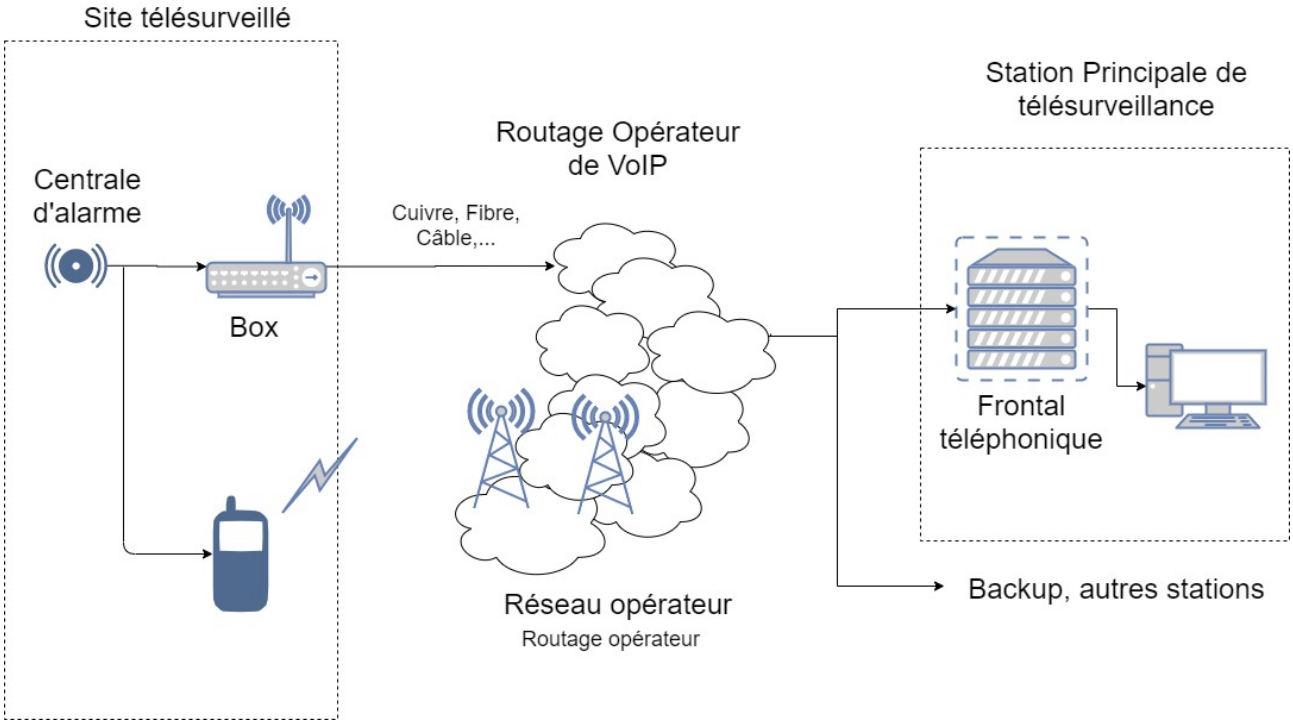
CARACTERISTIQUES

Contrôles	Contraintes	Conformité R31
Ligne téléphonique active et abonnement Connexion sur un autocom à proscrire Câblage maitre (prioritaire sur terminal de paiement, etc.) Programmation du n° d'appel Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station Abonnement auprès d'un opérateur acceptant ce type d'usage	Câblage filaire Fermeture en 2023 du réseau commuté Orange (plus de nouvelles installations depuis le 15 novembre 2018) Débit utile limité Compatibilité du protocole de transmission Couverture dépendante de l'opérateur (zones blanches)	En cas de défaillance de la liaison principale RTC, activation de la liaison secondaire GSM restée disponible *La détection et la signalisation d'une défaillance de la liaison de transmission principale apparaissent à la station de télésurveillance en moins de 10 min* (en pratique, par l'exploitation de la perte du 48V de ligne) par la centrale d'alarme *et* *La détection et la signalisation d'une défaillance de la liaison de transmission secondaire apparaissent à la station de télésurveillance en moins de 24 h* (en pratique, par l'attente des tests cycliques GSM) Pour les tests cycliques voir tableaux en page 9.
Qualité de transmission vocal suffisante Programmation du n° d'appel Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station CGV autorisent mise en place carte sim dans alarme CGV autorisent utilisation de numéro SVA	Débit utile limité (~10 kb/s) Support lié à l'opérateur et doit être changer en cas de changement d'opérateur Le support est un consommable qui peut tomber en panne	

ANALYSE DE RISQUE DU MODE DE TRANSMISSION

Évènements perturbateurs	Conséquences	Contre-mesures
Foudre	Destruction du transmetteur RTC – reprise par le GSM Destruction du transmetteur GSM – reprise par le RTC Destruction des antennes-relais – reprise par le RTC	Installation de parafoudres Antenne intérieure si possible Protections des antennes-relais + redondance de cellules
Rupture physique de la ligne d'abonné	Indisponibilité signalée dans un délai < à 10 min et reprise par la liaison GSM	Dissimulation du cheminement, protection mécanique (vaut également pour transmetteur externe et son antenne)
Défaillance du réseau RTC	Indisponibilité, signalée dans un délai < période Tc1 Les informations sont transmises par la liaison GSM après N tentatives pour établir la liaison RTC (limité par Td)	(Non critique à la première défaillance du système) Garantie contractuelle de rétablissement
Défaillance ou surcharge du réseau de l'opérateur GSM	Indisponibilité non critique, signalée dans un délai < période Tc2	Garantie de rétablissement de l'opérateur (hors cas force majeure)
Perturbations électro-magnétiques, brouillage radio	Non critique : Indisponibilité du secours, permanente (signalée dans un délai < période Tc2), ou intermittente (incertain)	Néant
Usurpation de réseau (La carte SIM n'authentifie pas le réseau)	Non critique : Indisponibilité, signalée dans un délai < période Tc2	Néant
Attaque cyber	Neutralisation des fonctions d'alarmes	Protection contre les appels entrants Utilisation de matériels certifiés NF&A2P@ Télémaintenance via un seul des deux canaux

9. VoIP + secours GSM (canal de communication voix)



Paramètres fonctionnels du système de transmission

Tc1 : période du test cyclique RTC (1h < Tc1 < 24h)

Tc2 : Période du test cyclique GSM (3h < Tc2 <24h)

Tt : temporisation de la détection de défaut (1 à 5 min)

Td: délai de mise à disposition de l'information (R31 Ann. 6)

N : nombre limite de tentatives d'appels sur VoIP

CARACTERISTIQUES

Contrôles	Contraintes	Conformité R31
Abonnement auprès d'un opérateur Programmation du n° d'appel Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station Abonnement auprès d'un opérateur acceptant ce type d'usage Qualité de transmission vocal suffisante Programmation du n° d'appel Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station CGV autorisent mise en place carte sim dans alarme CGV autorisent utilisation de numéro SVA	Câblage filaire, box éventuellement éloignée Eligibilité ADSL (suivant support) Box compatible DTMF sur VoIP Alimentation de la box externe Bande passante suffisante pour de la voix sur IP Utilise le codec G711 Compatible DTMF RAPIDE Dispositif vulnérable si non protégé Sécurisation de la connectique Compatibilité du protocole de transmission Couverture dépendante de l'opérateur (zones blanches) Débit utile limité (~10 kb/s)	En cas de défaillance de la liaison principale box, activation de la liaison secondaire GSM restée disponible *La détection et la signalisation d'une défaillance de la liaison de transmission principale apparaissent à la station de télésurveillance en moins de 10 min* (en pratique, par l'exploitation d'un signal VoIP KO) *et* *La détection et la signalisation d'une défaillance de la liaison de transmission secondaire apparaissent à la station de télésurveillance en moins de 24 h* (en pratique, par l'attente des tests cycliques GSM) Pour les tests cycliques voir tableaux en page 9.

	Support lié à l'opérateur et doit être changer en cas de changement d'opérateur Le support est un consommable qui peut tomber en panne	

ANALYSE DE RISQUE DU MODE DE TRANSMISSION

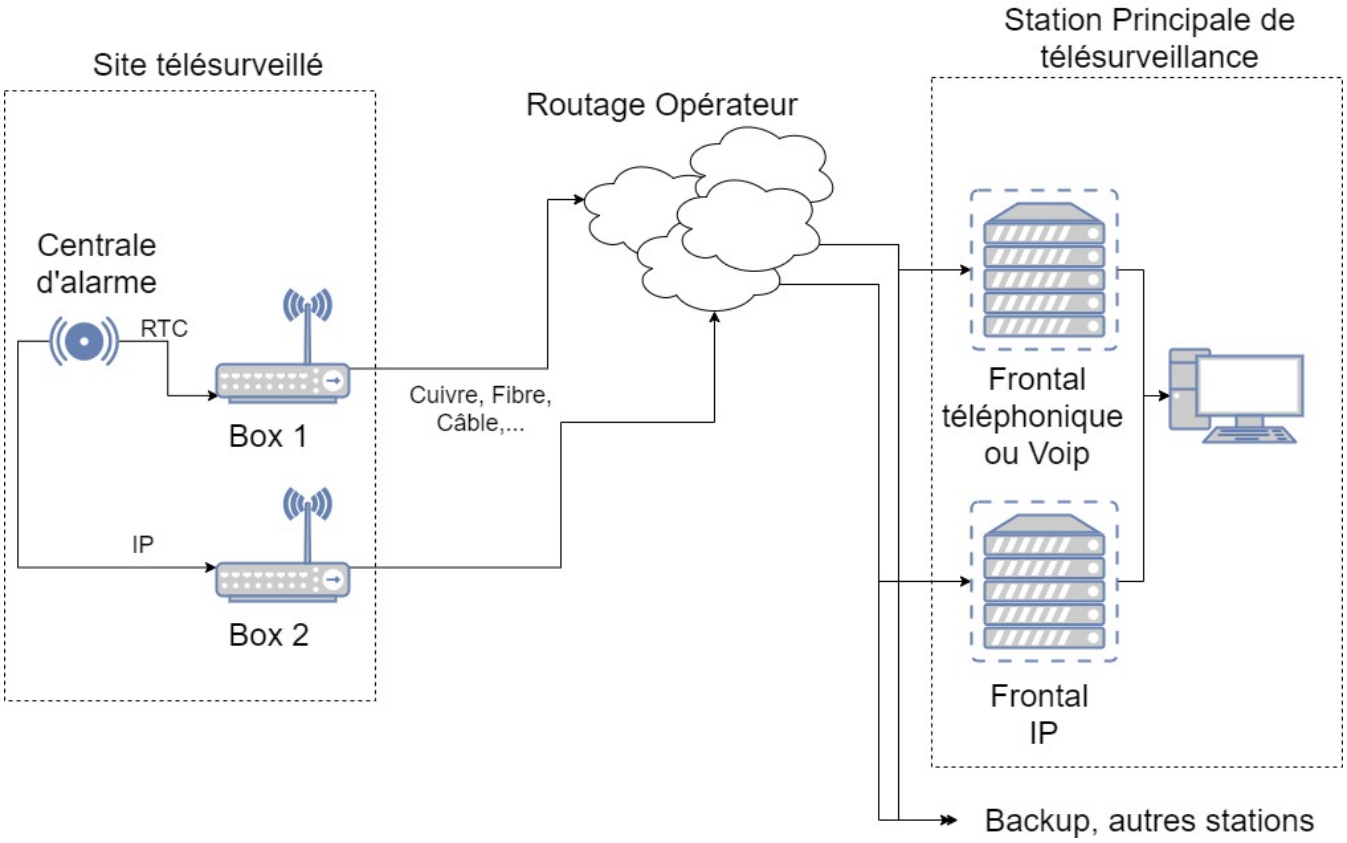
Évènements perturbateurs	Conséquences	Contre-mesures
Foudre	Destruction de la box – reprise par le GSM Destruction du transmetteur GSM – reprise par la box Destruction des antennes-relais – reprise par la liaison box	Installation de parafoudres Antenne intérieure si possible Protections des antennes-relais + redondance de cellules
Coupure secteur sur le site surveillé	- Néant jusqu'à la fin de l'autonomie si la box est alimentée par la centrale (36h si conforme R81) - Arrêt de la box si non alimentée (et report sur le GSM) La coupure est signalée localement + en option à distance	Néant
Rupture physique de la ligne ADSL (ou câble ou fibre)	Indisponibilité signalée dans un délai < à 10 min et reprise par la liaison GSM	Dissimulation du cheminement, protection mécanique (vaut également pour transmetteur externe et son antenne)
Défaillance du réseau VoIP	Indisponibilité, signalée dans un délai < période Tc1 Les informations sont transmises par la liaison GSM après N tentatives pour établir la liaison primaire (limité par Td)	(Non critique à la première défaillance du système) Garantie contractuelle de rétablissement
Défaillance ou surcharge du réseau de l'opérateur GSM	Non critique : Indisponibilité, signalée dans un délai < période Tc2	Garantie de rétablissement de l'opérateur (hors cas force majeure)
Perturbations électro-magnétiques, brouillage radio	Non critique : Indisponibilité permanente du secours (signalée dans un délai < période Tc2), ou intermittente (incertain)	Néant
Usurpation de réseau (La carte SIM n'authentifie pas le réseau)	Non critique : Indisponibilité, signalée dans un délai < période Tc2	Néant
Attaque cyber	Prise de contrôle de la centrale Neutralisation des fonctions d'alarmes	Protection contre les connexions entrantes Pare-feu de la box, proxy inverse Utilisation de matériels certifiés NF&A2P@ Télémaintenance via un seul des deux canaux

Sans changer la logique de fonctionnement, le niveau de transmission II peut être conservé à condition de disposer localement de la détection de défaut de connectivité VoIP :

- Pour les transmetteurs GSM de type « passerelle » (émulation de ligne RTC), la box VoIP doit reproduire l'absence de tension de ligne. A défaut, une programmation de la centrale et l'activation d'une sortie sont nécessaires. Mais dans les meilleurs cas, les box actuelles ne donnent à exploiter qu'un voyant lumineux, ou un diagnostic sur leur interface HTTP.
- Pour un transmetteur GSM intégré à la centrale, les mêmes considérations s'appliquent.
- Même besoin encore pour les relais GSM externes à la centrale, à qui il revient de transmettre l'alarme de défaut ligne présentée sur l'une des entrées.

A terme, il y aura confusion entre le point d'entrée de la voie VoIP et le point d'entrée de la voie GSM au niveau de la station de télésurveillance, qu'il s'agisse d'une passerelle T2 ou d'un accès direct VoIP.
Jusqu'ici la conservation du niveau II (deux supports distincts) était assurée par la séparation des réseaux d'opérateurs (relativement facile à identifier) et/ou par l'existence d'une destination backup (qu'elle soit reroutée par un traducteur, ou qu'elle soit adressée en repli dès l'émission). La notion de séparation des réseaux devra être remplacée par une notion de redondance du système de réseaux par rapport au(x) point(s) de destination : à tout instant il ne doit exister aucun nœud critique, à moins qu'un tel évènement ne soit signalé dans un certain délai et dûment tracé.

10.IP + secours VoIP



Paramètres fonctionnels du système de transmission

Tc1 : période du test IP (10s < Tc1 < 300 s)

Tc2 : Période du test cyclique VoIP (1h < Tc2 <24h)

N : nombre de confirmation du test IP

CARACTERISTIQUES

Contrôles	Contraintes	Conformité R31
Abonnement auprès d'un opérateur Mise en place de l'adressage Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station Paramétrage des accès autorisés Abonnement auprès d'un opérateur Programmation du n° d'appel Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station	Câblage filaire Eligibilité ADSL (suivant support) Alimentation de la box Bande passante suffisante pour une transmission IP en fonction du protocol ou de la quantité de données nécessaire à transmettre Dispositif vulnérable si non protégé Sécurisation de la connectique Câblage filaire, box éventuellement éloignée Eligibilité ADSL (suivant support) Box compatible DTMF sur VoIP Alimentation de la box externe Bande passante suffisante pour de la voix sur IP Utilise le codec G711 Compatible DTMF RAPIDE	En cas de défaillance de la liaison principale box 1, activation de la liaison VoIP secondaire restée disponible *La détection et la signalisation d'une défaillance de la liaison de transmission principale apparaissent à la station de télésurveillance en moins de 10 min* (en pratique, par l'absence répétée de tests IP) *et* *La détection et la signalisation d'une défaillance de la liaison de transmission secondaire apparaissent à la station de télésurveillance en moins de 24 h* (en pratique, par l'attente du test cyclique VoIP)

	Dispositif vulnérable si non protégé Sécurisation de la connectique	Pour les tests cycliques voir tableaux en page 9. Possibilité de niveau I si le signal "VoIP KO" est disponible et peut être transmis en moins de 10 min

ANALYSE DE RISQUE DU MODE DE TRANSMISSION

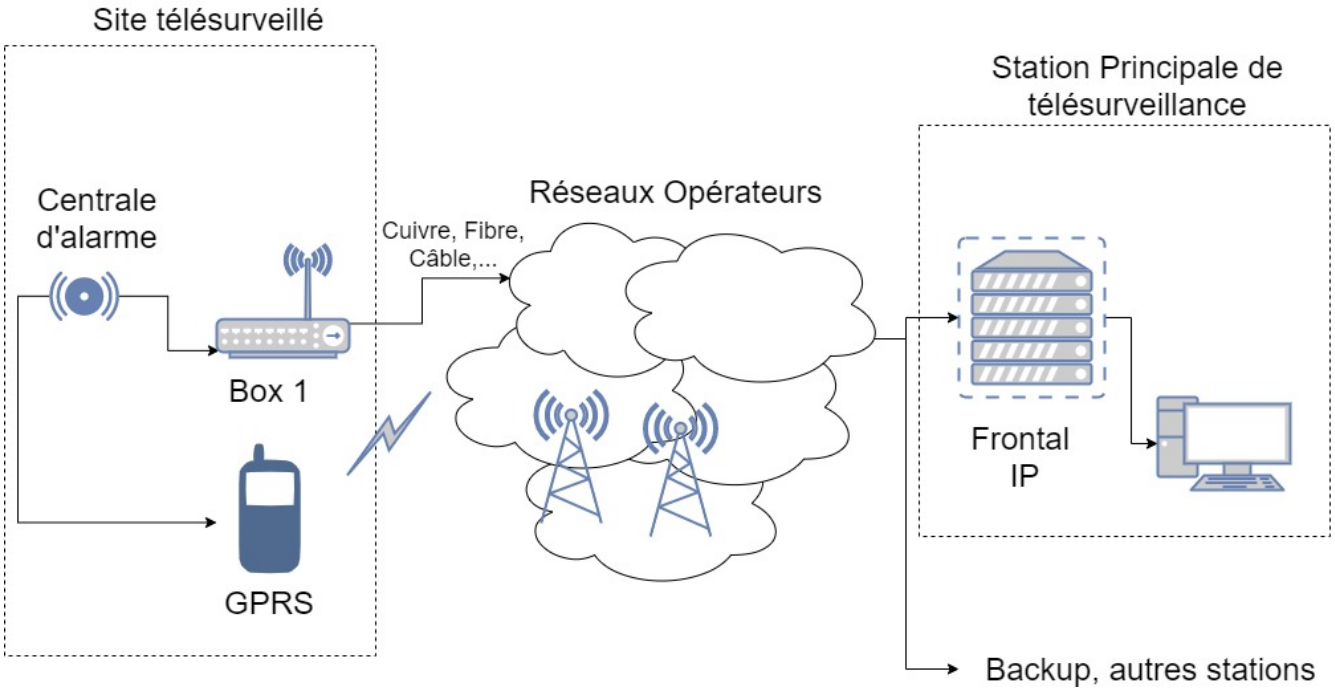
Évènements perturbateurs	Conséquences	Contre-mesures
Foudre	Destruction d'une box = reprise par l'autre Destruction des deux box = indisponibilité signalée	Installation de parafoudres
Coupure secteur sur le site surveillé	- Néant jusqu'à la fin de l'autonomie si les box sont alimentées par la centrale d'alarme (alimentation) (36h si conforme au référentiel APSAD R81 Détection d'intrusion – Règle d'installation) - Arrêt des box si non alimentées L'indisponibilité est signalée dans le délai N*Tc1	Néant
Rupture physique de la ligne ADSL (ou câble ou fibre) IP	Non critique : Coupure de la voie IP signalée, reprise par la voie VoIP	Dissimulation du cheminement, protection mécanique
Rupture physique de la ligne dédiée à la VoIP	Non critique : Retour de la liaison IP au niveau III, détection < Tc2	Dissimulation du cheminement, protection mécanique
Défaillance ou surcharge du réseau de l'opérateur IP	Non critique Indisponibilité, signalée dans un délai < N*Tc1	Garantie de rétablissement de l'opérateur (hors cas force majeure)
Défaillance du réseau VoIP	Non critique : Indisponibilité du secours, signalée dans un délai < Tc2	Garantie de rétablissement de l'opérateur (hors cas force majeure)
Perturbations électro-magnétiques	Néant ou incidence faible	S/O
Attaque cyber sur les réseaux	Non critique à la première attaque (Voir défaillances réseau)	Protections à jour
Connexion frauduleuse Attaque cyber sur les box	Prise de contrôle de la centrale, neutralisation	Protection contre les connexions entrantes en VoIP Activation de pare-feu, proxy inverse Utilisation de matériels certifiés NF&A2P@ Télémaintenance ouverte sur un seul des deux canaux

Cette solution pourra remplacer les installations existantes IP + secours RTC.

Pour que la transmission reste de niveau II, il faut que le réseau support du service VoIP soit distinct du réseau IP accessible, c'est-à-dire pas sur la même box.

Il ne doit pas non plus y avoir confusion des réseaux de transport jusqu'aux frontaux de la station, à moins que la redondance interne puisse être vérifiée comme équivalente à deux réseaux distincts.
Les conditions précisées au §2 s'appliquent pour la voie VoIP.

11.IP + secours data mobile (GPRS / 3G/4G/5G)



Paramètres fonctionnels du système de transmission

Tc1 : période du test IP (10s < Tc1 < 300 s)

Tc2 : Période du test GPRS (10s < Tc2 <24h)

N : nombre de confirmations du test IP

M : nombre de confirmations du test GPRS

CARACTERISTIQUES

Contrôles	Contraintes	Conformité R31
Abonnement auprès d'un opérateur Mise en place de l'adressage Paramétrage des tests cycliques Émission d'un test manuel et acquittement par la station Paramétrage des accès autorisés Abonnement auprès d'un opérateur Qualité de service suffisante (QoS) Adressage des interfaces Paramétrage des paquets de surveillance Sécurité du terminal Choix du mode de transmission et voir la limite de vie de la technologie auprès de l'ARCEP et la FFT	Câblage filaire Eligibilité ADSL (suivant support) Alimentation de la box Bande passante suffisante pour une transmission IP en fonction du protocole ou de la quantité de données nécessaire à transmettre Dispositif vulnérable si non protégé Sécurisation de la connectique Couverture hertzienne dépendante de l'opérateur (zones blanches) Débit utile 9,05 kb/s (mode CS-1) Incertitude dès 2016 sur la pérennité de la norme du service (évolutions annoncées dans le contexte UMTS)	En cas de défaillance de la liaison principale box, activation de la liaison GPRS secondaire restée disponible *La détection et la signalisation d'une défaillance de la liaison de transmission principale apparaissent à la station de télésurveillance en moins de 10 min* (en pratique, par l'absence répétée des tests IP) *et* *La détection et la signalisation d'une défaillance de la liaison de transmission secondaire apparaissent à la station de télésurveillance en moins de 24 h* (en pratique, par l'attente des tests cycliques GPRS) Pour les tests cycliques voir tableaux en page 9.

	Support lié à l'opérateur et doit être changé en cas de changement d'opérateur	(Autre possibilité de niveau I si le le GPRS gère un "défaut")

ANALYSE DE RISQUE DU MODE DE TRANSMISSION

Évènements perturbateurs	Conséquences	Contre-mesures
Foudre	Destruction de la box = repris sur GPRS // + Destruction GPRS = indisponibilité signalée	Installation de parafoudres
Destruction d'une antenne relais GPRS	Non critique : Retour de la liaison IP au niveau III, détection < M*Tc2	Accessibilité de plusieurs relais
Coupure secteur sur le site surveillé	- Néant jusqu'à la fin de l'autonomie si les box sont alimentées par la centrale d'alarme (36h si conforme au référentiel APSAD R81 Détection d'intrusion – Règle d'installation) - Arrêt de la box si non alimentée L'indisponibilité est signalée dans le délai N*Tc1	Néant
Rupture physique du support IP (ADSL, fibre ou câble)	Non critique : Coupure de la voie IP signalée, reprise par la voie GPRS	Dissimulation du cheminement, protection mécanique
Défaillance ou surcharge du réseau de l'opérateur IP	Non critique Indisponibilité, signalée dans un délai < N*Tc1	Garantie de rétablissement de l'opérateur (hors cas force majeure)
Défaillance du réseau GPRS	Non critique : Indisponibilité du secours, signalée dans un délai < M*Tc2	Garantie de rétablissement de l'opérateur (hors cas force majeure)
Perturbations électro-magnétiques	Non critique : Retour de la liaison IP au niveau III, détection < M*Tc2	Néant
Attaque cyber sur les réseaux	Non critique à la première attaque (Voir défaillances réseau)	Protections à jour
Attaque cyber sur la box ou la centrale d'alarme	Prise de contrôle, neutralisation	Protections pare-feu, proxy inverse Utilisation de matériels certifiés NF&A2P@ Télémaintenance ouverte sur un seul des deux canaux

Cette fiche est applicable à une configuration IP+IP, avec deux box.

Annexes

Annexe 1 : Glossaire général

ADSL
(Asymmetric Digital Subscriber Line)
Méthode de codage numérique, utilisable sur les paires de cuivre qui desservent les abonnés au téléphone dans un rayon de 3km environ à partir du NRA (Nœud de Raccordement d'Abonné, dans la terminologie de France Télécom).
Cette technologie et ses évolutions (ADSL2) tendent à céder la place au raccordement en fibre optique.

ARCEP
Autorité de Régulation des Communications Electroniques et des Postes
https://www.arcep.fr

Box n-play
Boitier d'interface (modem-routeur) distribuant chez l'abonné les différents services de l'opérateur :

- Connexion internet
- Télévision directe ou à la demande
- Téléphonie en *VoIP*

Certification @
Cette certification délivrée par le CNPP distingue les produits certifiés pour leurs caractéristiques de cybersécurité (Plus d'information sur https://www.cnpp.com).

Disponibilité
Mesure de performance en % d'un équipement ou d'un système, idéalement 100%.
Rapport de la durée de fonctionnement non dégradé comparé à la durée de besoin de ladite fonction.
Ce chiffre est lié, par exemple, pour les machines aux notions de MTTF, MTBF, MTTR et de taux de défaillance.

FAI
Un Fournisseur d'Accès à Internet ou FAI est un organisme offrant une connexion à Internet, le réseau informatique mondial.

GPRS
General Packet Radio Service
Protocole dérivé du GSM, permettent un débit de données supérieur, parfois dénommé 2,5G.
L'innovation majeure est la transmission des données par paquets, qui permet d'obtenir une connectivité continue du point de vue réseau, émis en n'allouant les ressources radio qu'à la demande.

GTR
Garantie de Temps de Rétablissement : délai contractuel dans lequel le service doit être rétabli.
Il diffère de la GTI, qui s'arrête au délai de l'intervention corrective.
Ne pas confondre avec le MTTR (Mean Time To Recovery), délai probable ou statistiquement constaté.

IP
Internet Protocol
Protocole offrant un service d'adressage unique pour les terminaux raccordés à la même infrastructure réseau. Ce protocole seul n'assure pas l'intégrité des données transmises, il est nécessaire de faire appel pour cela à des protocoles complémentaires de niveau supérieur.
Souvent employé comme raccourci de TCP/IP, qui en est la réalisation pratique sur les réseaux de type internet.

KO
Autre notation de NOK (non-OK).

LAN
Local Area Network
Réseau local, limité à une zone restreinte, ou à un seul utilisateur, ou de faible portée radio.

LPWAN
Low Power *WAN*
Désigne un réseau étendu de type hertzien, optimisé pour un grand nombre de terminaux.

- Peu gourmands en énergie
- N'émettant que peu de données chacun (faible bande passante)

Les plus connus sont LoRaWAN et Sigfox, développés pour l'internet des objets.

Niveau de transmission
Classement conventionnel des moyens de transmission de données, combinant les performances (décroissantes de I à IV) de délai de traversée et de *disponibilité* (voir définition).

Pare-feu (Firewall, packet filter)
Forme de proxy, filtrant au niveau de la couche réseau.
Le plus souvent mis en place sous forme de composant logiciel, il bloque les paquets de données en fonction :

- de leur origine et/ou de leur destination (adresses IP, ports) ;
- d'autres caractéristiques : taille des données, validité, conformité à un protocole, cohérence des échanges.

Le principe dit « de moindre privilège » consiste à interdire tout ce qui n'est pas autorisé. Un pare-feu fonctionne avec des listes explicites d'accès autorisés.
Les box des opérateurs contiennent en général un pare-feu. Il n'est pas toujours re-paramétrable à un besoin spécifique.

Passerelle
(Eng. Gateway)
En matière d'échange de données, désigne un dispositif permettant d'établir la communication entre deux réseaux de type différent, ou de deux protocoles différents de même niveau.
Une passerelle peut être matérielle ou logicielle.
Exemple : la box reliant internet au réseau local est une passerelle.

Protocole
Ensemble de règles régissant l'établissement de communication entre machines et les échanges de données.
Par extension et improprement, peut aussi désigner la structure et les détails du codage des données (comme c'est le cas pour les codes d'alarme exploités par les télésurveilleurs).

Proxy
Un serveur proxy est une machine qui se substitue à toutes les machines que le sous-réseau local (ici un terminal ou une centrale d'alarme) est susceptible d'adresser.

- Elle peut filtrer à plusieurs niveaux (y compris applicatif) ce qui transite par son intermédiaire.
- Elle peut masquer les informations d'identité du terminal en y substituant d'autres, voire même aucune.

(La fonction de cache souvent associée au proxy n'a pas d'intérêt dans une application d'alarme).

Proxy inverse (reverse proxy)
Machine qui se substitue au réseau local (ici un terminal ou une centrale d'alarme) vis-à-vis de l'extérieur.
Elle intercepte toutes les requêtes venant de l'extérieur et leur applique des règles.
Elle peut porter un encodage et filtrer les contenus.

Redondance

Technique destinée à accroitre la *disponibilité* (voir définition).

- Mise en place de deux ou plusieurs dispositifs ou systèmes susceptibles de réaliser la même fonction, afin de faire face aux pannes de l'un d'entre eux.
- Codage redondant : codage intégrant la répétition des informations (sous des formes éventuellement différentes) de manière à permettre la correction d'erreurs.

RNIS (Eng. ISDN)

Réseau Numérique à Intégration de Services (ou commercialement "Numéris").

Connexion agrégeant plusieurs canaux logiques sur le même support, en pratique jusqu'à 2 Mb/s en bande de base.

Ex : L'accès primaire T2 offre 30 canaux numériques à 64kbps.

RTC

Réseau Téléphonique Commuté.

Cela correspond à la téléphonie historique.

SIP

Session Initiation Protocol

Protocole de signalisation permettant l'établissement et la libération de sessions multimédia. Il ne s'applique pas seulement à la VoIP.

Ce protocole est la référence pour l'interconnexion des différents réseaux de téléphonie.

SVA

Ces numéros à 10, 6 ou 4 chiffres permettant d'accéder à un service lors d'un appel téléphonique, qu'ils soient désignés communément numéros "spéciaux" ou "surtaxés" (même si le service lié au numéro n'est pas toujours facturé) sont des numéros de **S**ervices à **V**aleur **A**joutée (numéro SVA).

VoIP

Voice over IP, littéralement voix sur IP.

Technologie consistant à numériser les fréquences vocales, et à transmettre les paquets de données correspondant sur un réseau IP, moyennant un protocole supplémentaire assurant que tous les paquets sont reçus dans l'ordre et sans perte.

La mesure subjective des résultats par des groupes de population privilégie le codage nommé G711.

L'exemple bien connu de ce service est Skype.

Cette technique est déjà répandue dans les réseaux d'entreprise.

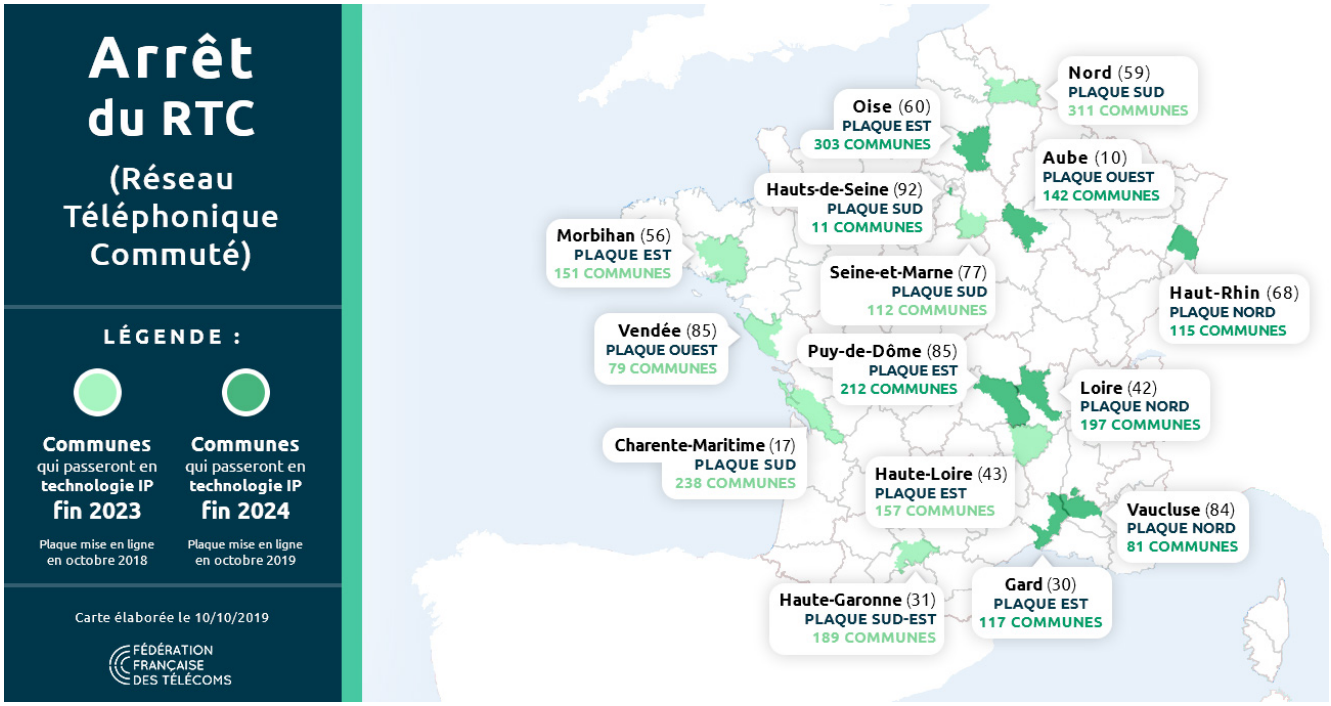
Elle est disponible sur les box internet des opérateurs, interfacée avec les autres réseaux existants.

WAN

Wide Area Network (littéralement : réseau étendu)

Désigne un réseau couvrant une vaste zone géographique, jusqu'à la terre entière (peu importe les technologies mises en œuvre).

Annexe 2 : Plaques arrêtées par France Télécom



(Source F.F.T)

Plus de détails sur https://www.fftelecoms.org

Annexe 3 : Zones Blanches

La cartographie est en évolution permanente.
Des informations détaillées avec leur date d'actualisation sont disponibles sur ces sites web :

- L'observatoire trimestriel et les publications de l'Arcep :

https://www.arcep.fr/la-regulation/grands-dossiers-reseaux-mobiles/la-couverture-mobile-en-metropole.html

- Le site dédié https://www.monreseaumobile.fr/
- Le service public https://www.data.gouv.fr/fr/datasets/monreseaumobile/

Annexe 4 : Risque de foudre - Zones kérauniques

Météo-France ne publie pas directement de données consolidées sur son site. Pour une actualité 2018 voir :http://www.meteofrance.fr/actualites/69551975-2018-annee-la-plus-foudroyee-depuis-30-ans
Le site dédié est : https://www.meteorage.com/fr/ressources/carte-interactive-gratuite.

Le niveau kéraunique (noté Nk) est le nombre de jours d'orages par an dans une zone donnée.
De manière plus précise la densité de foudroiement (notée Ng) indique le nombre d'impacts de foudre par km² et par an dans une zone donnée. On estime empiriquement que Ng ≈ Nk/10.

Ce Guide a été réalisé en partenariat entre

Et

Contacts :

CNPP https://www.cnpp.com/

ADMS adms.adms@sfr.fr https://adms-france.fr/