ECA
Prévenir Secourir Assurer

Alarmes automatiques

Règle de prescription pour la transmission sécurisée d'alarmes sur IP

Etablissement Cantonal d'Assurance, Division Prévention
Av. du Grey 111 - 1002 Lausanne - Téléphone +41 58 721 21 21 | prevention@eca-vaud.ch | www.eca-vaud.ch

Edition :

Etablissement cantonal d'assurance contre l'incendie et les éléments naturels du Canton de Vaud
Division Prévention
Av. du Grey 111
1002 Lausanne
+41 58 721 21 21
prevention@eca-vaud.ch
Décembre 2009

Etablissement cantonal d'assurance contre
l'incendie et les éléments naturels du canton de Vaud

Police cantonale Fribourg

Règle de prescription
pour la transmission sécurisée d'alarmes sur IP

Cette règle de prescription est principalement basée sur les Normes Européennes EN 50136-x-x et EN 50131-x-x (y compris leurs annexes), les directives techniques SES, les références normatives de l'AEAI, la règle de prescription R31 et le standard ANSI/SIA DC-09:2007.

Elle s'applique aux transmissions d'alarmes pompiers vers des centres de réception officiels et peut, par analogie, s'appliquer également à la transmission de tout type d'alarmes (police, techniques) vers des centres de réception officiels ou non.

Ces spécifications sont appliquées par les centres officiels de traitement d'alarmes suivants:

VD	CTA – 118
FR	CEA – 112 – 117 – 118

Version 1.5 – Décembre 2009

Cette version remplace et annule toutes les précédentes.

Sommaire

1 Domaine d'application

Cette règle de prescription, basée sur les Normes Européennes EN 50136-x-x et EN 50131-x-x (et leurs annexes), les directives techniques SES, le standard ANSI/SIA DC-09:2007 et la règle de prescription R31, s'applique aux transmissions d'alarmes pompiers (incendie, inondation, gaz, etc.) vers des centres de réception officiels et peut, par analogie, s'appliquer à la transmission de tout type d'alarmes (intrusion, contrôle d'accès, agression, etc.) vers des centres de réception, officiels ou non. Elle décrit les exigences techniques spécifiques permettant de communiquer entre une centrale d'alarme domestique et un centre de réception officiel.

Différents systèmes d'alarme peuvent délivrer, outre des messages d'alarme, d'autres types de messages tels que des messages d'état ou de dérangement. Ces messages sont considérés au même titre que les messages d'alarme. Le terme d'alarme est ainsi utilisé dans l'ensemble de ce document dans cette large interprétation. Dans ce sens, le transmetteur d'alarme devrait être multi-usage.

Des exigences supplémentaires relatives aux types spécifiques de systèmes de transmission d'alarmes sont indiquées dans des parties distinctes de cette norme. Ceci n'empêche pas l'utilisation d'un quelconque système de transmission d'alarmes non couvert par l'une de ces parties spécifiques, sous réserve qu'il satisfasse aux exigences générales.

2 Références normatives

Cette règle de prescription comporte des dispositions d'autres publications, par référence datée ou non datée. Ces références normatives sont citées aux endroits appropriés dans le texte et les publications sont énumérées ci-après.

Publication	Titre
EN 50136-x-x	Systèmes d'alarme – Systèmes et équipements de transmission d'alarme
EN 50131-x-x	Systèmes d'alarme – Systèmes d'alarme intrusion et hold-up
APSAD R31	Règle de prescription – Télésurveillance
AEAI	Prescriptions de protection incendie – Association des Etablissements d'Assurance Incendie
Directives SES	Directives techniques de l'Association Suisse des Constructeurs de Systèmes de Sécurité pour les installations de détection incendie
I&HAS (ex-IALA)	Prescriptions pour installations d'alarme effraction et agression – selon Institut Suisse de Promotion de la Sécurité
C-ESéc	Concordat sur les entreprises de sécurité – Règles régissant l'activité des entreprises de sécurité
ANSI/SIA DC-09:2007	Security Industry Association – SIA Digital Communication Standard – Internet Protocol Event Reporting
ISO 27001:2005	Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences
ISO 27002:2007	Technologie de l'information – Code de bonne pratique pour la gestion de la sécurité de l'information
ITU-T X.1051	Information Security Management – Requirements for Telecommunications (ISMS-T)
DETEC/OFCOM	Lignes directrices relatives à la sécurité et à la disponibilité des infrastructures et des services de télécommunication
VdS 2153	Richtlinien für die Anerkennung von Wach- und Sicherheitsunternehmen – Notruf- und Service-Leitstellen (NSL)

3 Objet

Cette règle de prescription a pour objet de stipuler les exigences générales relatives aux caractéristiques de fonctionnement, de fiabilité et de sécurité des transmetteurs (émetteurs-récepteurs) d'alarmes et de garantir leur aptitude à être utilisés avec différents systèmes et équipements de transmission et de traitement de critères d'alarmes.

4 Définitions

4.1 Alarme

Situation issue de l'activation d'un ou plusieurs détecteur(s) des installations du site surveillé, suite à la survenance d'un événement que ces installations ont pour mission de signaler.

4.2 Auto surveillance

Fonction propre aux installations de détection d'intrusion. Celles-ci assurent alors la surveillance de leurs propres éléments, ainsi que de leurs liaisons, et signalent ainsi toute manœuvre (malveillante ou non) susceptible de nuire à leur fonctionnement. Critère: sabotage.

4.3 Centrale d'alarme (domestique)

Système assurant la collecte centralisée d'événements signalés par des systèmes de détection spécifiques (détecteurs incendie, gaz, contrôle d'accès, inondation, etc.) dans un bâtiment d'entreprise ou chez un particulier.

4.4 Centre de réception et/ou de traitement d'alarmes

Centre assurant la prestation contractuelle (réception et/ou traitement des alarmes) en mode de fonctionnement normal ou dégradé. Peut être **officiel** (soit légalement mandaté par l'Autorité Compétente) ou non.

4.5 Centre de télésurveillance et/ou de transit

Centre situé à distance du site surveillé dans lequel l'information concernée par l'état d'une ou plusieurs centrale(s) d'alarme domestique(s) (chez le client) est recueillie soit pour un report (c'est-à-dire un centre de réception d'alarmes), soit pour poursuivre la transmission.

4.6 Communication

Transmission d'un message entre une centrale d'alarme (côté client) et un centre de traitement des alarmes par l'intermédiaire d'une voie de transmission. Les messages d'alarme sont prioritaires par rapport aux autres informations.

4.7 Dérangement

Fonction propre aux installations de détection de critères pompiers ou police ou aux installations techniques. Celles-ci assurent alors la surveillance de leurs propres éléments et de leurs liaisons et signalent l'apparition d'une anomalie. Critère: dérangement / technique.

4.8 Installations homologuées

Par installation homologuée au niveau feu, il est entendu une installation conforme aux normes et directives de l'AEAI (Association des Etablissements d'Assurance Incendie).

Par installation homologuée au niveau des critères police, il est entendu une installation conforme aux recommandations pour la classification des risques de l'I&HAS (ex-IALA), selon l'Institut Suisse de Promotion de la Sécurité (Organisme pour la protection intrusion - FFIS).

4.9 Levée de doute

Notion différente si appliquée aux alarmes pompiers ou police. Elle considère aussi bien les aspects techniques qu'organisationnels (ressources humaines); cette levée de doute consiste à effectuer un premier contrôle de l'alarme reçue et, si l'alarme est confirmée, permet d'engager des ressources et des moyens adaptés à la situation.

4.10 Liaison de sécurité d'un centre de traitement d'alarmes officiel

Liaison prévue entre un centre de traitement d'alarmes officiel et un autre centre de traitement (privé) certifié dans un type au moins égal, destiné à la transmission automatique d'informations de sécurité. Les appels d'urgence peuvent être transmis aux forces de l'ordre.

4.11 Mode normal de fonctionnement d'un centre de traitement d'alarmes

Ce mode correspond à une situation dans laquelle le centre dispose de tous ses moyens propres d'exploitation ainsi que ceux des réseaux auxquels il est rattaché.

4.12 Récepteur (Fonction)

Par *"récepteur"*, il faut plutôt entendre *"fonction récepteur".* Le récepteur n'est pas un équipement ou un boîtier constituant une paire avec le transmetteur situé côté client, mais est un ensemble d'équipements modulaires et redondants, dont le rôle consiste à collecter les trames d'alarmes issues de tous types de transmetteurs et les traiter pour en extraire les messages d'alarmes (critères), soit pour un traitement local ou pour transmission à un système supérieur. Le récepteur peut être utilisé pour envoyer des commandes et pour de la télémaintenance.

4.13 Réseau

Ensemble de supports de voies de transmission mettant en relation la centrale d'alarme côté client et le centre de traitement d'alarmes (officiel ou privé).

4.14 Sabotage

Action volontaire ayant pour but la mise hors service d'une installation de détection / transmission d'alarmes (coupure de la voie de transmission, ouverture du boîtier de la centrale d'alarmes du client, entre autres possibilités).

4.15 Support de transmission

Moyen physique de transmission de l'information (exemples: ligne cuivre, câble coaxial, fibre optique, ondes hertziennes,...).

4.16 Surveillance de ligne (Polling)

Vérification du fonctionnement d'une voie de transmission.

Cette surveillance peut être définie en fonction du type d'alarme (cf. chapitre 7.1):

- continue (la période entre deux vérifications est inférieure ou égale à 20 secondes),
- discontinue (la période entre deux vérifications est inférieure ou égale à 24 heures).

4.17 Télémaintenance

La télémaintenance est l'action de se connecter à distance aux équipements du client pour éviter de générer immédiatement une intervention sur site. De façon générique, la télémaintenance signifie la maintenance d'une unité fonctionnelle assurée par télécommunication directe entre cette unité et un centre spécialisé.

4.18 Télésurveillance

De façon générique, la télésurveillance signifie surveillance à distance d'une unité fonctionnelle ou de personnes. Elle est assurée par télécommunication directe entre les équipements terminaux (par exemple, des caméras de surveillance) et un centre spécialisé.

4.19 Transmetteur

Dispositif, autonome ou intégré à un système, installé dans la continuité de la centrale d'alarme côté client, dont la fonction est d'envoyer vers un ou plusieurs récepteur(s), par le biais d'un réseau de transmission, des messages porteurs d'informations, notamment celles délivrées par la centrale d'alarme du client.

4.20 Voie de transmission

Une voie de transmission est constituée par un ensemble de réseaux de télécommunication, de même nature ou non, permettant l'acheminement de messages échangés entre la centrale d'alarme côté client et le centre de traitement d'alarmes (officiel ou privé). Cet échange est aussi appelé 'communication'.

4.21 Voie de transmission primaire (ou principale)

Voie utilisée pour l'acheminement normal des communications entre la centrale d'alarme côté client et le centre de traitement d'alarmes (officiel ou privé).

4.22 Voie de transmission secondaire (ou alternative)

Voie utilisée en cas de défaillance de la voie de transmission primaire pour l'acheminement des communications entre la centrale d'alarme domestique côté client et le centre de traitement d'alarmes (officiel ou privé).

4.23 Voie de transmission de secours

Voie prévue entre la centrale d'alarme côté client et le centre de traitement d'alarmes (officiel ou privé), permettant d'acheminer l'information de défaillance de la voie de transmission primaire ou secondaire, ainsi que des alarmes, le cas échéant. Son support de transmission doit être différent de celui utilisé pour les voies de transmission primaire et secondaire.

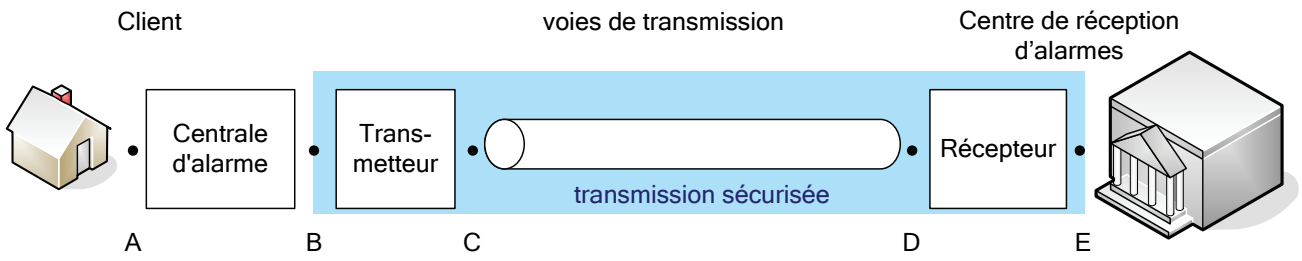
5 Exigences conceptuelles

La présente règle de prescription est élaborée dans le but d'uniformiser les transactions sécurisées mises en œuvre pour la transmission d'alarmes pompiers vers des centres de réception officiels, afin de proposer une solution sécurisée ouverte (non propriétaire) basée sur des protocoles de sécurité standard. Elle peut, par analogie, s'appliquer à la transmission de tout type d'alarmes (police, techniques) vers des centres de réception officiels ou non.

L'objectif de cette règle de prescription consiste, d'une part, à uniformiser le format des messages d'alarmes transmis et, d'autre part, à définir une spécification technique permettant à des transmetteurs conformes d'établir des liaisons sécurisées avec des récepteurs de tierces parties. Ce document décrit les exigences en rapport avec cet objectif.

5.1 Architecture

La figure suivante illustre les parties en présence pour une transmission d'alarme:

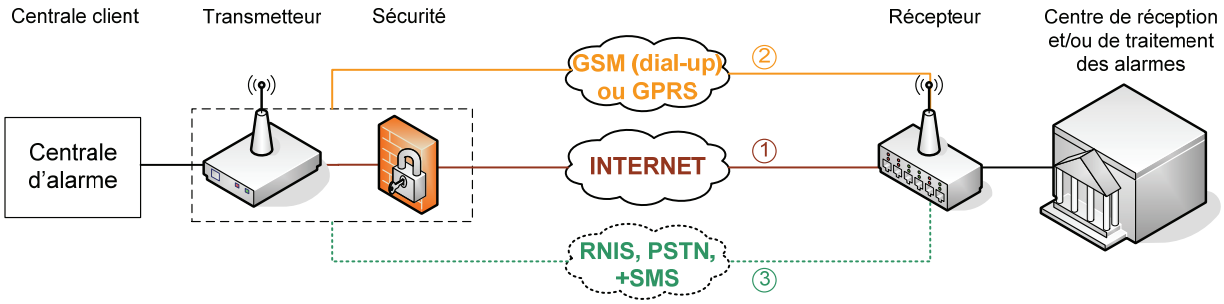


Une transmission sécurisée signifie qu'un message (dans notre cas une alarme) est transmis de manière sûre et confidentielle entre un transmetteur et un récepteur, tous deux formellement identifiés et authentifiés, par le biais d'une voie de transmission dédiée, à l'intérieur de laquelle l'information est cryptée et n'a subi aucune modification en cours de transmission.

5.2 Voies de transmission

Compte tenu du niveau de fiabilité requis et des besoins opérationnels y relatifs, le système devra disposer de 2 voies de transmission physiquement séparées, avec possibilité d'une 3ème voie optionnelle, dite de secours.

Binôme recommandé: Internet comme voie primaire, le réseau mobile (GSM dial-up[1] et/ou GPRS ou tout autre protocole IP de transmission de données plus récent, tel que HSDPA) comme voie secondaire et, optionnellement, le réseau téléphonique fixe ou/et le SMS comme voie de secours.



D'autres binômes, combinaison des technologies retenues ci-dessus, sont admis, tant que la condition des voies de transmission physiquement séparées est respectée.

---

[1] Les centres de réception **officiels** ne supportent pas le GSM dial up, ni le RNIS, ni le PSTN.

5.3 Transmetteur

Le transmetteur est un équipement modulaire offrant différentes interfaces spécifiques. Son rôle principal consiste à collecter les messages issus de la centrale d'alarme du client et à les traiter pour pouvoir les transmettre au(x) centre(s) de réception associé(s) (cf. 4.4) via les différentes voies de transmission définies (cf. 5.2).

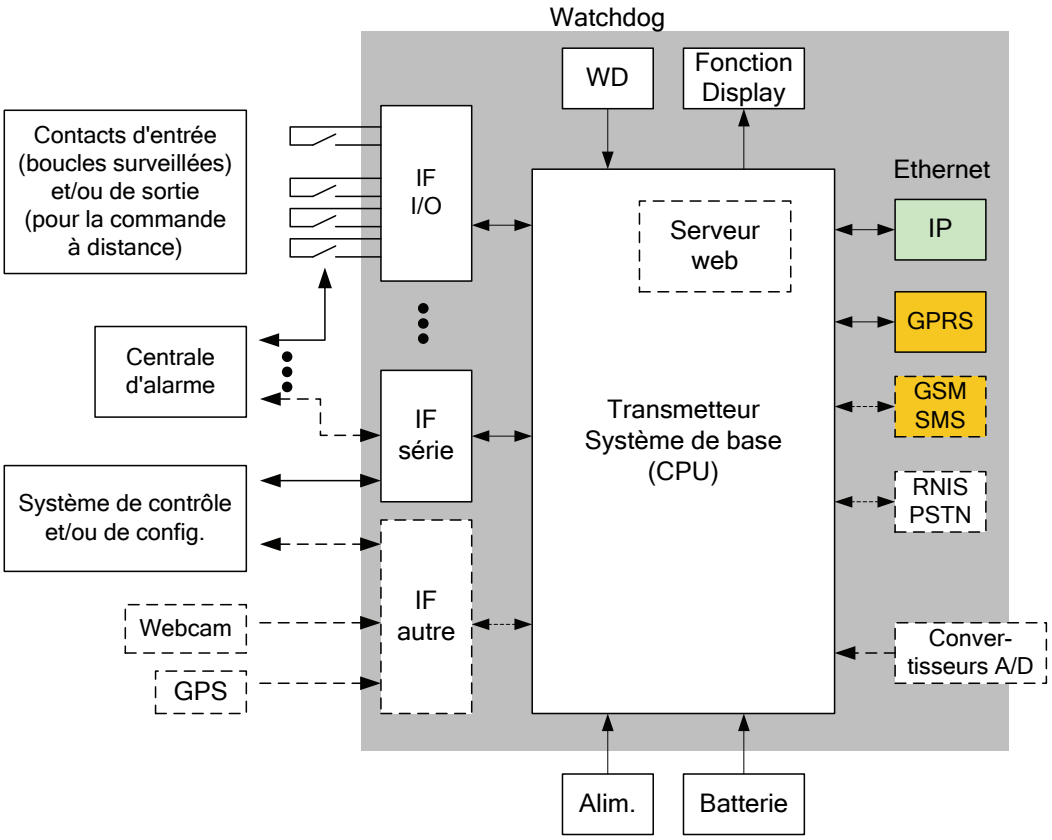
Le transmetteur doit disposer d'un mécanisme lui permettant de surveiller ses interfaces et son état de fonctionnement (watchdog). En cas de défectuosité matérielle détectée, il devra notifier une alarme technique au centre compétent et signaler une alarme locale (alarme optique et acoustique en cas d'incendie, selon AEAI). Les critères optiques et acoustiques devront être paramétrables en fonction du type d'alarme.

Lors d'une transmission d'alarme effraction, le transmetteur doit être protégé contre le sabotage au sens de I&HAS (ex-IALA). En cas d'alarme sabotage, cette alarme doit être transmise à la centrale officielle.

La constitution du transmetteur devrait lui permettre d'évoluer avec les nouvelles technologies et d'intégrer de nouvelles interfaces ou fonctionnalités. Par exemple, l'intégration d'un serveur web pour la télésurveillance et/ou la télémaintenance, l'affichage des alarmes traitées ou en suspens, l'état du transmetteur ou son paramétrage à travers une interface graphique.

Le transmetteur peut être modélisé comme suit:

(schéma fonctionnel)



Les composants en pointillé sont optionnels.

Une ou plusieurs entrées analogiques peuvent permettre de connecter des éléments permettant de faire la détection de niveau ou de flanc (utilisable comme signal déclencheur).

Les équipements de transmission sont, en principe, conformes à EN 50131 et à EN 50136.

5.3.1 Exigences

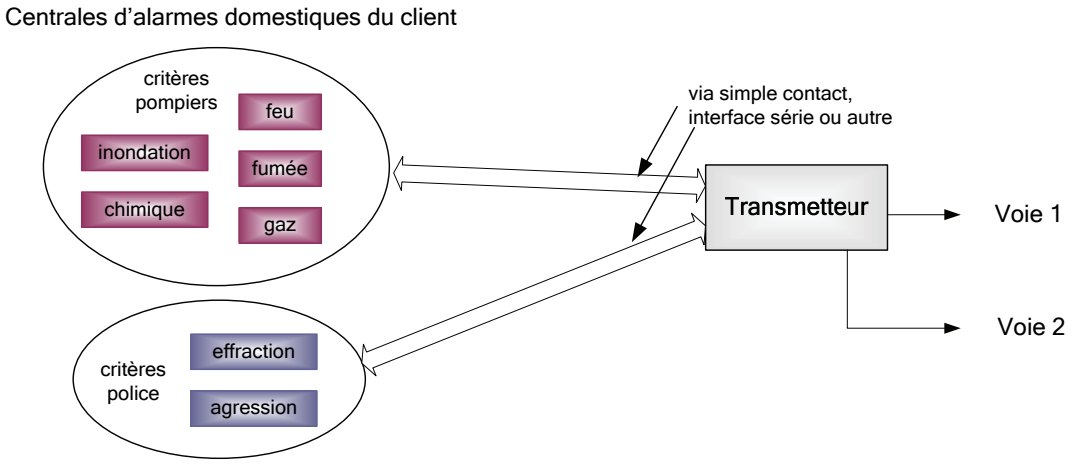
- Le transmetteur a pour fonction d'encapsuler l'information d'entrée dans un protocole de transmission approuvé par l'Autorité compétente.
- En sortie : le format de sortie des données du transmetteur doit satisfaire au(x) protocole(s) de transmission approuvé(s) par l'Autorité compétente.

5.3.2 Autres exigences

- Interface IP = Ethernet 10/100+ selon IEEE 802.3
- Interfaces I/O = contacts d'entrée et/ou de sortie, libres de potentiel.
- Le transmetteur peut-être alimenté par le système hôte lorsqu'il y est intégré. Sinon, il disposera de sa propre alimentation et de batteries de secours. Dans les deux cas, une autonomie minimum de 24 heures doit être garantie.
- La fonction « display » peut être assurée par un affichage alphanumérique ou par de simples LED associées à des critères particuliers. Cette fonction permet un diagnostic du transmetteur. Exigence minimum: une LED doit indiquer l'état « En service / hors service » et une autre le statut « Alarme / pas d'alarme ».
- Le transmetteur doit être capable d'enregistrer les événements en local (fichier log). Ces évènements (défectuosité détectée, message d'alarme, etc.) doivent pouvoir être lus à travers les interfaces locales ou via le serveur web intégré, si disponible.
- Les destinataires doivent être programmables en fonction du type et/ou du critère d'alarme. Dans ce sens, le transmetteur doit supporter la définition de 8 destinataires (adresses IP) par type et/ou critère d'alarme.
- Si le transmetteur intègre un serveur web, il doit supporter les mises à jour de sécurité nécessaires pour prévenir les attaques depuis Internet (spam, virus, déni de service, etc.). Ce serveur web, optionnel, devrait être accessible par le protocole crypté SSL/TLS.
- Pour des applications particulières, l'Autorité Compétente peut exiger que le transmetteur soit apte à recevoir des quittances, des commandes et des mises à jour (firmware, antivirus, etc.).

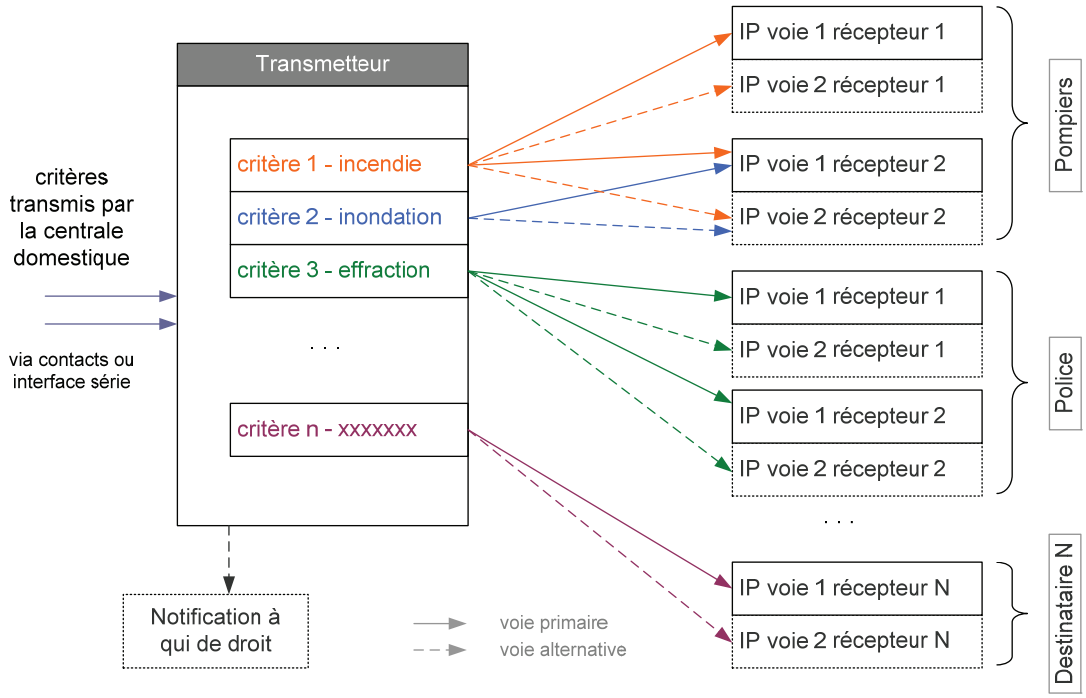
Note:

Les centrales d'alarmes domestiques doivent être raccordées sur le transmetteur via une interface spécifique. La figure suivante illustre ce propos.



5.3.3 Définition des destinataires par critère

La figure suivante illustre les possibilités de configuration d'un transmetteur. Chaque critère peut être envoyé à plusieurs destinataires, chaque destinataire disposant d'au moins un récepteur, accessible par son adresse IP (Ethernet) de la voie primaire ou secondaire:



Partant du principe que l'on doit pouvoir adresser au moins 4 récepteurs différents par critère, le transmetteur doit supporter la définition d'au moins 8 destinations par critère. Cette définition peut être représentée de façon matricielle:

Exemple de programmation des destinataires par critère

	Dest.1				Dest.2		Dest.3		Dest.4		Dest.5	
	R1 IP voie 1	R1 IP voie 2	R2 IP voie1	R2 IP voie 2	R1 IP voie 1	R1 IP voie 2	R1 IP voie 1	R1 IP voie 2	R1 IP voie 1	R1 IP voie 2	R1 IP voie 1	R1 IP voie 2
crit. 1	X	X	X	X	X	X	X	X				
crit. 2	X	X	X	X			X	X	X	X		
crit. 3					X	X	X	X			X	X

avec (exemple):

Table des critères

crit. 1	incendie
crit. 2	inondation
crit. 3	effraction
crit. n	xxxxxx

Table des destinataires

Dest.1	R1 IP voie1	a.b.c.d
	R1 IP voie 2	b.c.d.e
	R2 IP voie 1	c.d.e.f
	R2 IP voie 2	d.e.f.g
Dest.2	R1 IP voie 1	e.f.g.h
	R1 IP voie 2	f.g.h.i
Dest.3	R1 IP voie1	g.h.i.j
	R1 IP voie 2	h.i.j.k
Dest.4	R1 IP voie 1	i.j.k.l
	R1 IP voie 2	j.k.l.m
Dest.5	R1 IP voie1	k.l.m.n
	R1 IP voie 2	l.m.n.o

5.4 Récepteur

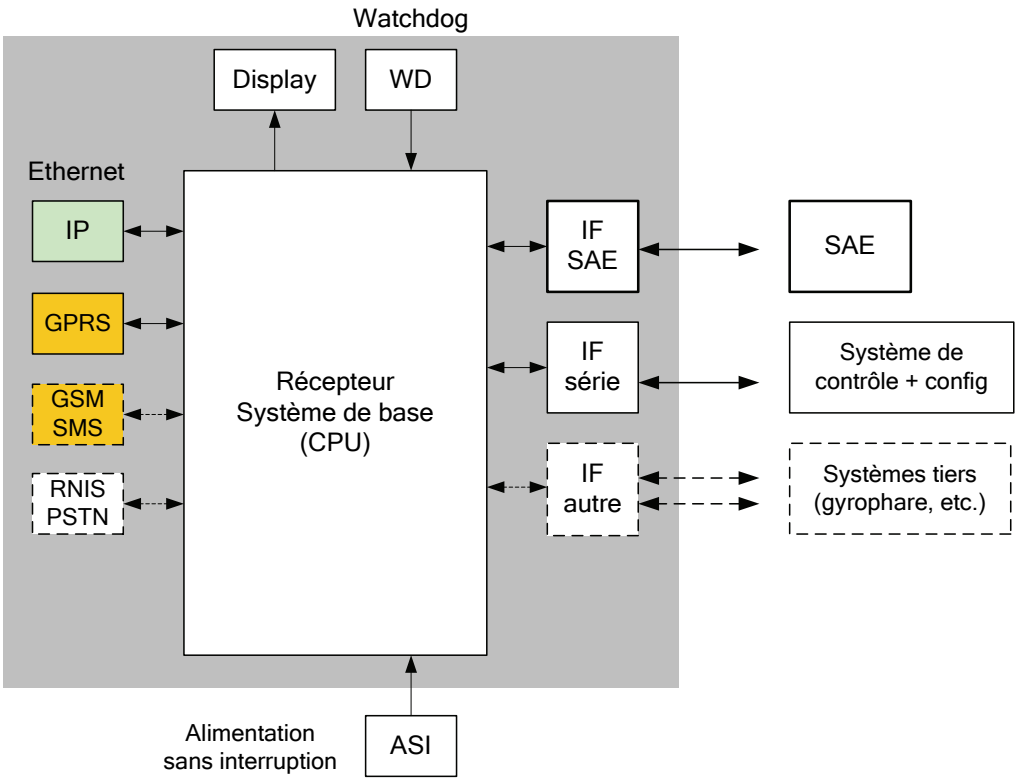
Par *"récepteur"*, il faut plutôt entendre *"fonction récepteur".* Attention, le récepteur n'est pas un équipement ou un boîtier constituant une paire avec le transmetteur situé côté client, mais est un ensemble d'équipements modulaires et redondants, dont le rôle consiste à:

- collecter les trames d'alarmes issues de tous types de transmetteurs IP compatibles et transmises sur différents supports;
- les traiter pour en extraire les messages d'alarmes (critères) soit pour un traitement local ou pour transmission à un système supérieur, dans le cas des centres officiels le Système d'Aide à l'Engagement (SAE).

A l'extrême, le *récepteur* peut simplement être un applicatif sur un serveur web qui va lire les informations contenues dans le transmetteur qui est, lui aussi, un serveur web.

Le *récepteur* doit fonctionner de façon autonome. Il doit disposer d'un mécanisme lui permettant de surveiller ses interfaces et son état de fonctionnement (fonction d'auto-surveillance via un watchdog). De plus, il doit être capable de transmettre des commandes de télégestion ou de télémaintenance.

Le *récepteur* peut être modélisé comme suit (**schéma fonctionnel**):



Le *récepteur* est en fait un système de réception redondant, capable de fonctionner par lui-même. Chaque élément de ce système doit être en mesure de collecter et de mémoriser tous les messages reçus. Leur traitement incombe en principe au système supérieur (le SAE) mais peut être effectué, en mode dégradé, par un sous-système simple de type terminal.

Les équipements de transmission sont, en principe, conformes à EN 50131 et à EN 50136.

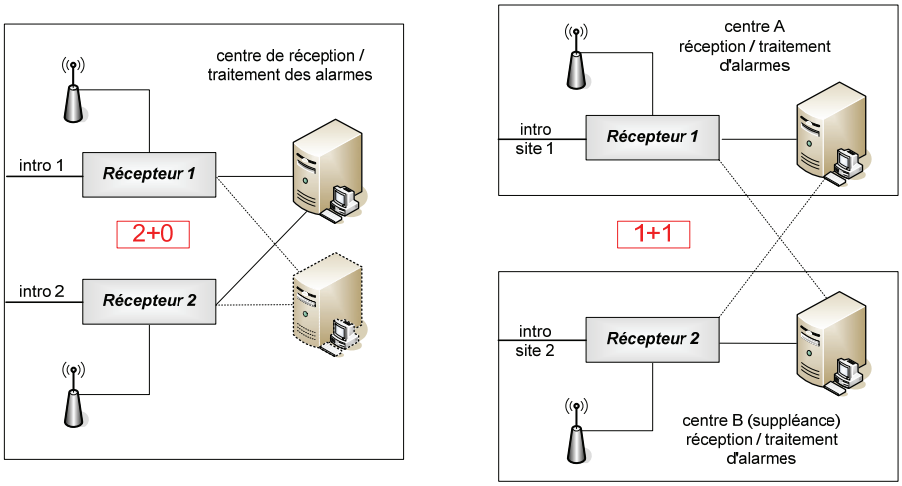
5.5 Redondance

Au même titre que les voies de transmission multiples, les centres de réception doivent disposer d'au moins 2 systèmes de réception ou assurer la redondance par un centre de suppléance (qui peut être privé), ce centre devant présenter un niveau de sécurité équivalent au centre de réception officiel.

La redondance côté réception est de type 2+0 (1 centre avec 2 systèmes de réception sur le même site) ou 1+1 (2 centres sur 2 sites séparés, avec 1 système de réception chacun). Dans ce second cas, les 2 centres peuvent faire partie de la même entité ou représenter deux entités partenaires.

En mode 2+0, les systèmes de réception doivent être cloisonnés dans des locaux séparés et connectés via des cheminements séparés, conformément aux prescriptions AEAI (voir également annexe 3). En mode 1+1, une liaison dédiée redondante doit être mise en œuvre entre les deux centres (sites) partenaires.

La redondance côté réception peut être représentée comme suit:



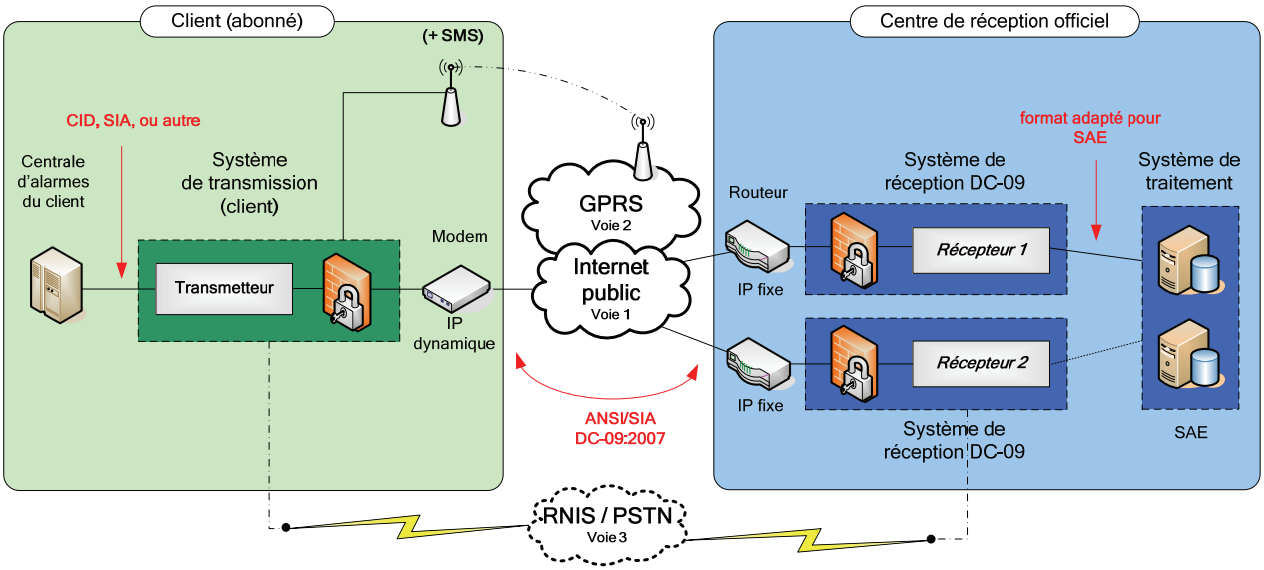
1 seul centre, 2 récepteurs sur le même site (redondance locale, 2 introductions séparées)

2 centres partenaires, 1 récepteur sur chaque site (redondance mutuelle)

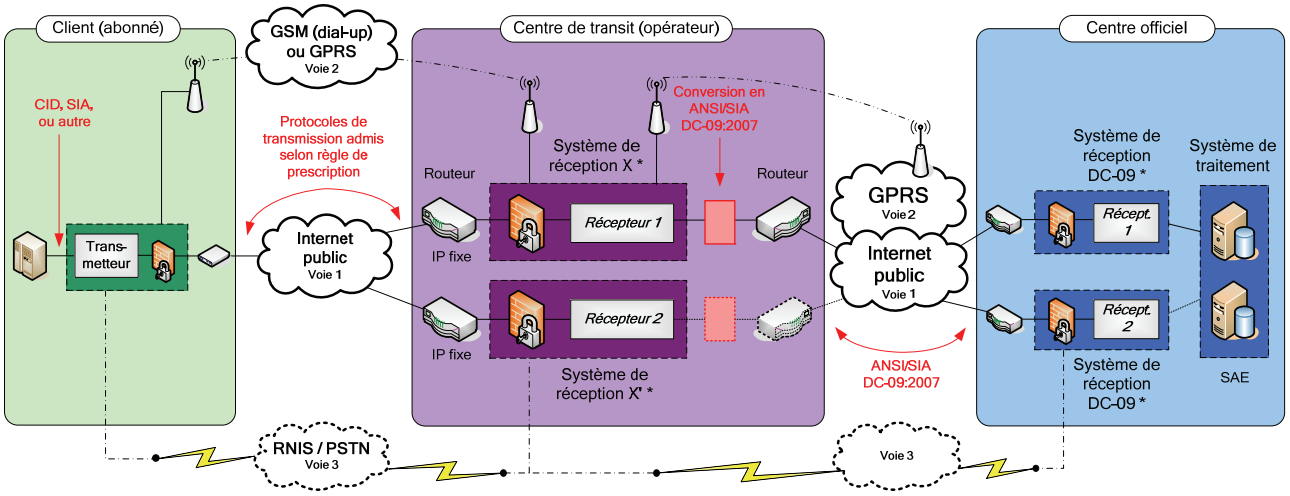
Si un système de réception n'est plus capable de garantir le traitement d'un critère reçu, il se déconnecte du réseau et n'envoie plus de quittance. Le transmetteur renvoie alors le message sur le second système de réception (envoi séquentiel pour simplifier le traitement et l'organisation). cf. Annexe 2.

La redondance effectuée par des systèmes informatiques à architecture virtualisée est acceptée, pour autant que la redondance physique des machines soit respectée.

5.5.1 Cas général: transmission directe à un centre officiel



5.5.2 Cas particulier: transmission via un centre de transit



* se référer à 6.3.2

Notes :

Les 2 récepteurs représentés au sein d'une même entité peuvent être situés sur un même site (mode 2+0) ou sur 2 sites distincts (mode 1+1). Cette remarque s'applique aussi bien au centre officiel qu'au centre de transit.

Dans le cas particulier d'une transmission via un centre de transit, la transmission n'est admise comme directe que si elle est effectuée sans intervention humaine (**routage automatique**).

5.6 Filtrage et transfert

Le système de réception doit être capable de filtrer les messages reçus en fonction du type d'alarme et/ou du critère, de façon à ne quittancer que les critères liés au domaine d'activité et de responsabilité du centre de traitement.

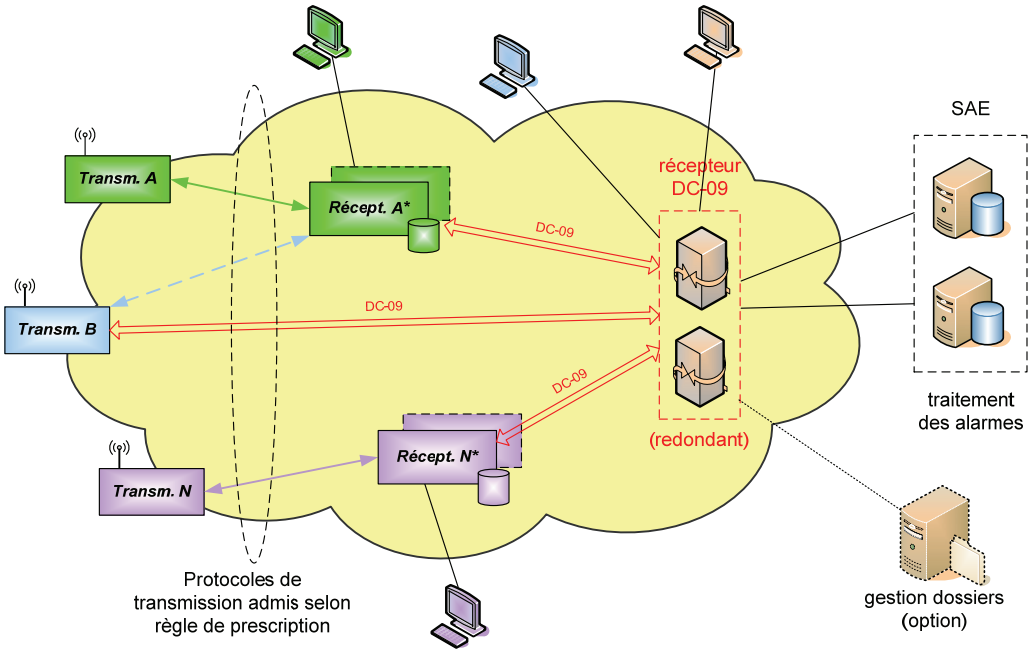
Un éventuel message reçu par erreur doit être simplement rejeté. Un tel filtrage est implicite avec des communications cryptées grâce au processus d'authentification mutuelle associé.

Un système de réception peut ainsi faire office de passerelle (routeur) et de convertisseur de protocole entre un parc de transmetteurs répondant aux conditions de la présente règle de prescription et un centre officiel. Dans ce cas, les temps de transmission, définis au point 7.2, ainsi que toutes les exigences doivent être strictement respectés, notamment ce qui concerne les voies de transmission, la sécurité et l'interopérabilité.

De plus, pour les critères pompiers de classe C4 (cf. 7.1.1), la conversion de protocole doit être totalement transparente et bidirectionnelle, notamment en cas de commandes émises depuis le centre officiel vers les transmetteurs (commande de vannes incendie, sirènes, asservissements, etc.).

Une seule conversion de protocole est admise entre un transmetteur et le récepteur DC-09 du centre officiel.

Concept global générique:



* se référer à 6.3.2

Les destinataires respectifs pour chacun des critères considérés sont à programmer dans le transmetteur.

Les clients avec critères tactiques pompiers et, le cas échéant, sécurité, doivent satisfaire aux exigences de la présente règle de prescription (voies multiples, cryptage, etc.).

De même, la présente règle de prescription s'applique intégralement pour la transmission DC-09 **entre un centre de transit et le récepteur d'un centre officiel**, quelles que soient les voies de communication utilisées entre les centres de transit et le centre officiel.

Note :

Les différents modes opérationnels liés à ce modèle sont décrits dans les « Directives organisationnelles pour la transmission sécurisée d'alarmes sur IP ».

6 Exigences relatives au système

6.1 Généralités

Le segment TCP ainsi que le datagramme IP sont normalisés (selon RFC 793 et RFC 791).

Le message à transmettre (alarme, statut ou dérangement) est transmis en une seule trame TCP/IP si sa longueur le permet. Dans le cas contraire, le message est fractionné en plusieurs parties, chacune d'elles étant transmise dans une trame standard. Le message d'origine est ensuite reconstitué coté destinataire. Ce processus, automatique, est géré par la couche TCP.

6.2 Informations considérées pour la transmission d'alarmes

6.2.1 Informations requises (OBLIGATOIRES), basé sur l'existant

- Numéro d'événement, unique.
- Identifiant de message (incrémental).
- Critère d'alarme: feu | chimique | pollution | effraction | etc.
- Priorité: haute | normale | basse.
- Etat de l'alarme: active | quittancée | rétablie | TEST.
- Adresse IP de l'émetteur.
- Adresse IP du destinataire.
- Identifiant du transmetteur (p.ex. n° de série).
- Format d'origine du message (selon protocole(s) approuvé(s) par l'Autorité compétente).
- Date et heure de l'événement (format HH:MM:SS, MM-DD-YYYY).
- Date et heure de transmission (format HH:MM:SS, MM-DD-YYYY).

6.2.2 Informations supplémentaires (optionnelles, non exhaustives)

Les informations supplémentaires suivantes peuvent être extraites d'une ou plusieurs bases de données externes par corrélation avec les informations obligatoires :

- Identifiant du destinataire.
- Texte de l'alarme (description ou commentaires).
- Nom du site d'où provient l'alarme (texte ou code).
- Bâtiment d'où provient l'alarme (texte ou code).
- Lieu du site d'où provient l'alarme (texte ou code).
- Local d'où provient l'alarme (code alphanumérique).
- Déclencheur d'alarme (n° détecteur ou bouton poussoir).
- Coordonnées y (490000 à 590000).
- Coordonnées x (115000 à 205000).
- Coordonnées z (altitude).

Les informations ci-après, collectées également depuis une ou plusieurs sources externes (bases de données ou terminal IP), peuvent être transmises optionnellement ou sur exigence expresse de l'Autorité compétente :

- Adresse texte de l'émetteur ou identifiant.
- Image, audio et/ou vidéo associée à un événement, pour la levée de doute dans le cas d'objets présentant des risques accrus, notamment pour les établissements publics ou très fréquentés, ou encore des ouvrages difficiles d'accès (par exemple les tunnels).
- Informations complémentaires, notamment des descriptifs et états de stock pour des locaux abritant des matières dangereuses.

Pour préserver la confidentialité des informations, la transmission doit être cryptée ou seuls des "codes" interprétables par le(s) récepteur(s) destinataire(s) devront être utilisés (voir aussi 6.5).

6.3 Uniformisation du format des messages

Les messages d'alarmes issus des centrales domestiques peuvent avoir des formats divers. Pour pouvoir transmettre ces messages sur IP, une syntaxe de message uniformisée est requise. D'une façon générale, les messages à transmettre sur IP doivent être (re)formatés pour satisfaire à une syntaxe unifiée, reconnue par les récepteurs compatibles.

6.3.1 Format de message unifié

Le message doit contenir un certain nombre d'informations, requises ou optionnelles, codées dans une syntaxe flexible et évolutive. **Le(s) format(s) d'entrée défini(s) dans le(s) protocole(s) approuvé(s) par l'Autorité compétente s'impose(nt) dans cette fonction**.

6.3.2 Intégration des formats courants

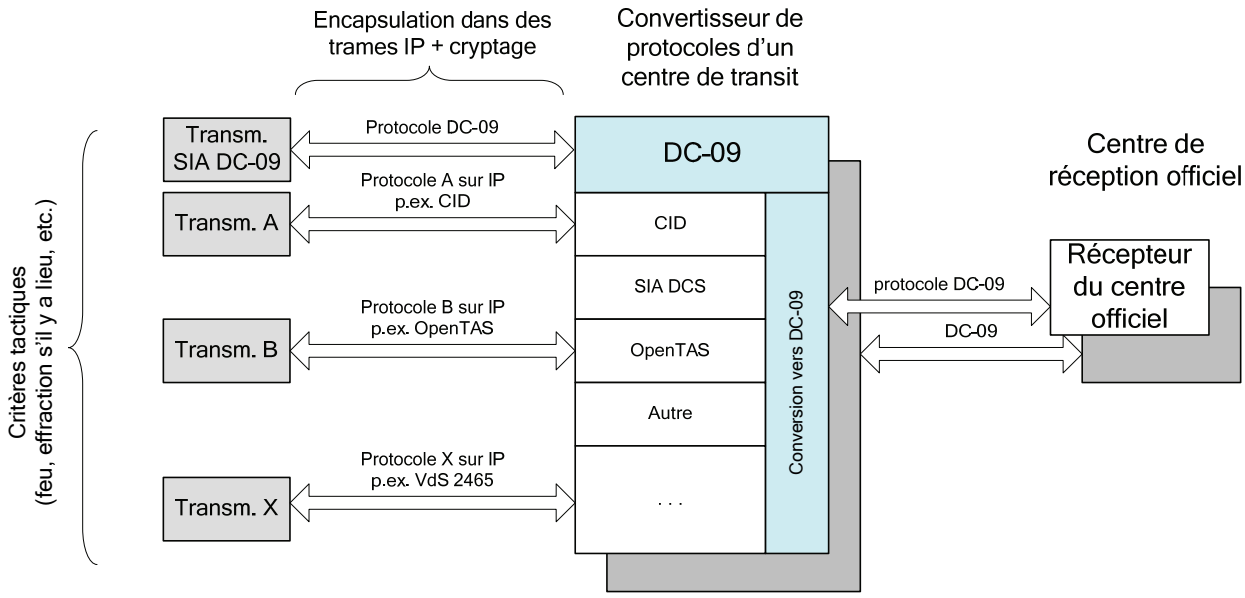
Le récepteur du centre officiel supporte le standard ANSI/SIA DC-09:2007, avec comme format de message le SIA-DCS, ce qui signifie que tous les transmetteurs compatibles peuvent adresser le système.

Le récepteur du centre de transit supporte, en entrée, d'autres protocoles et standards et, en sortie, le standard ANSI/SIA DC-09:2007.

Les transmetteurs utilisant d'autres formats propriétaires ou non pourront transiter par un convertisseur de protocoles, afin d'assurer la continuité.

Messages de commande / Télégestion : pour ce type de commande, se référer au § 6.5.9.

La figure suivante illustre le concept de réception multi-protocoles:



La présente règle de prescription s'applique intégralement pour la transmission DC-09 **entre un centre de transit et le récepteur d'un centre officiel.**

6.4 Les datagrammes

Les datagrammes permettent de 'transporter' les messages d'alarme sur un réseau IP. Chaque message est encapsulé dans un bloc de données, lequel est précédé d'un en-tête. Ce dernier contient toutes les informations nécessaires pour pouvoir transmettre les données sur IP (entre autres les adresses IP source et destination).

6.4.1 Types de datagrammes

Plusieurs types de datagrammes sont considérés:

- Datagramme avec message encapsulé en format d'origine.
- Datagramme avec message formaté avec données spécifiques.
- Datagramme de surveillance (supervision).
- Datagramme de commande (télégestion, télémaintenance).

Ces différents datagrammes utilisent un format standard. Seul le contenu du message est différent.

Le format de message **entre le transmetteur et le récepteur ou le convertisseur** est basé sur le(s) protocole(s) approuvé(s) par l'Autorité compétente (cf. figure au chap. 5.5.2).

Le format de message unifié **entre un transmetteur compatible ou un convertisseur de protocole et le centre officiel de traitement d'alarmes** est basé sur le standard ANSI/SIA DC-09:2007 (cf. figure au chap. 5.5.1).

6.4.2 Types de messages

- Transmission d'alarme.
- Requête d'informations ou d'état.
- Message de statut (état / changement).
- Accusé de réception (quittance ok / pas ok).
- Envoi de commande (télégestion / télémaintenance).
- Surveillance de ligne (supervision).

6.4.3 Information associée à un évènement

Le standard ANSI/SIA DC-09:2007 prévoit dans sa spécification (cf. § 5.5.1.8.2) un paramètre optionnel de vérification permettant de fournir une information concernant du texte, de l'audio, une image ou un flux vidéo lié à l'évènement transmis. Cette information est utilisable pour la levée de doute ou à d'autres fins.

L'information signale par exemple qu'un flux vidéo ou un état de stock est disponible à l'adresse IP <aaa.bbb.ccc.ddd>, et peut être téléchargé ou visualisé (par exemple, pour consultation) avec un protocole spécifique, depuis le centre.

6.5 Paramètres de transmission

6.5.1 Généralités

D'une manière générale, seuls les échanges de données cryptées entre équipements formellement identifiés (ou transmises à travers un VPN crypté ou solution équivalente) sont autorisés. Toutes les autres requêtes ou tentatives d'accès au transmetteur depuis l'extérieur sont rejetées.

6.5.2 Adressage IP

La connexion du transmetteur à Internet s'effectue avec adressage IP dynamique ou selon l'accès existant du client. Le transmetteur doit être accessible par une adresse IP publique. Les récepteurs des centres de réception doivent quant à eux disposer d'adresses IP fixes.

6.5.3 Communications

En raison de l'adressage IP dynamique prévu côté client, les communications sont dans tous les cas initiées par le transmetteur, sur la voie primaire ou secondaire. Typiquement, pour établir la liaison sécurisée avec le(s) récepteur(s) de leur centre de réception.

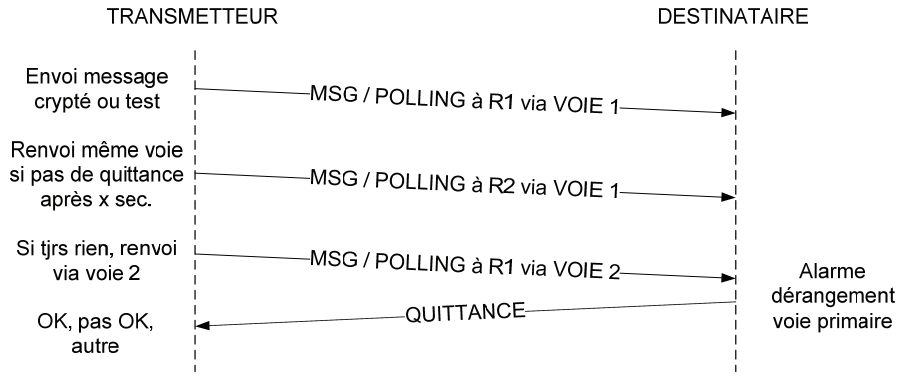
6.5.4 Transmission sécurisée

La transmission sécurisée de messages sur IP est réalisée avec des outils standard qui sont en fait des protocoles dédiés à la sécurisation des échanges de données et qui permettent de garantir la confidentialité, l'intégrité et l'authentification des échanges (cf. 6.6).

6.5.5 Retransmission séquentielle

Les messages à transmettre utilisent par défaut leur voie primaire, puis en cas de défaillance ou d'indisponibilité de celle-ci, la voie secondaire, éventuellement une voie de secours, si disponible.

Le délai d'attente d'une quittance avant de retransmettre le message doit être fixé de façon à pouvoir garantir le délai de transmission max. admis (voir 7.2), en tenant compte des retransmissions sur la même voie ou sur une voie alternative. La séquence de retransmission ci-après n'est qu'une des variantes possibles.



6.5.6 Transmission à plusieurs destinataires

La transmission d'un message (alarme, dérangement ou autre) à plusieurs destinataires est effectuée séquentiellement. Ces transmissions sont effectuées sur la voie primaire ou, à défaut, sur une voie alternative.

6.5.7 Basculement sur une voie alternative

Le temps de basculement d'une voie de transmission à une autre (c.à.d. entre une transmission infructueuse sur une voie et une retransmission sur une voie alternative) doit permettre de garantir les exigences spécifiées sous 7.2.

6.5.8 Quittancement technique

Tous les messages transmis correspondant aux critères traités par le centre de réception doivent être quittancés. Ce procédé, automatique, permet aux émetteurs d'avoir la confirmation que le destinataire a bien reçu le message, que ce message a été transmis sans erreur (checksum), et que le destinataire est à même de le traiter.

6.5.9 Messages de commande / Télégestion

Le centre officiel de réception et/ou de traitement peut envoyer des messages de commande pour la télégestion des transmetteurs affiliés. Ces derniers ayant dans la plupart des cas une adresse IP publique attribuée dynamiquement, les messages de commande doivent être envoyés en lieu et place d'un message d'acquittement de polling. Dans ce cas, l'adresse IP du transmetteur est connue (car reçue lors du message), de plus, les différentes protections (routeurs, firewall,..) sont ouvertes. L'envoi de la commande peut s'effectuer sur une des voies disponible, en général, la même que celle utilisée pour la réception du polling.

L'adresse IP obtenue lors du dernier polling est en effet un paramètre permettant d'atteindre un transmetteur. Les commandes envoyées au transmetteur permettent les actions suivantes:

- Test de présence du transmetteur.
- Consultation de l'état du transmetteur et historique des événements (serveur web).
- Envoi de commandes de télégestion (p.ex. ouverture d'une porte à distance).

Lorsque des commandes (p.ex. asservissements) sont transmises depuis le centre officiel vers un(des) transmetteur(s), l'Autorité compétente fixe l'intervalle de polling minimum à respecter et peut exiger une connexion permanente côté transmetteur (voie primaire) conformément aux exigences spécifiques de sécurité requises (p.ex. sirènes PCi) et aux exigences de 7.2.

De plus, si une conversion de protocole est effectuée entre le centre émetteur et le transmetteur cible, cette dernière doit être totalement transparente **dans les deux sens** de manière à ne pas impacter la transmission de ces commandes.

6.5.10 Maintenance à distance et commandes évoluées

Par commandes évoluées, on entend des commandes permettant d'effectuer des actions de levée de doute: contrôle vidéo, des caractéristiques du bâtiments,…

Pour les travaux de maintenance à distance et l'envoi de commandes évoluées, les deux voies peuvent être utilisées.

Une fois la liaison établie à l'aide du protocole ANSI/SIA DC-09:2007, des commandes évoluées ou de maintenance peuvent être transmises sur la voie principale ou alternative en utilisant un autre protocole. On veillera dans ce cas à ne pas interrompre une transmission en cours.

Pour les sites demandant l'envoi de commandes ou de la maintenance à distance régulièrement, le Centre officiel peut demander au transmetteur d'effectuer une surveillance permanente des voies de communication. Le récepteur peut contacter le transmetteur sans délais, sur sa voie primaire ou secondaire, en se basant sur l'adresse IP publique utilisée lors du dernier polling.

Si le transmetteur est placé derrière un pare-feu, dans certains cas, une règle d'accès spécifique devra être définie dans le pare-feu pour en autoriser l'accès.

Pour un téléchargement spécifique (mise à jour, patch de sécurité, etc.), le récepteur peut notifier le transmetteur qu'une mise à jour est disponible à une adresse IP spécifiée. Le transmetteur peut alors télécharger lui-même cette mise à jour via sa voie primaire, au moyen du protocole spécifié.

6.5.11 Centre de télésurveillance

Les mécanismes discutés sous 6.5.9 et 6.5.10 peuvent également être utilisés par les centres de télésurveillance pour commander à distance les centrales de leurs clients dont ils assurent la gestion (par exemple, pour l'ouverture de portes, de coffres, l'accès à des caméras, etc.).

6.6 Paramètres de sécurité

6.6.1 Authentification

L'émetteur d'un message doit être identifié et authentifié de manière univoque. La provenance de la transmission est vérifiée de façon à exclure l'usurpation d'identité (pouvant conduire à des troubles d'exploitation ou à l'engagement de moyens importants pour de fausses alarmes).

La procédure d'authentification vérifie l'identifiant du transmetteur, en clair ou codé selon des paramètres convenus, et rejette toute tentative si l'authentification n'a pas pu être vérifiée.

6.6.2 Cryptage des données (confidentialité)

Le cryptage permet de garantir la confidentialité et l'authenticité des données. Cette fonction peut utiliser des algorithmes à échange de clés symétriques ou asymétriques (clé publique et clé privée) ou des certificats. Cette fonction est requise pour la transmission d'alarmes sur IP.

6.6.3 Hachage (contrôle d'intégrité)

Le hachage est une fonction non réversible qui associe à un ensemble de chaînes de caractères arbitraires une chaîne d'octets de longueur fixe (l'empreinte), et permet de vérifier l'intégrité d'un message (garantit que l'information n'a pas été modifiée en cours de transmission).

6.6.4 Protection contre la substitution

Pour prévenir l'usurpation d'identité, le transmetteur doit s'identifier dans le message par un code qui peut être transmis en clair ou crypté, permettant de l'identifier de façon univoque (p.ex. adresse MAC). Ce paramètre, correspondant à la norme EN 50136-1-1, § 6.5.1 est exigé.

6.6.5 Filtrage des communications entrantes

La transmission de messages d'alarme peut être effectuée par le biais de différentes voies de transmission (réseau IP public ou privé, réseaux mobiles ou fixes).

- Pour les voies IP, il est conseillé de mettre en œuvre des règles au niveau d'un firewall pour filtrer les émetteurs de messages potentiellement autorisés.
- Pour le centre de transit, lors de transmissions par les voies "téléphoniques" (réseaux mobiles ou fixes), un filtrage basé sur le numéro de téléphone de l'appelant est conseillé (ACL, Access Control List). Par cette mesure, seuls les numéros répertoriés dans une liste de contrôle sont considérés, permettant de se prémunir contre l'usurpation d'identité et le spam.

6.7 Paramètres requis pour l'interopérabilité

Les points listés ci-après représentent les conditions minimales devant être remplies pour satisfaire cette spécification et garantir un minimum d'interopérabilité entre les produits des divers fabricants.

6.7.1 Algorithmes de cryptage admis par l'Autorité compétente

Les algorithmes de cryptage ayant une clé de cryptage de 128 bits ou supérieur sont acceptés, soit, au minimum :

- AES – Advanced Encryption Standard, avec clé de cryptage de 128 bits ou supérieur.
- IDEA – International Data Encryption Algorithm, avec clé de cryptage de 128 bits.

Le transmetteur doit supporter au moins l'un des 2 algorithmes de cryptage susmentionnés (obligatoire). Le récepteur doit en revanche supporter les 2 algorithmes susmentionnés et, au niveau du cryptage AES, des clés de cryptage de 192 et 256 bits.

L'Autorité compétente se réserve le droit de mettre à jour, en fonction de l'évolution des techniques, les algorithmes de cryptage admis, de niveau équivalent ou supérieur à ceux susmentionnés.

6.7.2 Algorithmes de hachage acceptés par l'Autorité compétente

- MD5 – utilise une clé 128 bits
- SHA1 – utilise une clé de 160 bits

La fonction de hachage, qui permet de vérifier l'intégrité des messages, est optionnelle pour le transmetteur. Si un protocole non crypté est utilisé pour la transmission des messages, le hachage devient obligatoire.

L'Autorité compétente se réserve le droit de mettre à jour, en fonction de l'évolution des techniques, les algorithmes de hachage recommandés ou les contrôles d'intégrité exigés, de niveau équivalent ou supérieur à ceux susmentionnés.

6.7.3 Identification de l'émetteur d'un message

L'identification de l'émetteur d'un message est requise pour chaque transmission.

6.7.4 Vérification de l'émetteur par un autre critère

- Voie IP: adresse MAC (Media Access Control) et numéro de série normalisé.
- Voie mobile: IMEI (International Mobile Equipment Identity) ou numéro de téléphone.
- Voie fixe: numéro de téléphone de l'émetteur (pour le centre de transit).

Les coordonnées GPS peuvent également être utilisées (système ad hoc requis).

6.7.5 Protocole de communication: TCP vs UDP

La présente règle de prescription tolère les 2 protocoles. Pour éviter des incompatibilités entre produits (p.ex. si le transmetteur ne fait que du TCP et le récepteur que de l'UDP), le récepteur doit supporter les 2 protocoles.

6.7.6 Horodatage

La méthode d'horodatage utilisée doit permettre de répertorier 3 timestamps:

- Date et heure de survenance de l'événement.
- Date et heure de transmission de l'événement par le transmetteur.
- Date et heure de réception de l'événement transmis.

Les informations d'horodatage doivent tenir compte de l'heure d'hiver et de l'heure d'été. Les équipements de transmission et de réception sont responsables de synchroniser leur horloge interne, par exemple par NTP en se connectant au moins 1x par jour sur des serveurs de temps de référence (par exemple pool.ntp.org ou time.nist.gov).

6.8 Enregistrement des événements

- Les divers événements (alarmes, dérangements, quittances ou autres) relatifs à un site particulier doivent être enregistrés en local sur le transmetteur client.
- Suite à une indisponibilité des voies de transmission, le transmetteur doit être capable de transmettre automatiquement au récepteur les alarmes non transmises mais enregistrées en local, dès qu'une des voies de transmission est à nouveau disponible.
- Les événements enregistrés en local doivent pouvoir être consultés au travers d'une des interfaces du transmetteur, moyennant les droits d'accès adéquats selon EN 50136-2-1.
- Les centrales de réception doivent pouvoir conserver les logs, conformément aux exigences de EN 50136 et/ou EN 50131. **Le système de réception doit être dimensionné de sorte à pouvoir mémoriser les événements des 3 derniers mois**, conformément à R31.

7 Surveillance et performances

7.1 Surveillance de ligne

7.1.1 Niveaux de surveillance pour les alarmes pompiers (ou feu)

La surveillance de ligne est effectuée selon la classification du risque définie par les directives AEAI soit:

- Classe C4, implique une surveillance permanente (toutes les 20 sec) pour les sites à fort risque.
- Classe C3, implique une surveillance toutes les 5 heures.
- Classe C2, implique une surveillance toutes les 23 heures.
- Classe C1, pour les sites sans surveillance ou surveillés 1x par mois pour les sites à moindre risque et la voie de secours.

La fréquence de polling appliquée doit satisfaire aux critères définis dans EN 50136. **L'autorité compétente peut cependant exiger une fréquence de polling plus élevée.**

Note **:**

La classe C1 s'applique aux installations antérieures à 2005.

7.1.2 Niveaux de surveillance pour les alarmes effraction et agression (ou police)

Se référer aux « Exigences relatives aux Systèmes de transmission d'alarme – ATS » de l'Institut de Sécurité. La surveillance de ligne dépend des exigences ATS pour les différentes classes considérées.

7.1.3 Niveaux de surveillance pour les alarmes techniques se rapportant aux installations de détection et d'extinction

La fréquence de polling appliquée à ce type d'alarme doit permettre de garantir les performances décrites sous 7.2.3.

7.1.4 Polling depuis le transmetteur

La surveillance principale de la connexion entre le transmetteur et le système de réception est confiée au transmetteur. Ce dernier surveille non seulement ses propres interfaces (cf. 7.1.6) mais également ses différentes voies de transmission en envoyant périodiquement son état au système de réception (méthode « push ») qui doit lui retourner une quittance.

→ Si une quittance est retournée, la liaison est vérifiée.

Si la voie primaire devient indisponible, la fréquence de polling définie pour la voie secondaire reprend celle de la voie primaire.

7.1.5 Contrôle du polling depuis le centre de réception

Le récepteur doit connaître l'intervalle de polling de chacun de ses transmetteurs clients (directement raccordés ou par l'opérateur) et pouvoir générer une alarme s'il n'a rien reçu dans un délai défini.

7.1.6 Surveillance interne des équipements

Si la surveillance interne d'un équipement identifie un problème sur une de ses interfaces, une notification de dérangement est immédiatement envoyée au centre de réception via une voie disponible. Tant que cet état demeure, les transmissions s'effectuent sur cette voie. Dès que le dérangement est levé une notification est envoyée au centre de réception compétent.

7.1.7 Activation de la voie alternative

Si après un polling ou la transmission d'un message, le transmetteur ne reçoit aucune quittance du récepteur dans un délai défini, il active la voie alternative et renvoie le message par ce vecteur (cf. 6.5.5 et annexe 2). Dans ce cas, la fréquence de polling pour la voie secondaire reprend celle de la voie primaire.

7.1.8 Sabotage

En matière d'effraction, une rupture des 2 voies de communication doit être considérée comme un sabotage, au sens des prescriptions édictées par l'I&HAS (ex-IALA) ; elle doit être interprétée, au niveau du récepteur, comme un sabotage, en particulier pour les ouvrages de classe C4.

7.2 Performances

Exigences selon références EN 50136-1-1.

7.2.1 Exigences pour alarmes pompiers (ou feu)

Performances	Valeur	Réf. EN 50136-1-1
Délai de transmission	10 sec	D4 selon 6.3.2, table 1
Délai de transmission max.	20 sec	M4 selon 6.3.2, table 2
Disponibilité annuelle	99.8%	A4 selon 6.4.5, table 4

L'exigence maximum concernant le temps de report pour les alarmes tactiques est de 180 secondes (T4 selon EN 50136-1-1).

7.2.2 Exigences pour alarmes effraction et agression (ou police) (s'il y a lieu)

Les performances exigées en terme de temps de reports, délai de transmission, délai de transmission maximum et de disponibilité annuelle pour les alarmes effraction et agression (ou police) sont définies sous 7.1.2.

7.2.3 Exigences pour alarmes techniques se rapportant aux installations de détection et d'extinction (s'il y a lieu)

Performances	Valeur	Réf. EN 50136-1-1
Délai de transmission	60 sec	D2 selon 6.3.2, table 1
Délai de transmission max.	120 sec	M2 selon 6.3.2, table 2
Disponibilité annuelle	99.3%	A2 selon 6.4.5, table 4

L'exigence maximum concernant le temps de report pour les alarmes techniques est de 180 secondes (T4 selon EN 50136-1-1).

Notes :

- Si plusieurs critères sont considérés sur un site (pompiers, police, etc.), ce sont les exigences liées au critère le plus contraignant qui s'appliquent (à tous les critères considérés).
- Les installations volontaires ne sont pas concernées par ces exigences.

7.3 Exigences en fonction du degré de risque

Pour les sites avec degré de risque élevé (surveillance permanente, classe C4 selon 7.1.1), il est obligatoire d'avoir 2 voies de transmission physiquement séparées de bout en bout.

Pour les sites avec degré de risque moins élevé (classes C2 et C3 selon 7.1.1), il est obligatoire d'avoir 2 voies de transmission physiquement séparées côté client. Le passage au travers d'un vecteur Internet commun est admis (considéré comme suffisamment maillé et redondant).

Pour les sites avec degré de risque faible (classe C1 selon 7.1.1, par exemple), il est admis de n'avoir qu'une seule voie de transmission côté client. Une 2ème voie est cependant recommandée.

Lors de cas exceptionnels liés à des raisons techniques et économiques particulières, l'Autorité Compétente statue.

Pour les centres de réception (de transit et officiels), les prescriptions édictées par l'AEAI et/ou l'I&HAS (ex-IALA) en termes d'infrastructures s'appliquent intégralement. Les exigences complémentaires figurant dans la règle R31 et dans VdS 2153 sont recommandées mais pas obligatoires.

ANNEXE 1 – Syntaxe selon ANSI/SIA DC-09:2007

Syntaxe pour chaque événement, selon ANSI/SIA DC-09:2007[2]:

```
                                <LF><crc><0LLL>
<"id"><seq><Rrcvr><Lpref><#acct>[<pad>|…data…][x…data…]<timestamp>
                                <CR>
```

avec *LLL* = longueur du message, "*id*" = code indiquant le format d'entrée, *seq* = numéro de séquence (pas incrémenté lors d'un renvoi), *acct* = identifiant du transmetteur, *pref* = préfixe, *rcvr* = identifiant du récepteur et *timestamp* = heure de transmission.

Flag de cryptage: Lorsque les données et l'horodatage sont cryptés, un astérisque est inséré dans le code de format d'entrée ("*id*"), après le 1er guillemet. Exemple: "*****SIA-DCS"

Exemples de messages selon ANSI/SIA DC-09:2007:

Dans ces exemples, les paramètres suivants sont constants. "Format …" représente le format d'entrée.

```
seq:    9876
rcvr:   579BDF
pref:   789ABC
acct:   12345A
```

1) Alarme Feu, Zone 129, Format SIA DC-04, Crypté

Le message est montré avant le cryptage de la région comprise entre le "[" d'ouverture et le <x0D> de fermeture. Il y a 12 octets de padding dans ce message. La longueur du paquet est donnée après le processus de cryptage.

```
<x0A>XXXX0084
"*SIA-DCS"9876R579BDFL789ABC#12345A
[<x9F4602D9055F24A26544928C>|#12345A|NFA129]_13:14:15,02-15-2006<x0D>
```

2) Alarme Intrusion, Zone 65, Format SIA DC-04, Non crypté, Adresse MAC

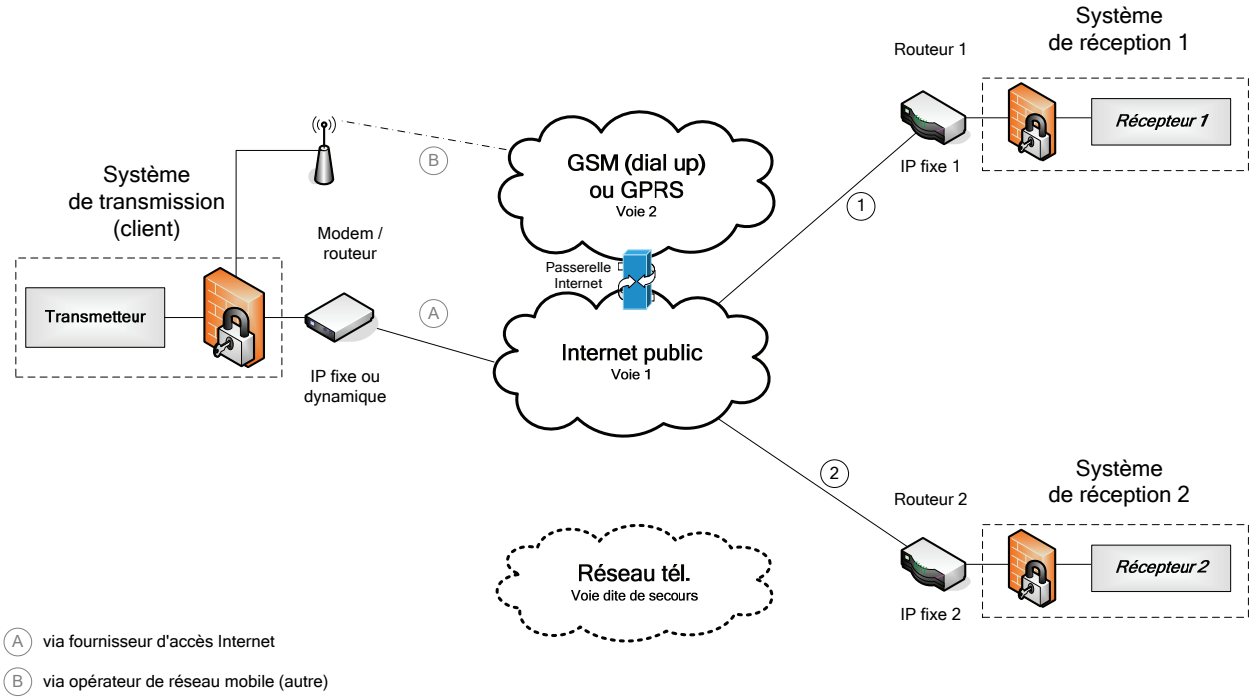
Le message ne comporte pas de padding et d'horodatage (message non crypté), le BA en format SIA est utilisé pour Burglary Alarm. Dans le champ d'extension (*x…data…*) ce trouve l'adresse MAC précédée du caractère M.

```
<x0A>42620042
"SIA-DCS"9876R579BDFL789ABC#12345A
[#12345A|NBA0065][M1234567890AB]<x0D>
```

[2] Des informations complémentaires figurent dans le document « Complément technique à la Règle de prescription ».

ANNEXE 2 – Redondance et séquence de retransmission

La figure suivante illustre le principe:



A via fournisseur d'accès Internet

B via opérateur de réseau mobile (autre)

1 via fournisseur d'accès Internet #1

2 via fournisseur d'accès Internet #2

Séquence de retransmission en cas de non quittancement:

1 - envoi sur R1 via voie 1,
2 - si pas de quittance, renvoi sur R2 via voie 1,
3 - si pas de quittance, renvoi sur R1 via voie 2,
4 - si pas de quittance, renvoi sur R2 via voie 2.

Notes:

La séquence de retransmission ci-dessus n'est qu'une des variantes possibles.

Les centres de réception **officiels** ne supportent pas le GSM dial up, ni le RNIS, ni le PSTN.

ANNEXE 3 – Check-lists techniques

3.1 Exigences pour le transmetteur

3.2 Exigences pour le système de réception du centre officiel et/ou de transit

3.3 Exigences pour les infrastructures d'un centre de réception officiel et/ou de transit

Annexe 3.1: Exigences pour transmetteur

Les codes sous Réf. correspondent aux sections référencées de la règle de prescription.
En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

Transmetteur proposé (Marque/modèle): .....

			Exigences		Produit
N°	**Réf.**	**Désignation**	**Requis**	**Option**	**OK**
		Généralités			
1.	5.3	Surveillance interne (watchdog) *Le transmetteur dispose d'un mécanisme lui permettant de surveiller ses interfaces et son état de fonctionnement.*	☒	☐	☐
2.	5.3	Protection contre le sabotage *Le transmetteur est protégé selon AEAI et I&HAS (ex-IALA) (s'il y a lieu), EN 50136 et EN 50131.*	☒	☐	☐
		Interfaces			
3.	5.3	Interfaces de communication (voies de transmission): ☐ Ethernet 10/100+ selon IEEE 802.3 ☐ GPRS ☐ EDGE ☐ autre: ..... ☐ PSTN ☐ RNIS ☐ GSM *Attention: au moins 2 cases à cocher sur 2 lignes différentes !* ***Ethernet obligatoire en cas de surveillance permanente.***	 ☒ ☒ ☐	 ☐ ☐ ☒	 ☐ ☐ ☐
4.	5.3	Interfaces de communication (périphériques locaux): ☐ RS232 nombre: ..... ☐ USB nombre: ..... ☐ autres: ..... nombre: ..... *Pour maintenance locale ou raccordement d'équipements spéciaux tels que webcam, GPS, imprimante ou autre.*	☐	☒	☐
5.	5.3	Interface pour connecter la centrale du client: ☐ RS232 ☐ USB ☐ contact ☐ autre: ..... **ou**: ☐ transmetteur intégré dans la centrale d'alarme ☐ centrale d'alarme intégrée dans le transmetteur *Attention: au moins une des cases proposées doit être cochée !*	☒	☐	☐
6.	5.3	Interfaces d'entrées/sorties (I/O): ☐ contacts d'entrée (boucles surveillées) nombre: ..... ☐ contacts de sortie (libres de potentiel et individuels) nombre: ..... *Les contacts de sortie doivent pouvoir être activés à distance.*	☒ ☐	☐ ☒	☐ ☐
7.	5.3	Autres interfaces (optionnelles): ☐ interface(s) analogique(s) de type PT100 (0..10V, 0..20mA) nombre: ..... ☐ autre(s): ..... nombre: ..... *Interfaces analogiques utilisables comme déclencheur selon détection de niveau ou de flanc.*	☐ ☐	☒ ☒	☐ ☐

Annexe 3.1: Exigences pour transmetteur

Les codes sous Réf. correspondent aux sections référencées de la règle de prescription.
En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

			Exigences		Produit
N°	**Réf.**	**Désignation**	**Requis**	**Option**	**OK**
		Communication			
8.	6.5.2	Adressage IP: ☐ fixe ☐ dynamique (DHCP)	☒	☐	☐
9.	5.3 5.5	Protocole de transmission : ▪ Supporte le standard de communication ANSI/SIA DC-09:2007 pour les transmissions numériques via IP ▪ Autre(s) protocole(s) : …… *Le protocole DC-09 est requis pour la transmission d'alarmes tactiques à un centre officiel.*	☒ ☐	☐ ☒	☐ ☐
10.	6.7.5	Protocoles de communication supportés: ☐ TCP ☐ UDP *Le transmetteur **doit supporter au moins l'un des 2 protocoles** susmentionnés.*	☒	☐	☐
11.	--	Gestion de la priorité des messages (avant l'envoi). *Les évènements détectés notifiés au transmetteur doivent être traités (transmis) dans l'ordre de survenance en tenant compte des priorités définies selon le type d'alarme et/ou le critère.* ***Requis** pour les transmetteurs qui traitent **conjointement** des alarmes **tactiques feu et autres** (p.ex. effraction).*	☒	☐	☐
12.	6.5.7 7.1.7	Basculement sur une voie de transmission alternative. *Le basculement (automatique) sur la voie alternative doit garantir le respect du délai de transmission et du temps de report.*	☒	☐	☐
13.	7.1.1	Fréquence de polling programmable. Intervalle ajustable entre ..... et ..... (durée) *La durée entre 2 pollings doit satisfaire aux exigences spécifiées dans la règle de prescription pour la surveillance dite permanente (classe C4).*	☒	☐	☐
14.	7.1.4	Surveillance périodique (polling). *Le transmetteur doit pouvoir tester périodiquement la présence de son (ses) destinataire(s) principal(aux) via la voie primaire et, via une voie alternative. La fréquence de polling peut être différente pour les voies primaire et secondaire. Si une quittance est retournée, la liaison est vérifiée.*	☒	☐	☐
15.	7.1.7	Adaptation de la fréquence de polling. *Si la voie primaire devient indisponible, la fréquence de polling définie pour la voie secondaire reprend celle de la voie primaire.*	☒	☐	☐
16.	7.1.8	Sabotage. *Une rupture des 2 voies de communication doit être considérée comme un sabotage (une alarme est remontée au récepteur).*	☒	☐	☐
17.	6.5.5 7.2	Délai d'attente avant retransmission (programmable). *Le délai d'attente d'une quittance avant de renvoyer un message doit être paramétrable en fonction du type d'alarme, et défini de façon à garantir le délai de transmission max. en tenant compte des retransmissions.*	☒	☐	☐

Annexe 3.1: Exigences pour transmetteur

Les codes sous Réf. correspondent aux sections référencées de la règle de prescription.
En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

			Exigences		Produit
N°	**Réf.**	**Désignation**	**Requis**	**Option**	**OK**
		Fonctionnalités			
18.	5.3	Signalisation locale d'une alarme: Sur transmetteur: ☐ optique détail: ..... ☐ acoustique détail: ..... *Le transmetteur doit afficher au minimum les états « En service / hors service » et « Alarme / pas d'alarme ».*	☒ ☐	☐ ☒	☐ ☐
19.	5.3	Signalisation locale d'une alarme: Via périphériques: ☐ optique détail: ..... ☐ acoustique détail: ..... *La signalisation locale par le biais de périphériques connectés au transmetteur (gyrophare, sirène, etc.) doit être programmable en fonction du type d'alarme et/ou du critère.* *AEAI exige une alarme acoustique en plus de l'alarme optique.*	☐ ☐	☒ ☒	☐ ☐
20.	5.3	Signalisation locale programmable selon type d'alarme. *Par ex. alarme incendie -> activation d'une sirène.*	☒	☐	☐
21.	5.3	Destinataires programmables: ☐ par type d'alarme (pompiers, police ou technique) ☐ par critère (feu, inondation, chimique, effraction, etc.) *Le transmetteur doit supporter la définition d'au moins 8 destinataires par type d'alarme et/ou par critère (cf. matrice « critères vs destinataires » sous 5.3.)* ***Par critère: requis** pour les transmetteurs qui traitent **conjoin-tement** des alarmes **tactiques feu et autres** (p.ex. effraction).*	☒ ☒	☐ ☐	☐ ☐
22.	6.5.9	Notification directe par le transmetteur ? ☐ SMS ☐ MMS ☐ email ☐ autre: ..... *Le transmetteur est capable d'envoyer lui-même une notification en cas d'alarme ou de défectuosité détectée. Cette notification doit pouvoir être personnalisée en fonction du type d'évènement.*	☐	☒	☐
23.	5.3	Serveur web intégré. Protocole(s) supporté(s): ☐ http ☐ https (SSL/TLS) ☐ autre(s): ..... *Pour consulter l'état du transmetteur, la liste des évènements enregistrés, etc. et faire de la maintenance à distance.*	☐ ☐ ☐	☒ ☒ ☒	☐ ☐ ☐
		Sécurité			
24.	6.7.3	Identifiant du transmetteur (programmable). *L'identifiant du transmetteur doit pouvoir être programmé via une interface locale. Il doit toujours être transmis, en clair ou crypté.*	☒	☐	☐

Annexe 3.1: Exigences pour transmetteur

Les codes sous Réf. correspondent aux sections référencées de la règle de prescription.
En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

			Exigences		Produit
N°	**Réf.**	**Désignation**	**Requis**	**Option**	**OK**
25.	6.7.4	Vérification de l'émetteur par un autre critère: ☐ adresse MAC (carte réseau) ☐ N° de série ☐ numéro IMEI (identifiant mobile unique) ☐ numéro MSN (n° de tél. fixe ou mobile) *Ce paramètre permet la différentiation, de manière univoque, de chaque transmetteur.*	☒ ☐ ☐	☐ ☒ ☒	☐ ☐ ☐
26.	6.6.1 6.6.4	Authentification: ☐ Authentification du transmetteur *D'une façon générale, l'authentification est requise pour les initiateurs de communication.*	☒	☐	☐
27.	6.5.4 6.6.2 6.7.1	Protocole de cryptage: ☐ AES ☐ IDEA ☐ Autres:..... Longueur de la clé de cryptage: ☐ 128 bits ☐ 192 bits ☐ 256 bits *Au moins un des deux protocoles ci-dessus (AES, IDEA) doit être supporté. Une clé de cryptage de 128 bits est un minimum requis.* *(Info: la NSA utilise AES 128 bits pour sa classification «secret», et AES 192 ou 256 bits pour sa classification «top secret»).*	☒ ☐ ☐	☐ ☒ ☒	☐ ☐ ☐
28.	6.6.3 6.7.2	Protocole(s) de hachage (contrôle d'intégrité): ☐ SHA-1 ☐ MD5 *Le transmetteur doit supporter l'un des deux protocoles de contrôle d'intégrité si aucun cryptage n'est effectué.*	☐	☒	☐
29.	6.6.5	Firewall intégré: ☐ filtrage des communications entrantes ☐ filtrage des communications sortantes *Le filtrage entrant doit ne laisser passer que les communications émises depuis des adresses IP connues et approuvées (centres de réception et/ou entités chargées de la maintenance).*	☒ ☐	☐ ☒	☐ ☐
30.	6.6.5	Filtrage des numéros d'appelants ? ☐ Access Control List (ACL) *Ce filtrage permet au transmetteur de ne répondre à un appel entrant que si le numéro d'appelant est répertorié dans une liste interne de contrôle d'accès (seuls les centres de transit et/ou entités chargées de la maintenance sont autorisés).*	☐	☒	☐
31.	5.3	Maintenance de sécurité (locale ou à distance): *En cas de serveur web intégré, doit supporter les mises à jour de sécurité nécessaires pour prévenir les attaques depuis Internet (spam, virus, déni de service, etc.)*	☒	☐	☐

Annexe 3.1: Exigences pour transmetteur

Les codes sous Réf. correspondent aux sections référencées de la règle de prescription.
En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

		Divers			
32.	5.3	Alimentation du transmetteur: ☐ DC, fournie par la centrale d'alarme existante ☐ DC, fournie via un transformateur sur réseau 230V ☐ AC, réseau 230V	☒	☐	☐
33.	5.3	Batterie de secours: ☐ interne ☐ externe Autonomie à pleine charge d'au minimum 24h ?: ..... *L'autonomie de la batterie doit être au moins égale à celle de la centrale d'alarme à laquelle le transmetteur est connecté.*	☒	☐	☐
34.	6.7.6	Horloge interne programmable ? Si oui, méthode: ☐ NTP ☐ autre: ..... *La synchronisation de l'horloge interne avec une base de temps de référence est primordiale (requise) pour un traitement correct des évènements.*	☒	☐	☐
35.	6.7.6	Gestion applicative de l'heure d'été / d'hiver ? ☐ automatique ☐ autre: ..... *Attention: le changement d'heure (été/hiver) doit être assuré !*	☒	☐	☐
36.	6.7.6	Horodatage: ☐ date et heure de transmission de l'événement *Toutes les transmissions (sortantes ou entrantes) doivent inclure la date et l'heure effective de transmission.*	☒	☐	☐
37.	5.4	Mémorisation des événements en local: ☐ mode buffer (mémoire tampon) *Si les voies de transmission sont temporairement indisponibles (défectuosité ou maintenance), le transmetteur doit être capable de mémoriser en local les événements potentiels puis de les transmettre automatiquement au récepteur aussitôt qu'une des voies de transmission est à nouveau disponible.*	☒	☐	☐
38.	6.8	Enregistrement des événements: ☐ défectuosité détectée (p.ex. ligne centrale domestique) ☐ type d'évènement avec date et heure de survenance ☐ date et heure de transmission des évènements ☐ enregistrement dans un fichier log *Les événements (défectuosité technique ou message d'alarme) doivent être enregistrés en local sur le transmetteur dans une file d'attente cyclique (les enregistrements les plus anciens sont remplacés par les derniers événements survenus) permettant de mémoriser au moins les 250 derniers évènements (1000 pour les sites à haut risque), selon EN 50131-1.* *Cette liste doit pouvoir être consultée et exportée via les interfaces locales, ou à distance, moyennant les droits d'accès adéquats selon EN 50136-2-1. La tenue d'un fichier log est requise.*	☒ ☒ ☒ ☒	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐

Annexe 3.1: Exigences pour transmetteur

Les codes sous Réf. correspondent aux sections référencées de la règle de prescription.
En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

39.	6.5.10	Supporte la maintenance à distance et les commandes évoluées. *Par exemple, mise à jour du firmware du transmetteur ou pour l'envoi d'informations détaillées dans le cas de la levée de doute.*	☒	☐	☐
40.	6.5.9	Supporte la réception de commandes à distance *Le transmetteur est capable de recevoir des messages de commande ou de télégestion (redémarrage du transmetteur ou activation d'un contact pour une ouverture de porte à distance).* *Les commandes seront envoyées par défaut sur la voie primaire. En cas d'échec, la voie secondaire pourra être utilisée.*	☒	☐	☐

Le centre de réception ci-après s'engage à fournir, sur demande du prescripteur, toutes les informations d'ordre matériel et/ou logiciel relatives au transmetteur proposé et à ses composants. Une documentation détaillée doit être fournie, décrivant le transmetteur et ses fonctionnalités. Une liste des certifications obtenues peut être fournie, le cas échéant.

Les soussignés, engageant valablement le centre de réception mentionné ci-après, déclarent avoir reçu tous les renseignements nécessaires pour compléter le présent document, certifient l'avoir rempli conformément à la réalité, et s'engagent à satisfaire aux exigences susmentionnées, en respectant les prescriptions, normes et règlements en vigueur.

Lieu, date: ....

Nom et fonction: ....

Timbre et signature: ....

Annexe 3.2: Exigences pour système de réception (centre officiel et/ou de transit)

S'applique aux centres de réception officiels et/ou de transit (réception et/ou traitement de critères tactiques).

Les codes sous Réf. correspondent aux sections référencées de règle de prescription.

En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

Equipement proposé (Marque/modèle): .....

			Exigences		Produit
N°	**Réf.**	**Désignation**	**Requis**	**Option**	**OK**
		Généralités			
1.	5.4	Surveillance interne (watchdog). *Le système de réception dispose d'un mécanisme lui permettant de surveiller ses interfaces et son état de fonctionnement.*	☒	☐	☐
		Interfaces			
2.	5.4	Interfaces de communication (voies de transmission): ☐ Ethernet 10/100+ selon IEEE 802.3 ☐ GPRS ☐ EDGE ☐ autre: ..... ☐ PSTN ☐ RNIS ☐ GSM *Dans tous les cas, le récepteur doit être atteignable par deux voies physiquement séparées.*	☒ ☐ ☐	☐ ☒ ☒	☐ ☐ ☐
3.	5.4	Interfaces de communication (périphériques locaux): ☐ RS232 nombre: ..... ☐ USB nombre: ..... ☐ autres: ..... nombre: ..... *Pour maintenance locale ou raccordement d'équipements spéciaux tels que webcam, GPS, imprimante ou autre.*	☒ ☐ ☐	☐ ☒ ☒	☐ ☐ ☐
		Communication			
4.	6.5.2	Adressage IP: ☐ **adresse IP fixe (publique)**	☒	☐	☐
5.	5.4 5.5	Protocole de transmission : a. Supporte le standard de communication ANSI/SIA DC-09:2007 pour les transmissions numériques via IP • En entrée • En sortie b. Autre(s) protocole(s) supportés en entrée ou sortie : ..... *Le protocole **DC-09 est requis** pour la réception d'alarmes tactiques à un centre officiel ainsi que pour le transfert d'alarmes tactiques vers un centre officiel (s'applique aux centres de transit).*	☒ ☒	☐ ☐	☐ ☐
6.	--	Gestion de la priorité des messages (traitement). *Les évènements reçus doivent être traités dans l'ordre de survenance en tenant compte des priorités définies selon le type d'alarme et/ou le critère.* *Ce point consiste en une gestion intelligente de la file d'attente en cas d'afflux massif de messages.* ***Requis** pour les centres de réception qui traitent conjointement des alarmes **tactiques feu ainsi que d'autres types d'alarmes** (p.ex. effraction).*	☒	☐	☐

Annexe 3.2: Exigences pour système de réception (centre officiel et/ou de transit)

S'applique aux centres de réception officiels et/ou de transit (réception et/ou traitement de critères tactiques).

Les codes sous Réf. correspondent aux sections référencées de règle de prescription.

En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

			Exigences		Produit
N°	**Réf.**	**Désignation**	**Requis**	**Option**	**OK**
7.	6.5.7 7.1.7	Doit être atteignable par deux voies physiquement séparées. *Les deux voies doivent être en permanence atteignables, le basculement de la transmission des alarmes s'effectue côté transmetteur.*	☒	☐	☐
8.	6.5.8	Quittancement d'une alarme. *Tous les messages reçus correspondant aux critères traités par le centre de réception doivent être quittancés. Ceci permet aux transmetteurs d'avoir la confirmation que le système de réception a bien reçu le message, que ce message a été transmis sans erreur (checksum) et que le centre est à même de le traiter.* *Si une conversion de protocole est requise, l'envoi de quittances devra être adressé via un centre de transit.*	☒	☐	☐
9.	6.5.9	Messages de commande / Télégestion. *Le centre de réception et/ou de traitement peut envoyer des messages de commande pour la télégestion des transmetteurs affiliés sur ces deux voies de communication.*	☒	☐	☐
10.	6.7.5	Protocoles de communication supportés: ☐ TCP ☐ UDP ***Le système de réception doit supporter les 2 protocoles susmentionnés**.*	☒	☐	☐
11.	7.1.1	Fréquence de polling programmable. Intervalle ajustable entre ..... et ..... (durée) *La durée entre 2 pollings doit satisfaire aux exigences spécifiées dans la règle de prescription pour la surveillance dite permanente.*	☒	☐	☐
12.	7.1.5	Surveillance périodique (polling). *Le récepteur doit connaitre l'intervalle de polling de chacun de ses transmetteurs clients et pouvoir générer une alarme s'il n'a rien reçu dans un délai défini.*	☒	☐	☐
13.	7.1.8	Sabotage. *Une rupture des 2 voies de communication doit être considérée comme un sabotage (une alarme est remontée au récepteur ou centre de traitement des alarmes).*	☒	☐	☐
		Fonctionnalités			
14.	5.4	Signalisation locale d'une alarme: Sur récepteur: ☐ optique détail: ..... ☐ acoustique détail: ..... *Le système de réception doit afficher au minimum les états « En service / hors service » et « Alarme / pas d'alarme ».*	☒ ☒	☐ ☐	☐ ☐
15.	5.4	Signalisation locale d'une alarme: Via périphériques: ☐ optique détail: ..... ☐ acoustique détail: ..... *La signalisation locale par le biais de périphériques connectés au système de réception (gyrophare, sirène, etc.) doit être programmable en fonction du type d'alarme et/ou du critère.*	☐ ☐	☒ ☒	☐ ☐

Annexe 3.2: Exigences pour système de réception (centre officiel et/ou de transit)

S'applique aux centres de réception officiels et/ou de transit (réception et/ou traitement de critères tactiques).

Les codes sous Réf. correspondent aux sections référencées de règle de prescription.

En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

			Exigences		Produit
N°	**Réf.**	**Désignation**	**Requis**	**Option**	**OK**
16.	5.3	Destinataires programmables: ☐ par type d'alarme (pompiers, police ou technique) ☐ par critère (feu, inondation, chimique, effraction, etc.) *Le système de réception doit supporter la définition d'au moins 8 destinataires par type d'alarme et/ou critère pour le **transfert** au(x) centre(s) officiel(s) spécifique(s).*	☒ ☒	☐ ☐	☐ ☐
17.	--	Notification au client: ☐ SMS ☐ MMS ☐ email ☐ autre: ..... *Le système de réception doit pouvoir envoyer une notification au client en cas d'alarme ou de défectuosité détectée. Cette notification doit pouvoir être personnalisée en fonction du type d'évènement.*	☒	☐	☐
18.	5.4	Serveur web intégré: protocoles supportés: ☐ http ☐ https (SSL/TLS) ☐ autre(s): ..... *Pour consulter la liste des évènements enregistrés, afficher les alarmes traitées, celles en cours de traitement, etc.*	☐ ☐ ☐	☒ ☒ ☒	☐ ☐ ☐
19.	5.5	Concept de redondance côté réception: ☐ 2+0 (2 récepteurs sur le même site, locaux séparés) ☐ 1+1 (2 sites différents avec 1 récepteur chacun) *Les centres de réception **doivent** disposer d'au moins 2 systèmes de réception ou assurer la redondance par un centre de suppléance.*	☒	☐	☐
20.	5.6	Filtrage et transfert: ☐ Le système de réception est capable de filtrer les messages reçus en fonction du type d'alarme ☐ Le système de réception est capable de filtrer les messages reçus en fonction du critère ***Au moins une des 2 exigences ci-dessus doit être remplie**.*	☒	☐	☐
		Sécurité			
21.	6.7.3	Identifiant du système de réception (programmable) *L'identifiant du système de réception doit pouvoir être transmis, en clair ou crypté.*	☒	☐	☐
22.	6.7.4	Vérification de l'émetteur par un autre critère: ☐ adresse MAC (carte réseau) ☐ N° de série ☐ numéro IMEI (identifiant mobile unique) ☐ numéro MSN (n° de tél. fixe ou mobile).	☒	☐	☐
23.	6.6.1 6.6.4	Authentification: ☐ Authentification du récepteur *D'une façon générale, l'authentification est requise pour les initiateurs de communication. Elle s'applique donc également au récepteur, initiateur pour la maintenance centralisée à distance.*	☒	☐	☐

Annexe 3.2: Exigences pour système de réception (centre officiel et/ou de transit)

S'applique aux centres de réception officiels et/ou de transit (réception et/ou traitement de critères tactiques).

Les codes sous Réf. correspondent aux sections référencées de règle de prescription.

En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

			Exigences		Produit
N°	**Réf.**	**Désignation**	**Requis**	**Option**	**OK**
24.	6.5.4 6.6.2 6.7.1	Protocoles de cryptage: ☐ AES ☐ IDEA ☐ Autres:..... Longueur de la clé de cryptage: ☐ 128 bits ☐ 192 bits ☐ 256 bits *Le système de réception **doit supporter les 3 niveaux** de cryptage AES et au minimum les 2 algorithmes de cryptage susmentionnés (AES et IDEA).*	 ☒ ☒ ☒	 ☐ ☐ ☐	 ☐ ☐ ☐
25.	6.6.3 6.7.2	Protocole(s) de hachage (contrôle d'intégrité): ☐ SHA-1 ☐ MD5 *Le système de réception doit supporter les deux protocoles de contrôle d'intégrité si aucun cryptage n'est effectué.*	 ☐ ☐	 ☒ ☒	 ☐ ☐
26.	6.6.5	Firewall intégré (côté amont) ☐ filtrage des communications entrantes ☐ filtrage des communications sortantes *Le filtrage du trafic entrant et sortant doit pouvoir être paramétré indépendamment avec des règles spécifiques adaptées.*	 ☒ ☒	 ☐ ☐	 ☐ ☐
27.	6.6.5	Filtrage des numéros d'appelants ? ☐ Access Control List (ACL) *Ce filtrage permet au système de réception de ne répondre à un appel entrant que si le numéro d'appelant est répertorié dans une liste interne de contrôle d'accès (entités autorisées).*	 ☐	 ☒	 ☐
28.	5.4	Maintenance de sécurité (locale ou à distance): *Supporte les mises à jour de sécurité nécessaires pour prévenir les attaques depuis Internet (spam, virus, déni de service, etc.)*	☒	☐	☐
		Divers			
29.	5.4	Alimentation du système de réception: ☐ AC, réseau 230V, simple ☐ AC, réseau 230V, double (redondance) ☐ DC, fournie via un transformateur sur réseau 230V	 ☒	 ☐	 ☐
30.	5.4	Alimentation sans coupure (onduleur): ☐ interne ☐ externe Autonomie à pleine charge: ..... *L'autonomie de l'onduleur doit être adaptable aux conditions fixées par le centre de réception.*	 ☒	 ☐	 ☐

Annexe 3.2: Exigences pour système de réception (centre officiel et/ou de transit)

S'applique aux centres de réception officiels et/ou de transit (réception et/ou traitement de critères tactiques).

Les codes sous Réf. correspondent aux sections référencées de règle de prescription.

En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

			Exigences		Produit
N°	**Réf.**	**Désignation**	**Requis**	**Option**	**OK**
31.	5.4	Mémorisation des événements en local: ☐ mode buffer (mémoire tampon) *Si le système supérieur est temporairement indisponible (défectuosité ou maintenance), le système de réception doit pouvoir mémoriser les événements potentiels en local puis de les transmettre automatiquement dès que le système supérieur est à nouveau disponible.*	☒	☐	☐
32.	6.5.10	Supporte l'envoi de commande de maintenance à distance et les commandes évoluées. *Le système de réception est capable d'envoyer des messages de commande ou de télégestion (redémarrage du transmetteur ou activation d'un contact).* *Les commandes seront envoyées par défaut sur la voie primaire, sur la voie secondaire si la voie primaire n'est pas disponible. Si une conversion de protocole est requise, l'envoi de commandes devra être adressé via un centre de transit.*	☒	☐	☐
33.	6.5.11	Supporte la maintenance à distance *Par exemple, mise à jour du firmware du récepteur. En principe la voie primaire sera utilisée.*	☒	☐	☐
34.	6.7.6	Horloge interne: synchronisation ☐ NTP ☐ autre: --------- *La synchronisation de l'horloge interne avec une base de temps de référence est primordiale (requise) pour un traitement correct des évènements.*	☒	☐	☐
35.	6.7.6	Gestion applicative de l'heure d'été / d'hiver ? ☐ automatique ☐ autre: --------- *Attention: le changement d'heure (été/hiver) doit être assuré !*	☒	☐	☐
36.	6.7.6	Horodatage: date et heure ☐ de survenance d'un événement (transmis) ☐ de transmission de l'événement (transmis) ☐ de réception de l'événement (transmis) *La date et l'heure de survenance d'un événement et de sa transmission effective sont transmises avec le message.* *Le système de réception doit pouvoir mémoriser la date et l'heure de réception du message dans un fichier log ou une base de données.*	☒ ☒ ☒	☐ ☐ ☐	☐ ☐ ☐

Annexe 3.2: Exigences pour système de réception (centre officiel et/ou de transit)

S'applique aux centres de réception officiels et/ou de transit (réception et/ou traitement de critères tactiques).

Les codes sous Réf. correspondent aux sections référencées de règle de prescription.

En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée.

			Exigences		Produit
N°	**Réf.**	**Désignation**	**Requis**	**Option**	**OK**
37.	6.8	Enregistrement des événements: ☐ défectuosité détectée (p.ex. interface) ☐ type d'évènement avec date et heure de survenance ☐ date et heure de transmission des évènements ☐ date et heure de réception des évènements ☐ enregistrement dans un fichier log *Les événements (défectuosité technique ou message d'alarme) doivent être enregistrés en local sur le récepteur dans une file d'attente cyclique (les enregistrements les plus anciens sont remplacés par les derniers événements survenus). Le système de réception* ***doit être dimensionné de sorte à pouvoir mémoriser les événements des 3 derniers mois****, selon R31.* *Cette liste doit pouvoir être consultée et exportée via les interfaces locales, ou à distance moyennant les droits d'accès adéquats selon EN 50136-2-1. La tenue d'un fichier log est requise.*	 ☒ ☒ ☒ ☒ 	 ☐ ☐ ☐ ☐ 	 ☐ ☐ ☐ ☐

Le centre de réception ci-après s'engage à fournir, sur demande du prescripteur, toutes les informations d'ordre matériel et/ou logiciel relatives au système de réception et à ses composants. Une documentation détaillée doit être fournie, décrivant le système de réception et ses fonctionnalités. Une liste des certifications obtenues peut être fournie, le cas échéant.

Les soussignés, engageant valablement le centre de réception mentionné ci-après, déclarent avoir reçu tous les renseignements nécessaires pour compléter le présent document, certifient l'avoir rempli conformément à la réalité, et s'engagent à satisfaire aux exigences susmentionnées, en respectant les prescriptions, normes et règlements en vigueur.

Lieu, date: ....

Nom et fonction: ....

Timbre et signature: ....

Annexe 3.3 : Exigences pour infrastructures d'un centre de réception

S'applique aux centres de réception officiels et/ou de transit (réception et/ou traitement de critères tactiques)

En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée. L'Autorité compétente peut, le cas échéant, délivrer des dérogations pour les centres de transit.

Note: les modes [2+0] et [1+1] mentionnés ci-après font référence à l'architecture de la redondance, selon règle de prescription, chapitre 5.5.

Identification du centre: .....

		Exigences		
N°	**Désignation**	**Requis**	**Option**	**OK**
	Télécom / courant faible			
1.	Deux introductions par bâtiment (FO et/ou cuivre)	☒	☐	☐
2.	Voies de communication selon règle de prescription	☒	☐	☐
3.	Une antenne GSM par récepteur (externe si nécessaire)	☒	☐	☐
4.	Si récepteurs installés dans un même bâtiment (mode 2+0):	[2+0]		
	- installation dans des locaux séparés, physiquement distants (conformément aux prescriptions AEAI)	☒	☐	☐
	- raccordement par des chemins de câbles distincts (1 chemin de câble par récepteur)	☒	☐	☐
5.	Câblage universel de catégorie 5, classe D-2002 (selon ISO 11801, édition 2) ou supérieur	☐	☒	☐
	Alimentation électrique et éclairage			
6.	Alimentation sans interruption :			
	- par onduleur (ASI avec batteries)	☒	☐	☐
	- par génératrice (p.ex. diesel)	☐	☒	☐
	- autonomie minimum en cas de coupure : 24 h	☒	☐	☐
7.	Si récepteurs installés dans un même bâtiment :			
	- récepteurs alimentés par 2 alimentations distinctes (pas sur la même phase ou le même onduleur)	☐	☒	☐
8.	Eclairage de secours :	☒	☐	☐
	- autonomie minimum en cas de coupure : 24 h	☒	☐	☐
	Locaux techniques et opérationnels			
9.	Chemins de câbles :			
	Le câblage de communication installé respecte les normes et prescriptions en vigueur (ISO 11801, EN 50173, …)	☒	☐	☐
10.	Garantie de température ambiante maximum au sein des locaux techniques (max. 26° selon recommandation OFEN)	☒	☐	☐
11.	Protection incendie (selon implémentation) :	[2+0]	[1+1]	
	- porte coupe-feu pour le local avec les équipements	☒	☒	☐
	- passages de câbles coupe-feu pour ces mêmes locaux	☒	☒	☐
	- coffre anti-feu pour les dossiers d'intervention	☒	☒	☐
12.	Contrôle d'accès :			
	- contrôle d'accès par badge	☒	☐	☐
	- accès limité au personnel d'exploitation autorisé	☒	☐	☐
	- vidéosurveillance	☐	☒	☐
	- traçabilité, enregistrement	☒	☐	☐

Annexe 3.3 : Exigences pour infrastructures d'un centre de réception

S'applique aux centres de réception officiels et/ou de transit (réception et/ou traitement de critères tactiques)

En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée. L'Autorité compétente peut, le cas échéant, délivrer des dérogations pour les centres de transit.

Note: les modes [2+0] et [1+1] mentionnés ci-après font référence à l'architecture de la redondance, selon règle de prescription, chapitre 5.5.

		Exigences		
N°	**Désignation**	**Requis**	**Option**	**OK**
13.	système anti-agression	☒	☐	☐
	Protection bâtiment			
14.	Mise à terre selon prescriptions Electrosuisse	☒	☐	☐
15.	- parasurtensions (selon directives USIE) - paratonnerre (selon prescriptions Electrosuisse) - parafoudre (selon prescripteur cantonal)	☒ ☐ ☐	☐ ☒ ☒	☐ ☐ ☐
	Equipements de réception			
16.	Deux systèmes de réception mutuellement redondants	☒	☐	☐
17.	Installation / environnement : - équipements dans 2 bâtiments distincts, ou - installation dans le même bâtiment (2 locaux distincts)	 ☒ ☒	 ☐ ☐	 ☐ ☐
18.	Rack pour les équipements (1 par local ou par site)	☐	☒	☐
19.	Systèmes d'enregistrement redondants	☐	☒	☐
	Intégration IT / sécurité			
20.	Récepteurs placés dans une zone protégée (DMZ)	☒	☐	☐
21.	Zone protégée par firewall : - vis-à-vis du réseau informatique interne - vis-à-vis d'Internet - firewall redondant (requis pour [2+0] [1], optionnel pour [1+1] [2])	 ☒ ☒ ☒ [1]	 ☐ ☐ ☒ [2]	 ☐ ☐ ☐
22.	Equipements actifs (switches, routeurs) : - infrastructure backbone redondante (1+1) - switches et routeurs interconnectés en redondance (1+1) - équipements actifs alimentés par des ASC	 ☐ ☐ ☒	 ☒ ☒ ☐	 ☐ ☐ ☐
23.	Equipements de communication : - téléphonie (vecteurs fixe et mobile) - télécommunication (accès distant, VPN) - messagerie (email, autres) - enregistrement de toutes les conversations téléphoniques	 ☐ ☐ ☐ ☒	 ☒ ☒ ☒ ☐	 ☐ ☐ ☐ ☐
24.	Pour les centres de transit, routage automatique des alarmes tactiques, sans intervention humaine	☒	☐	☐
	Exploitation (cf. Directives techniques SES, annexe 5)			
25.	Présence de personnel technique : - sur site 24h/24 (requis pour centre officiel)	 ☒	 ☐	 ☐

Annexe 3.3 : Exigences pour infrastructures d'un centre de réception

S'applique aux centres de réception officiels et/ou de transit (réception et/ou traitement de critères tactiques)

En cochant la case dans la colonne OK l'exploitant du centre de réception confirme sa conformité à l'exigence spécifiée. L'Autorité compétente peut, le cas échéant, délivrer des dérogations pour les centres de transit.

Note: les modes [2+0] et [1+1] mentionnés ci-après font référence à l'architecture de la redondance, selon règle de prescription, chapitre 5.5.

		Exigences		
N°	**Désignation**	**Requis**	**Option**	**OK**
26.	Directives d'exploitation :			
	- processus d'exploitation, scenarii	☒	☐	☐
	- matériel requis pour donner / transmettre une alarme	☐	☒	☐
	- équipements de protection incendie (extincteurs, …)	☒	☐	☐
27.	Dossiers d'intervention :			
	- dossiers en version papier en lieu sûr (coffre)	☒	☐	☐
	- fichiers informatiques accessibles à qui de droit	☒	☐	☐
	- sauvegardés à 2 endroits distincts	☐	☒	☐

Autres exigences

Exigences envers les centrales d'alarme incendie et les installations de transmission des alarmes.

cf. « Directives techniques SES, Installations de détection d'incendie », consultables à l'adresse ci-dessous :

http://sicher-ses.ch/F_B/html/installations_de_detection_d_i.html

Le centre de réception s'engage à fournir, sur demande du prescripteur, toutes les informations relatives aux infrastructures au sein de son centre, en particulier à ses composants et équipements. Une documentation détaillée doit être fournie, décrivant les infrastructures et leurs fonctionnalités. Une liste des certifications obtenues peut être fournie, le cas échéant.

Les soussignés, engageant valablement le centre de réception mentionné en page 1, déclarent avoir reçu tous les renseignements nécessaires pour compléter le présent document, certifient l'avoir rempli conformément à la réalité, et s'engagent à satisfaire aux exigences susmentionnées, en respectant les prescriptions, normes et règlements en vigueur.

Lieu, date: ....

Nom et fonction: ....

Timbre et signature: ....