ECA
Prévenir Secourir Assurer

Alarmes automatiques

Transmissions sécurisées d'alarmes sur IP
Complément technique à la Règle de prescription

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

ECA
Incendie et éléments naturels

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

POLICE

Police cantonale Fribourg

Transmission sécurisée d'alarmes sur IP
Complément technique à la Règle de prescription

Ce document a pour objectif de clarifier certains points de la Règle de prescription v1.5 de décembre 2009, potentiellement sujets à interprétation, afin de garantir une implémentation uniforme du protocole DC-09 par les différents constructeurs et assurer l'interopérabilité entre produits.

Il permet en outre d'identifier plus clairement les paramètres requis et optionnels décrits dans la règle de prescription, et de les situer soit dans le datagramme DC-09, soit dans les en-têtes IP ou TCP/UDP, voire même pour certains de les déduire d'autres paramètres transmis et donc de les exclure de la transmission elle-même.

Plusieurs scénarios sont illustrés entre la transmission d'un événement par un transmetteur client et les diverses possibilités de quittancement par le récepteur, ainsi que le contrôle de ligne et l'envoi de commandes.

Ce complément technique est appliqué 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

Ce document a pour objectif de clarifier certains points de la Règle de prescription v1.3 de juillet 2009, potentiellement sujets à interprétation, afin de garantir une implémentation uniforme du protocole DC-09 par les différents constructeurs et assurer l'interopérabilité entre produits.

Il permet d'identifier plus clairement les paramètres requis et optionnels décrits dans la règle de prescription, et de les situer soit dans le datagramme DC-09, soit dans les en-têtes IP ou TCP/UDP, voire même pour certains de les déduire d'autres paramètres transmis et donc de les exclure de la transmission elle-même.

1.1 Conventions d'écriture

Les conventions d'écriture suivantes sont appliquées dans le présent document, dans les différents chapitres décrivant les datagrammes DC-09 :

- Si un paramètre est **requis** il est inscrit **en gras**.
- Les paramètres optionnels sont inscrits en orange.

1.2 Terminologie

TR : Transmetteur (ou PE, Premises Equipment).

CSR : Système de réception (Central Station Receiver).

CTA : Centre de Traitement des Alarmes (centre officiel).

CT : Centre de Transit (tous types d'alarmes).

2 Définitions

Les définitions suivantes s'appliquent en particulier aux en-têtes de colonnes du tableau du chapitre 5.

2.1 DC-09 de base

Paramètres définis du standard ANSI/SIA DC-09:2007 en l'état.

2.2 DC-09 extensions

Paramètres transmis dans les champs d'extension de données (x.data). Les données d'extension sont identifiées par des balises spécifiques (cf. 6.1.3).

2.3 Autre

Paramètres pas transmis dans les champs de données du datagramme DC-09 mais ailleurs (par exemple dans l'en-tête IP), voire pas transmis du tout mais déduits du code de critère transmis.

2.4 Format d'entrée

Format ou codage d'origine des données à transmettre. Le format d'entrée est spécifié dans le champ "id" du datagramme DC-09. Les autres champs sont repris tels quels dans le datagramme DC-09.

Important: Pour simplifier l'implémentation, le prescripteur a décidé de ne supporter qu'**un seul format d'entrée** au niveau de son système de réception**,** en l'occurrence le format **SIA-DCS.** Le prescripteur se réserve le droit de supporter ultérieurement d'autres formats d'entrée selon l'évolution des standards.

2.5 Code de critère

Code de 2 caractères (pour le SIA-DCS), identifiant un événement spécifique (p.ex. FA, Fire Alarm). Une liste des codes supportés par le prescripteur sera publiée séparément.

Le code de critère est suivi d'une adresse sur 4 chiffres (toujours complétée, soit par ex. 0004), appelée "zone", correspondant à l'adresse de contact du code de critère.

2.6 Cryptage

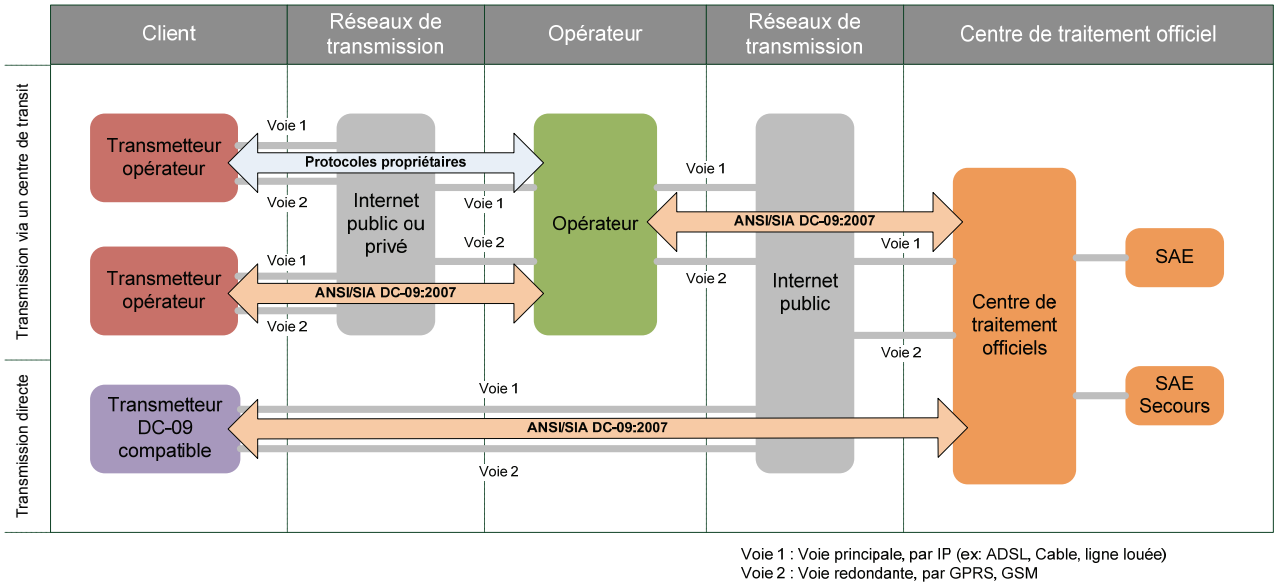
Le prescripteur demande que les données qui lui sont adressées soient cryptées. Toutefois, la méthode de cryptage est laissée libre, pour autant que les pré-requis soient respectés (cf. Règle § 6.7.1). Le cryptage doit être fait au niveau des datagrammes DC-09.

Dans le cas d'une communication cryptée, le prescripteur ne demande pas de fonction de hachage. Si la transmission est non cryptée, le hachage est obligatoire.

3 Architecture

3.1 Modèle global

Le principe global de transmission des alarmes automatiques est présenté sur la figure suivante:

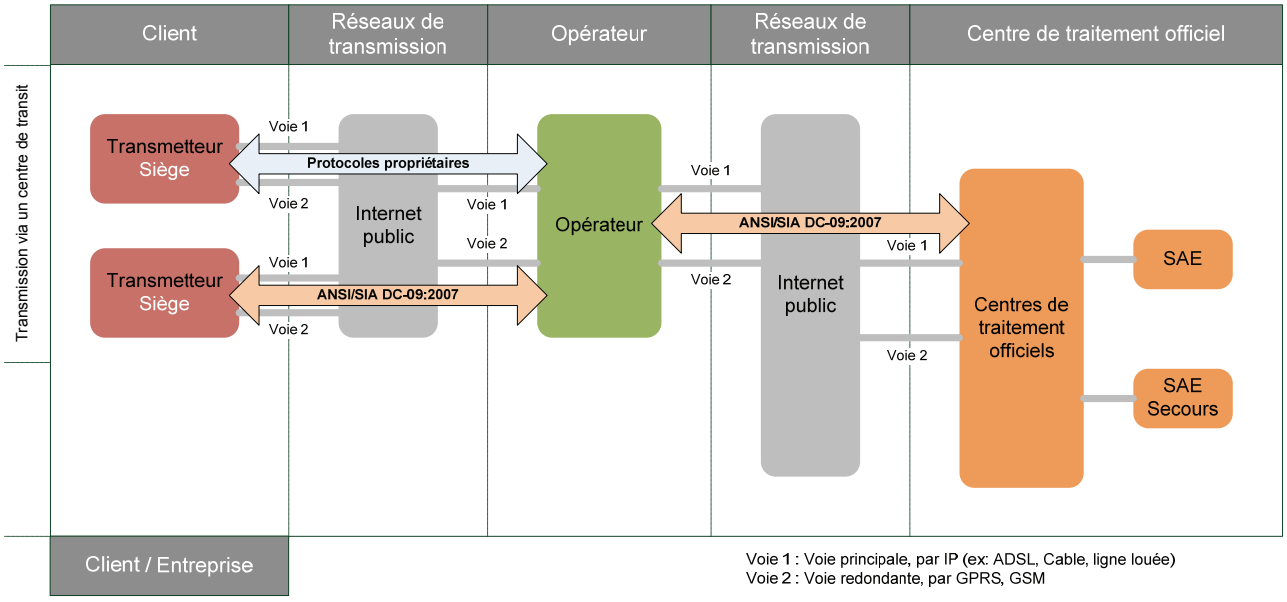


Voie 1 : Voie principale, par IP (ex: ADSL, Cable, ligne louée)
Voie 2 : Voie redondante, par GPRS, GSM

Pour obtenir les explications détaillées de cette figure, se référer à la Règle de prescription.

3.2 Exemple d'implémentation n°1

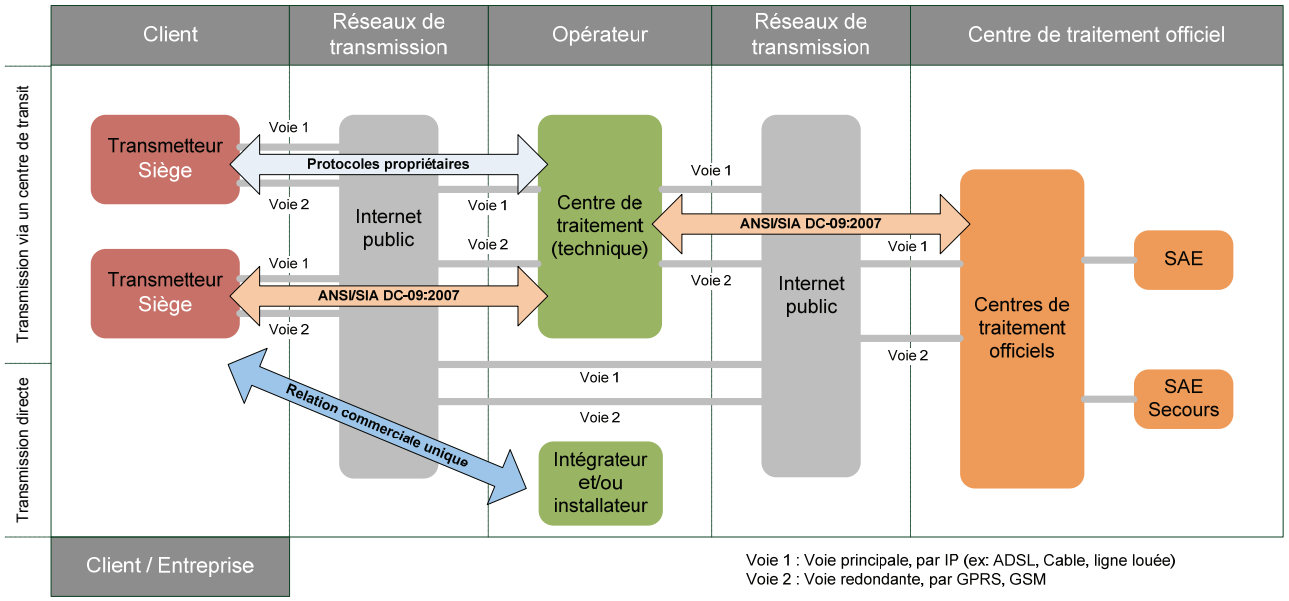
La figure suivante schématise **<u>un exemple d'implémentation</u>** de la transmission. Ce schéma propose une implémentation possible de la transmission des alarmes automatiques pour une entreprise ne désirant pas effectuer la réception et le traitement des alarmes techniques. Dans ce cas, l'Opérateur propose une solution "clé en main".



Voie 1 : Voie principale, par IP (ex: ADSL, Cable, ligne louée)
Voie 2 : Voie redondante, par GPRS, GSM

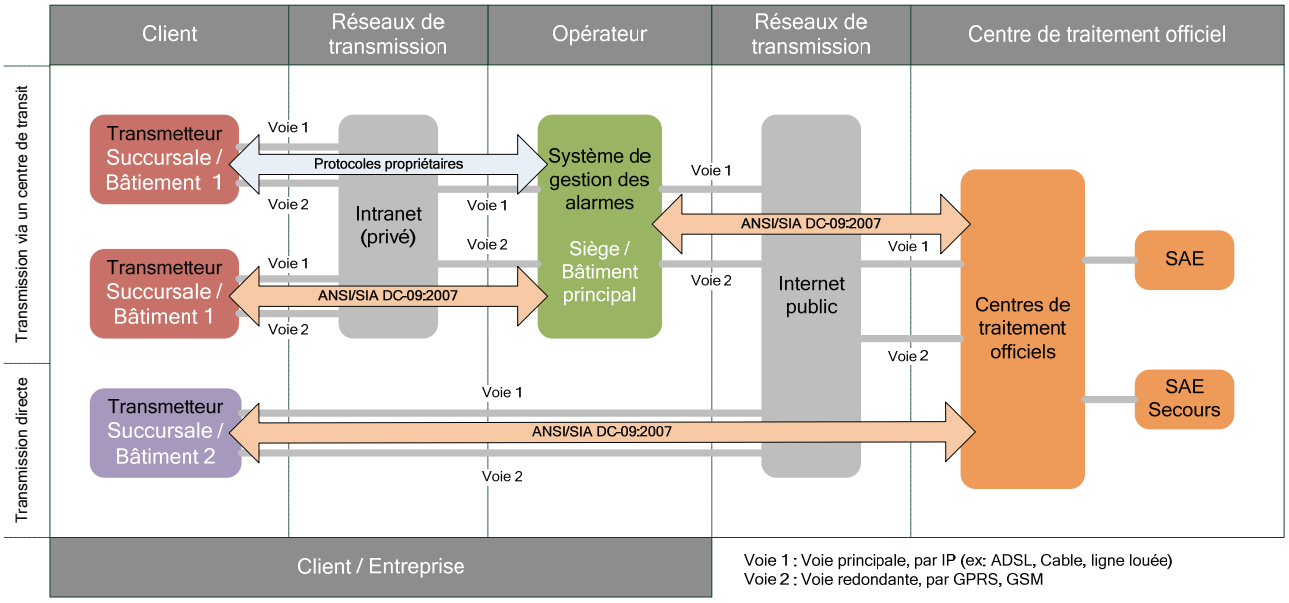
3.3 Exemple d'implémentation n°2

La figure suivante schématise **un exemple d'implémentation** de la transmission. Ce schéma propose une implémentation possible de la transmission des alarmes automatiques pour une entreprise désirant gérer ces propres transmetteurs, mais mandate une société externe pour effectuer la réception et le traitement des alarmes techniques.



3.4 Exemple d'implémentation n°3

La figure suivante schématise **un exemple d'implémentation** de la transmission. Ce schéma propose une implémentation possible de la transmission des alarmes automatiques pour une entreprise désirant gérer de bout en bout la transmission des alarmes.



3.5 Remarques générales sur l'implémentation

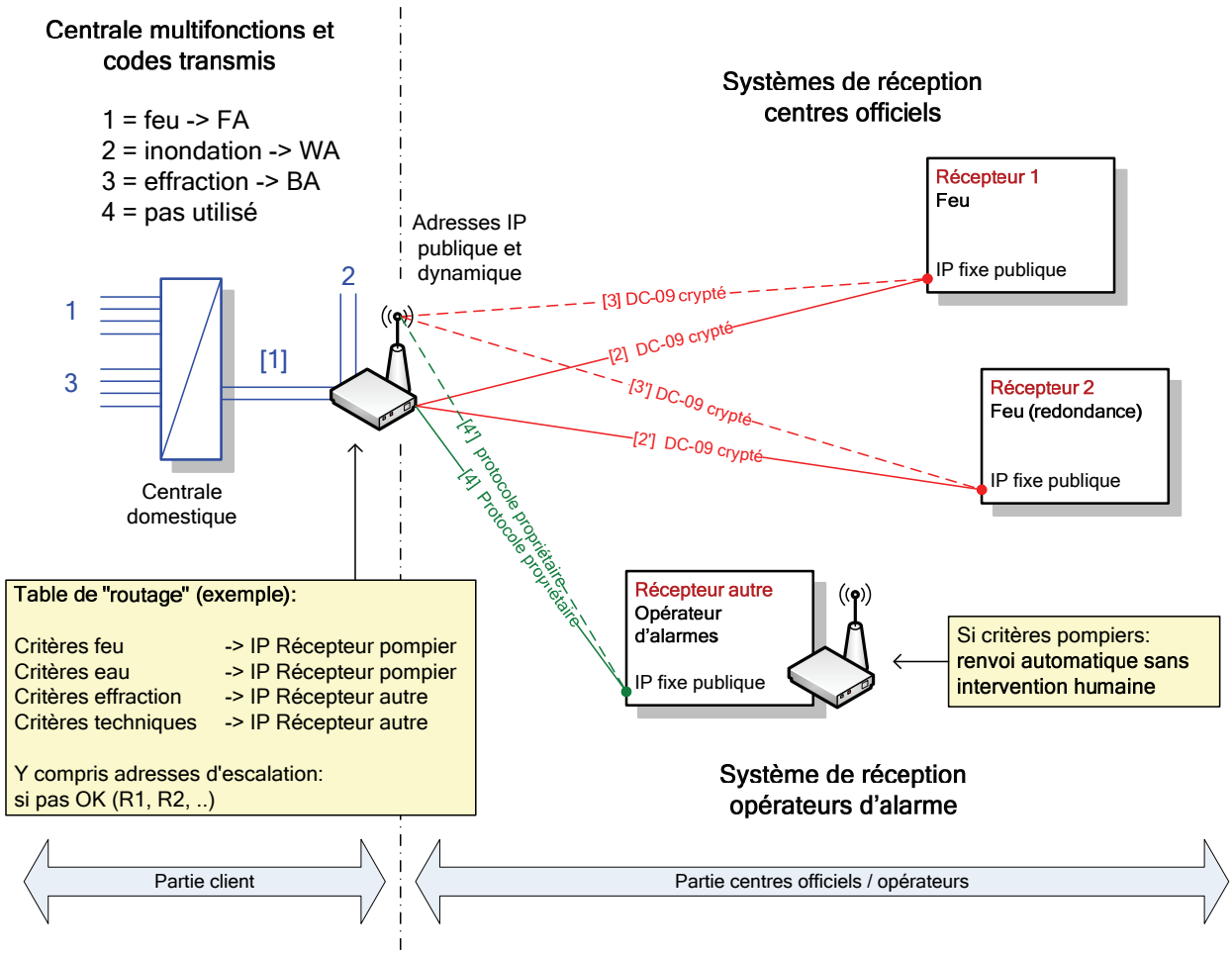
Dans certains cas, il est tout à fait envisageable que le réseau privé de l'entreprise et ses accès à Internet soient utilisés pour transmettre les alarmes aux différents centres officiels (exemple 3.4). En effet, plusieurs services peuvent transiter sur un même réseau IP. Dans ce cas précis, la société en question devient elle-même opérateur d'alarme au sens des Directives Organisationnelles.

Le serveur d'alarme (ou système de gestion des alarmes) peut être situé à l'intérieur même de l'entreprise, lui permettant de traiter les critères techniques nécessaire au bon fonctionnement de l'entreprise et de ses installations. Il est également envisageable de confier cette tâche à un prestataire externe (exemple 3.3). Dans ce cas, le prestataire externe reçoit et traite les alarmes techniques, mais ne gère pas administrativement les clients (raccordements).

Les transmetteurs envoient leurs informations à l'Opérateur, au(x) Centre(s) de traitement officiels ou au Système de gestion des alarmes (d'après les exemples en dessus), les critères techniques sont traités sur place. En ce qui concerne les critères tactiques, un renvoi automatique doit être effectué vers le centre officiel correspondant.

4 Principe et séquence de la transmission

Le schéma suivant illustre le cas d'une centrale domestique multifonctions qui transmet ses événements par des contacts secs ou par RS232 à un transmetteur qui génère les datagrammes correspondants et les envoie au(x) destinataire(s) respectif(s) dans le format approprié :



[1] : Message en sortie de la centrale domestique, par contacts ou via RS232, protocoles divers.

[2] : Message formaté en DC-09, encapsulé dans un datagramme IP et crypté: choix du centre officiel (prescripteur).

[2'] : Même message que [2], mais renvoyé au récepteur redondant, car aucune réponse du système de réception Récepteur 1 n'a été obtenue.

[3] : Même message que [2] (et [2']) mais renvoyé sur une voie alternative, car aucune réponse des systèmes de réception sur la voie primaire n'à été obtenue.

[3'] : Même message que [3], mais renvoyé au récepteur redondant sur une voie alternative, car aucune réponse du système de réception Récepteur 1 n'a été obtenue.

[4] : Message en format autre, protocole selon opérateur, doit respecter les directives du prescripteur pour les critères à transférer (critères pompiers).

[4']: Même message que [4], mais renvoyé au récepteur sur une voie alternative, car aucune réponse du système de réception Récepteur 1 n'a été obtenue.

Message [4] « retransmis » automatiquement par l'opérateur d'alarmes, car l'alarme concernée est une alarme tactique traitée par le centre officiel.

La retransmission n'est pas représentée, mais respecte le même séquencement que précédemment: [2], [2'], [3] et [3'].

Remarques:

Le séquencement présenté est valable pour une alarme Feu.

Si l'Opérateur d'alarmes reçois et traite les alarmes Effraction ou les critères techniques, à savoir pannes de la centrale domestique, déconnection du transmetteur, informations techniques sur l'état des systèmes du bâtiment, ces alarmes sont traitées sur place et aucune retransmission n'a lieue.

L'Opérateur d'alarmes peut avoir la fonction de:

- Centre de transit pour tout les types d'alarme (Feu, Effraction et technique) : reçois toutes les alarmes, traite une partie d'entre elle et retransmet de manière automatique si besoin est. Dans ce cas, il gère administrativement les clients.
- Centre de réception et traitement : reçois et traite uniquement les alarmes Effraction et/ou technique.

Dans le premier cas, le centre de transit a, à la fois une fonction d'Opérateur d'alarme et de gestionnaire administratif des clients (raccordements). Dans le deuxième cas, l'Opérateur d'alarmes est uniquement un centre de traitement des alarmes, il ne s'occupe pas de la gestion administrative des clients et de leurs raccordements.

5 Paramètres requis et optionnels

Paramètres requis et optionnels selon Règle de prescription et correspondance avec le standard DC-09 ou autre.

Paramètres requis (cf. Règle, 6.2.1)	**DC-09 de base**	**DC-09 extension**	**Autre**	**Longueur / format**	**Commentaire**
Numéro d'événement, unique	`seq`			4 chiffres	Un numéro par événement (0001-9999)
Identifiant de message (incrémental)	`data`				
Critère d'alarme: feu | pollution | effraction | etc.	`data`			2-3 car. hex	Caractères hexadécimaux 0-9, A-F
Priorité: haute | normale | basse (P0 | P1 | P2)			Pas transmis		Gérée par récepteur selon code de critère
Etat de l'alarme: active | quittancée | rétablie | TEST	`data`				Code de critère spécifique
Adresse IP de l'émetteur			En-tête IP		
Adresse IP du destinataire			En-tête IP		
Identifiant du transmetteur (p.ex. n° de série)	`#acct`			`#`+3-16 car. hex	Ev. reprise du n° AlarmNet (si existant)
Format d'origine du message (cf. formats approuvés)	`"id"`			cf. DC-07	SIA-DCS – selon liste du prescripteur
Date et heure de l'événement	`x.data`			20 caractères	Format _HH:MM:SS,MM-DD-YYYY
Date et heure de transmission	`timestamp`			20 caractères	Format _HH:MM:SS,MM-DD-YYYY
Paramètres optionnels (cf. Règle, 6.2.2)	**DC-09 de base**	**DC-09 extension**	**Autre**	**Longueur / format**	**Commentaire**
Port source (émetteur)			En-tête TCP/UDP		Paramétrable
Port de destination (destinataire)			En-tête TCP/UDP		Paramétrable
Adresse MAC du transmetteur	`x.data`	`Mxxxx`		`M`+12 car. hex	Prévu pour contrôle de substitution
Identifiant du destinataire	`Rrcvr`			`R`+1-6 car. hex	(pas utilisé)
Texte de l'alarme (description ou commentaire)	`x.data`	`Iccc..cc`		`I`+c caractères	Directive du prescripteur (`I` pourr Info)
Nom du site d'où provient l'alarme (texte ou code)	`x.data`	`Sccc..cc`		`S`+c caractères	Directive du prescripteur (`S` pour Site)
Bâtiment d'où provient l'alarme (texte ou code)	`x.data`	`Occc..cc`		`O`+c caractères	Directive du prescripteur (`O` pour Object)
Lieu du site d'où provient l'alarme (texte ou code)	`x.data`	`Qccc..cc`		`L`+c caractères	Directive du prescripteur (`L` pour Location)
Local d'où provient l'alarme (code alphanumérique)	`x.data`	`Rccc..cc`		`R`+c caractères	Directive du prescripteur (`R` pour Room)
Déclencheur d'alarme (n° détecteur ou poussoir)	`x.data`	`Tccc..cc`		`T`+c caractères	Directive du prescripteur (`T` pour Trigger)
Coordonnées x (115000 à 205000)	`x.data`	`Xnnnnnn`		`X`+6 chiffres	Directive du prescripteur
Coordonnées y (490000 à 590000)	`x.data`	`Ynnnnnn`		`Y`+6 chiffres	Directive du prescripteur
Coordonnées z (altitude)	`x.data`	`Znnnn`		`Z`+1-4 chiffres	Directive du prescripteur

Information du type d'alarme (pompiers | police | technique):

Le type d'alarme sera déduit du code de critère, mais l'information ne sera pas transmise pour éviter d'éventuelles incohérences.

Information de priorité:

Conformément au point 4.6 de la règle de prescription, les messages d'alarme sont prioritaires par rapport aux autres informations.

Cette exigence s'applique avant tout au système de réception (CSR) qui doit traiter les alarmes avant le reste. La gestion de la priorité n'est pas requise au niveau du transmetteur (TR) compte tenu du temps très court lors d'un envoi séquentiel et de la faible probabilité de survenance simultanée d'un critère d'alarme (urgent) et d'un critère technique (non urgent). La priorité sera déterminée par le système de réception en fonction du code de critère transmis mais aucune information de priorité (code ou texte) ne sera transmise pour éviter d'éventuelles incohérences.

Information de voie de transmission utilisée:

Même chose pour l'information de voie de transmission utilisée, qui n'a pas besoin d'être transmise. Elle sera détectée par le TR et le système de réception.

Informations supplémentaires (optionnelles, cf. Règle, section 6.2.2):

Les informations ci-après, peuvent être transmises optionnellement ou sur exigence expresse de l'Autorité compétente (liste non exhaustive):

- Adresse texte de l'émetteur ou identifiant, peut être directement tirée de la base de données selon le numéro de dossier.
- 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.

6 Types de messages

6.1 Messages d'événement (alarme feu)

Transmis généralement par le transmetteur client (PE Premises Equipment).

Syntaxe pour les messages d'événement, selon ANSI/SIA DC-09:2007 (transmis sans saut de ligne):

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

LF	Caractère ASCII Line Feed (0A en hexadécimal).
CRC	Contrôle de redondance cyclique (somme de contrôle, voir plus bas).
LLL	Longueur du message (3 digits hexadécimaux, précédés par le caractère zéro).
"id"	**Code identifiant le format d'entrée (cf. « Token » dans DC-07-2001.04).**
seq	**Numéro de séquence (0001-9999, pas incrémenté lors d'un renvoi).**
rcvr	Identifiant du récepteur, si utilisé (1-6 digits hexadécimaux, précédés d'un R).
pref	**Préfixe (1-6 digits hexadécimaux, précédés d'un L).**
acct	**Identifiant du transmetteur (3-16 digits hexadécimaux, précédés par un #).**
pad	Caractères de remplissage (uniquement quand le message est crypté).
data	Champ de données, libre, sans limite de longueur, syntaxe selon format d'entrée.
x.data	Paramètre d'extension, identifiable par la « balise » suivant le caractère « [». Sa valeur est le texte compris entre la balise et le crochet de fermeture «] ».
timestamp	Horodatage, heure de transmission du message, requis si le message est crypté (20 caractères, format "_HH:MM:SS,MM-DD-YYYY")
CR	Caractère ASCII Carriage Return (0D en hexadécimal)

Le contrôle de redondance cyclique (CRC) permet de détecter les erreurs de transmission par ajout de redondance (somme de contrôle). Le CRC est calculé avant et après la transmission ou duplication, puis comparé pour s'assurer que c'est le même.

Pour les messages cryptés, le CRC est calculé <u>après</u> le cryptage du message (données et horodatage).
En cas de renvoi, le message est ré-encrypté avec l'horodatage mis à jour.

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".

Le numéro de séquence 0000 est réservé pour les messages de supervision (NULL) et NAK.

Le préfixe, requis dans la syntaxe DC-09, consiste en 1 à 6 caractères hexadécimaux précédés d'un L. Selon directive du prescripteur, les 2 premiers caractères suivant le L identifient l'opérateur d'alarmes. Les 4 caractères suivants sont optionnels (utilisation future). Les identifiants d'opérateurs sont attribués par le prescripteur, d'entente avec les opérateurs concernés.

6.1.1 Précisions sur le champ data

Dans le champ `data`, les données utiles du message sont celles qui suivent le caractère « | ». Dans ce champ, des balises spécifiques (« qualifiers ») sont utilisées pour identifier les informations.
Ces balises diffèrent selon le format d'entrée défini dans le champ `"id"` (cf. DC-07-2001.04). En format SIA le qualifier pour un nouveau message est « `N` ».

Exemple:

Nouveau message, alarme eau (`WA`), zone 3 (format SIA-DCS) :

```
…|NWA0003]
<x0D>
```

6.1.2 Précisions sur les champs x.data

Les paramètres d'extension (`x.data`) sont utilisés pour transmettre les différents paramètres optionnels.
Ces paramètres sont codés selon la syntaxe « `[Xccc...cc]` » où `X` est la balise d'identification du paramètre (cf. 6.1.3) et `ccc...cc` sa valeur (texte de longueur variable compris entre la balise et le crochet de fermeture). Cette syntaxe s'applique à chaque paramètre d'extension.

Les paramètres d'extension peuvent ainsi être mis à la suite l'un de l'autre, dans n'importe quel ordre, chaque paramètre étant identifié par une balise univoque. La syntaxe « `<[><balise><valeur><]>` » doit être respectée pour chacun de ces paramètres.

La chaîne `<valeur>` ne doit pas contenir les caractères « `[` », « `|` » ou « `]` ».

6.1.3 Balises définies pour les champs x.data

Balises réservées dans le standard DC-09 (**en gras**) ou par le prescripteur pour les champs d'extension (selon DC-09 seules les lettres `G` à `Z` sont utilisables) :

Balise	Affectation	Format/longueur du champ
G		
H	Heure de survenance d'un événement	Format _HH:MM:SS,MM-DD-YYYY
I	Description (Information)	C caractères, longueur variable
J		
K		
L	Lieu ou étage (Location)	C caractères, longueur variable
M	**Adresse MAC**	**12 caractères hexa**
N		
O	Bâtiment (Object)	C caractères, longueur variable
P	**Données de Programmation**	**Libre (usage futur)**
Q		
R	Local (Room)	C caractères, longueur variable
S	Site ou campus (p.ex. EPFL)	C caractères, longueur variable
T	Déclencheur d'alarme (Trigger)	C caractères, longueur variable
U		
V	**Données de Validation**	**Libre (usage futur)**
W		
X	Coordonnées X	6 chiffres (115000 à 205000)
Y	Coordonnées Y	6 chiffres (490000 à 590000)
Z	Altitude (Z) ou numéro d'étage	1-4 chiffres

Note:

Les champs d'extension descriptifs, ayant pour valeur des chaînes de caractères de longueur variable, peuvent contenir des caractères accentués (ASCII 8 bits doit être supporté).

6.1.4 Déclencheur d'alarme (Trigger)

Le déclencheur d'alarme peut être un détecteur automatique (p.ex. détecteur feu, fumée, gaz, eau, etc.), semi-automatique (p.ex. sonde de température, d'humidité ou de pression, contact, etc.) ou un déclencheur manuel (p.ex. poussoir d'alarme).

Le déclencheur est identifié par une balise de type (`B`), suivie d'un identifiant alphanumérique de longueur libre (syntaxe: `[TBident]`). Les balises de type suivantes ont été définies par le prescripteur:

Balise	Affectation	Type
`F`	Détecteur feu / fumée (Fire)	Automatique
`G`	Détecteur Gaz (Gas)	Automatique
`W`	Détecteur eau / inondation (Water)	Automatique
`S`	Sonde (temp. / humid. / pression)	Semi-automatique
`C`	Contact (effraction ou autre)	Semi-automatique
`M`	Déclencheur Manuel (p.ex. poussoir)	Manuel

Syntaxe :

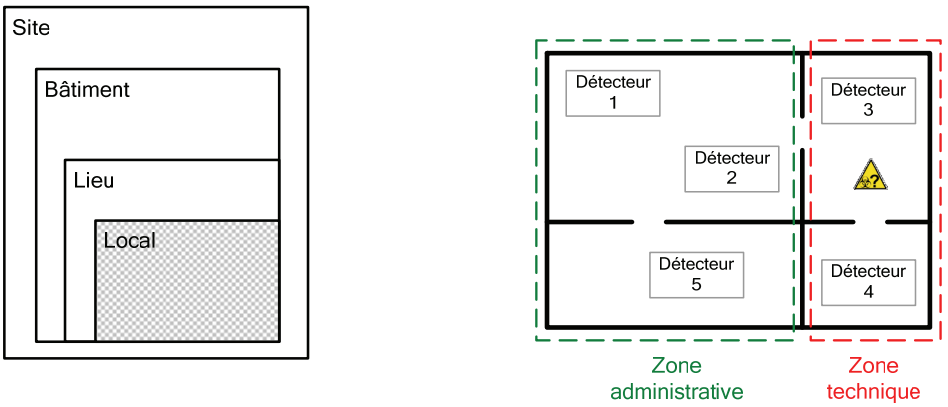
```
…<data>][Xnnnnnn][Ynnnnnn][Snom_du_site][Onom_du_bâtiment][Llieu][Rlocal]
[TBident][Itexte_descriptif][H_ HH:MM:SS,MM-DD-YYYY]
<x0D>
```

Exemple :

Message d'événement avec, comme paramètres optionnels, les coordonnées géographiques (533475/152263), le nom du site (EPFL), le bâtiment (Odyssea), le lieu (02 2ème étage), le local (B-205), le déclencheur d'alarme (détecteur gaz n°003), la description de l'événement / commentaire (texte descriptif) et l'heure de survenance:

```
…<data>][X152263][Y533475][SEPFL][OOdyssea][L02][RB-205]
[TG003][Itexte_descriptif][H_13:14:15,11-20-2008]
<x0D>
```

6.1.5 Arborescence – Synthèse



Dans cette arborescence, le Lieu peut être assimilé à une Zone (par exemple administrative ou technique), un département ou un étage. C'est le niveau de granularité intermédiaire entre le Bâtiment et le Local.

Dans l'exemple ci-dessus, l'affectation des locaux de la Zone Technique (par exemple dépôt de solvants) requiert des critères spécifiques (alarme chimique,…), inutiles pour la Zone Administrative (par exemple bureaux).

Si l'on ne dispose que d'un seul critère générique pour l'alarme pompiers (feu, gaz, inondation, chimique,…), le critère dominant sera considéré, mais les moyens engagés pourraient être surévalués.

6.1.6 Exemples de message en DC-09 (selon ANSI/SIA DC-09:2007)

Dans les exemples suivants, les paramètres ci-après sont utilisés:

CRC: XXXX (appliqué sur la portion de données cryptées)

seq: 9876

rcvr: - (pas utilisé dans les exemples suivants)

pref: 789ABC (les 2 premiers digits identifient l'opérateur d'alarmes)

acct: 12345A

Cas 1 : alarme feu, zone 129, format SIA DCS, crypté, avec horodatage

```
<x0A>XXXX007D
"*SIA-DCS"9876L789ABC#12345A
[<x44179D26F6D423A6569543>|#12345A|NFA0129]_13:14:15,11-20-2008<x0D>
```

Dans cet exemple, le datagramme est représenté avant le cryptage du texte compris entre le "[" d'ouverture et le <x0D> de fermeture. La portion de texte à crypter est surlignée en gris. On retrouve l'identifiant (acct), le N qui indique que c'est un nouveau message, le code de critère (FA, Fire Alarm), la zone (0129) et l'horodatage. Le message étant crypté, 11 octets de remplissage sont rajoutés. Le longueur du paquet (7D) est donnée après cryptage.

Cas 2 : alarme intrusion, zone 65, format SIA DCS, non crypté, avec adresse MAC

```
<x0A>8580003B
"SIA-DCS"9876L789ABC#12345A
[#12345A|NBA0065][M1234567890AB]<x0D>
```

Dans cet exemple, le N indique que c'est un nouveau message; il est suivi du code d'alarme cambriolage (Burglary Alarm, BA en format SIA), du numéro de zone, codé sur 4 chiffres (0065) et de l'adresse MAC à la suite du M dans le champ d'extension. Il n'inclut pas d'horodatage et pas de caractères de remplissage (message non crypté).

Dans les exemples ci-dessus, la zone qui suit le code de critère, fait référence à l'adresse de contact telle que définie sous 2.5.

6.2 Messages de quittancement

Transmis généralement par le système de réception (CSR, Central Station Receiver).

Le quittancement renvoyé accuse uniquement la réception du message transmis, ce n'est en aucun cas un quittancement opérationnel (typiquement, de prise en charge, défini dans un système d'aide à l'engagement en aval du processus ou dans tout autre système supérieur).

6.2.1 Quittancement positif (ACK)

Lorsqu'un message reçu est validé (somme de contrôle vérifiée et critère connu et supporté) le système répond par un quittancement positif (ACK). Syntaxe selon ANSI/SIA DC-09:2007:

```
<LF><CRC><0LLL>
<"ACK"><seq><Rrcvr><Lpref><#acct>[]
<CR>
```

Exemple :

```
<x0A>D6F30019
"ACK"9876L789ABC#12345A
[]<x0D>
```

Si le système répond positivement à un message crypté, le quittancement ACK est également crypté :

```
<LF><CRC><0LLL>
<"*ACK"><seq><Rrcvr><Lpref><#acct>[<pad>]<timestamp>
<CR>
```

Exemple :

```
<x0A>XXXX0059
"*ACK"9876L789ABC#12345A
[<x125A88A46F0E48DE8E68C3>]_13:14:15,11-20-2008<x0D>
```

6.2.2 Quittancement négatif (NAK)

Si la somme de contrôle d'un message reçu diffère de celle d'origine (transmise avec le message), le récepteur renvoie une quittance négative (NAK) au transmetteur pour qu'il renvoie le message.

De même, si l'heure de transmission transmise dans un message horodaté dépasse la tolérance de décalage admise (+20s/-40s) par rapport à l'heure du récepteur, ce dernier répond par un quittancement négatif, avec un horodatage de référence pour que le transmetteur ajuste son horloge interne:

<LF><CRC><0LLL> <"**NAK**"><**0000**><**R0**><**L0**><**A0**>[]<**timestamp**> <CR>

Le message NAK a toujours le numéro de séquence `0000` et n'est jamais crypté.

Exemple :

```
<x0A>2F780025
"NAK"0000R0L0A0
[]_11:11:38,12-14-2009<x0D>
```

6.2.3 Quittancement d'incapacité (DUH)

Si le récepteur reçoit un message correctement structuré mais ne sait pas comment le traiter, il répond par un quittancement d'incapacité (DUH, Data Unable to Handle):

<LF><CRC><0LLL> <"**DUH**"><**seq**><Rrcvr><**Lpref**><**#acct**>[] <CR>

Le message DUH n'est jamais crypté.

Exemple :

```
<x0A>05C90019
"DUH"9876L789ABC#12345A
[]<x0D>
```

6.2.4 Messages de supervision (NULL)

Le transmetteur et/ou le système de réception peuvent être configurés pour vérifier périodiquement la connexion par l'envoi d'un message de supervision (NULL). Le destinataire est supposé répondre par un quittancement positif (ACK) dans un intervalle de temps donné. cf. SIA DC-09:2007, section 5.5.2.

<LF><CRC><0LLL> <"**NULL**"><**0000**><Rrcvr><**Lpref**><**#acct**>[]<timestamp> <CR>

Les messages NULL ont toujours le numéro de séquence `0000`.

L'horodatage (timestamp) est optionnel pour les messages NULL non cryptés.

Exemple :

```
<x0A>3DCD001A
"NULL"0000L789ABC#12345A
[]<x0D>
```

Cas d'un message de supervision crypté :

<LF><CRC><0LLL> <"***NULL**"><**0000**><Rrcvr><**Lpref**><**#acct**>[<pad>]<**timestamp**> <CR>

L'horodatage (timestamp) est requis pour les messages NULL cryptés.

Exemple :

```
<x0A>XXXX005A
"*NULL"0000L789ABC#12345A
[<x6EC1C9C4C7B43FBD8D1D72>]_13:14:15,11-20-2008<x0D>
```

7 Envoi de commande

Ce chapitre décrit l'envoi de commandes du centre de réception (CSR ou CT) au transmetteur (TR), pour des applications de gestion à distance (p.ex. commande d'ouverture, de fermeture de vannes, déverrouillage de porte à distance, activation d'un signal optique ou sonore sur le site distant, télégestion, maintenance à distance, etc.).

La Règle définit des commandes simples et évoluées. Les commandes simples sont traitées dans ce document. Les commandes dites évoluées, sont utilisées pour de la télégestion, soit par exemple, pour la mise à jour logicielle du transmetteur, ou encore la demande d'informations permettant une levée de doute. Elles sont généralement utilisées par les opérateurs d'alarmes pour la maintenance des transmetteurs, et dans certains cas, pour effectuer une levée de doute.

Dans ce sens, le prescripteur part du principe que les commandes évoluées sont du ressort de l'opérateur d'alarme; mais le prescripteur se réserve néanmoins le droit de les exiger pour effectuer une levée de doute. Les commandes simples restent requises au niveau du transmetteur et du récepteur.

7.1 Commandes simples

Les commandes simples sont envoyées par le récepteur au transmetteur à la place d'un message d'acquittement (ACK) provoqué par un polling ou un message d'alarme. Pour ce faire, c'est le paquet DC-09 RSP qui est utilisé. Par conséquent le paquet RSP doit être considéré par le transmetteur comme un ACK. La syntaxe de ce paquet est la suivante:

```
<LF><CRC><0LLL>
<"RSP"><seq><Rrcvr><Lpref><#acct>[…rsp.data…]
<CR>
```

Si le message de polling ou d'alarme est crypté, le paquet RSP le sera:

```
<LF><CRC><0LLL>
<"*RSP"><seq><Rrcvr><Lpref><#acct>[<pad>…rsp.data…]<timestamp>
<CR>
```

…rsp.data… correspond à:

#acct|NZZCCnnnn

Avec:

N	Pour nouveau message
ZZ	Code de critère fixe, indiquant l'envoi d'une commande.
CC	Code de critère correspondant au type d'action, suivant la liste du prescripteur.
nnnn	Numéro de zone (correspond au numéro du contact physique).

Par exemple, non crypté:

```
<x0A>A3AF002A
"RSP"9876L789ABC#12345A
[#12345A|NZZRC0065]<x0D>
```

Par exemple, crypté (avant cryptage):

```
<x0A>XXXX0079
"*RSP"9876L789ABC#12345A
[<x29B43891FF0C3AA69E>|#12345A|NZZRC0065]_13:14:15,11-20-2008
<x0D>
```

Dans ces exemples, le code de critère `RC` est utilisé pour la fermeture d'un relais. Le `ZZ` indique une commande, le transmetteur doit fermer le relais correspondant au contact `0065`.

Dans le deuxième exemple, c'est la partie grisée qui est cryptée, soit le message qui débute par du remplissage, et fini par l'horodatage.

7.2 Processus d'envoi de la commande et de quittancement

En cas d'envoi de commandes, le message de quittancement (ACK) est remplacé par le message de commande (RSP). Le transmetteur doit considérer le polling (ou l'alarme) quittancé en recevant le RSP.

Ensuite, le transmetteur doit quittancer la bonne réception du message et le changement d'état demandé par le récepteur. Pour ce faire, il envoie un message d'alarme, avec comme code de critère le code utilisé pour la commande (par exemple `RC`).

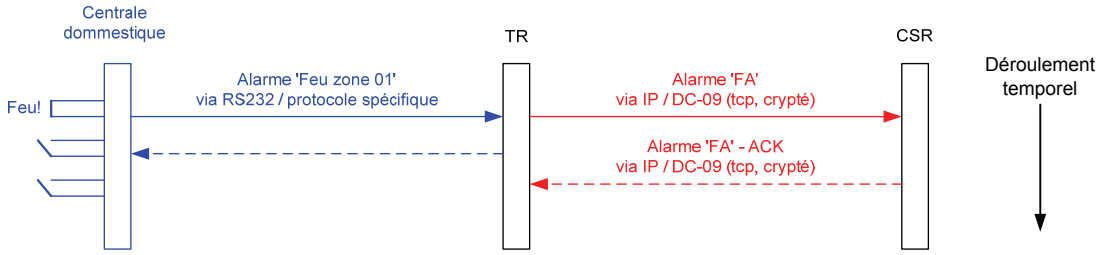
Finalement, le récepteur envoie un message d'acquittement en fonction (ACK, DUH, NULL), puisque la validation de la commande envoyée par le transmetteur est un message d'alarme standard.

8 Scénarii

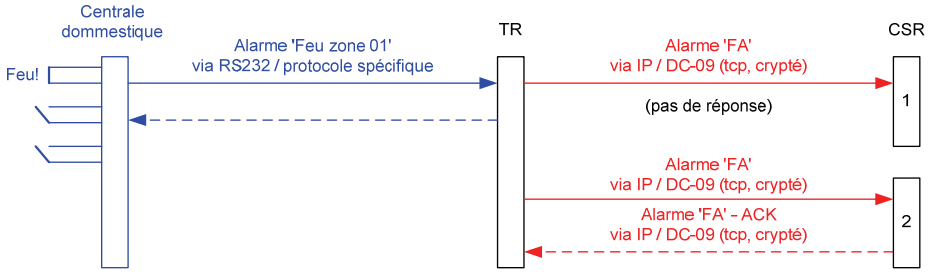
Les scénarii ci-après illustrent les différents cas de figure entre la transmission d'un événement par un transmetteur client et les diverses possibilités de quittancement par le récepteur, ainsi que le contrôle de ligne et l'envoi de commandes.

8.1 Scénario 1 – Alarme feu envoyée au CTA et ACK

- Message alarme feu envoyé au CTA en DC-09 (crypté, selon choix du prescripteur).
- Quittance ACK (OK, crypté car en réponse à un message crypté).

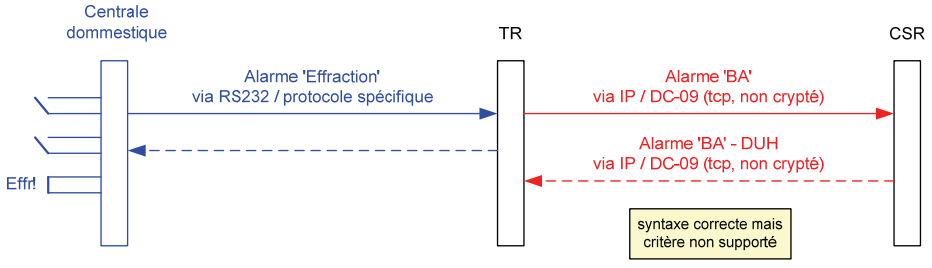


8.1.1 Escalade en cas de non réponse



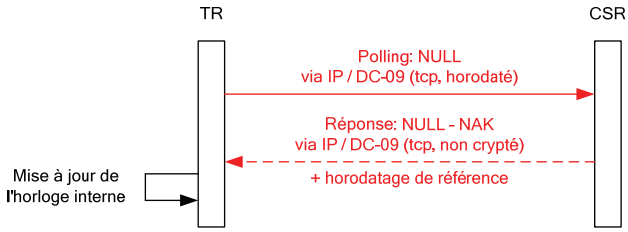
8.2 Scénario 2 – Message avec code non supporté et DUH

- Message événement avec code de critère non supporté ou inconnu, adressé au CTA (non crypté).
- Quittance DUH (pas supporté / pas connu, jamais crypté).



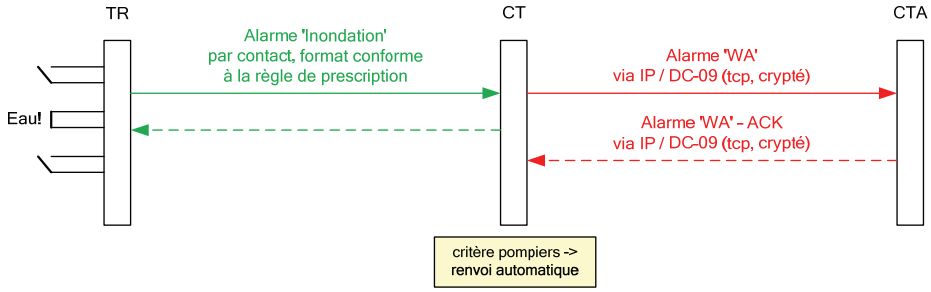
8.3 Scénario 3 – Message avec horodatage incorrect et NAK

- Message de supervision (polling, horodaté) / test de ligne depuis le transmetteur (NULL).
- Horodatage incorrect -> quittance NAK (PAS OK, jamais crypté) avec heure de référence.



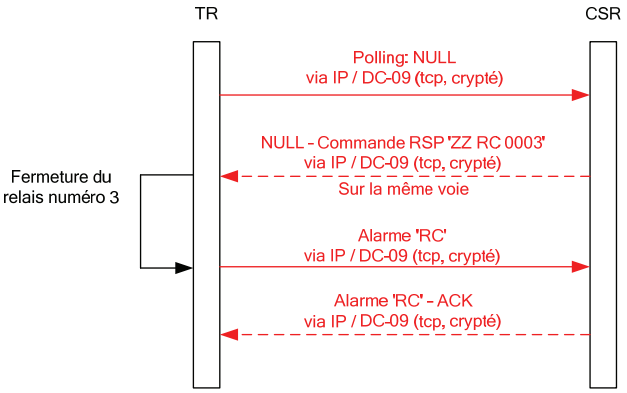
8.4 Scénario 4 – Alarme inondation au CTA via centre de transit

- Message alarme inondation adressé au CT en format conforme, puis relayé au CTA en DC-09:



8.5 Scénario 5 – Commandes à distance

- Message de supervision (polling, horodaté) / test de ligne depuis le transmetteur (NULL).
- Commande de fermeture de contact depuis le système de réception (RSP).
- Quittance ACK.



9 En-têtes IP, TCP et UDP

Ce chapitre permet de situer certains paramètres requis ou optionnels de la règle de prescription (selon chapitre 5 du présent document), qui ne figurent pas dans le datagramme DC-09 mais dans les en-têtes IP, TCP ou UDP, nécessaires au transport de l'information sur IP.

9.1 En-tête IP

Version (4 bits)	Longueur d'en-tête (4 bits)	Type de service (8 bits)	Longueur totale (16 bits)	
Identification (16 bits)			Drapeau (3 bits)	Décalage fragment (13 bits)
Durée de vie (8 bits)		Protocole (8 bits)	Somme de contrôle en-tête (16 bits)	
Adresse IP source (32 bits)				
Adresse IP destination (32 bits)				
Données				

Le champ **Protocole** indique, en décimal, le protocole utilisé (6=TCP, 17=UDP)

La **somme de contrôle** de l'en-tête IP, codée sur 16 bits, permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission.

9.2 En-tête TCP

Source Port (16 bits)							Destination Port (16 bits)
Sequence Number (32 bits)							
Acknowledgment Number (32 bits)							
Offset / Reserved	URG	ACK	PSH	RST	SYN	FIN	Window (16 bits)
Checksum (16 bits)							Urgent Pointer (16 bits)
Options (24 bits)							Padding

URG: si ce flag est à 1 le paquet doit être traité de façon prioritaire.

La somme de contrôle de l'en-tête TCP (**checksum**), codée sur 16 bits, appliquée aux champs de données de l'en-tête, permet de vérifier l'intégrité de l'en-tête.

9.3 En-tête UDP

Port Source (16 bits)	Port Destination (16 bits)
Longueur (16 bits)	Somme de contrôle (16 bits)
Données (longueur variable)	

Le **port de destination** est défini par l'opérateur d'alarmes (pour TCP et UDP).