

Transmission des alarmes automatiques issues d'installations obligatoires de détection et d'extinction incendie

Directive pour le canton de Vaud

PAGE DE GARDE

Par leurs présentes signatures, les soussignés appartenant à l'Etablissement d'assurance contre l'incendie et les éléments naturels du canton de Vaud de l'ECA attestent avoir dûment validés le contenu de la présente *Directive pour le canton de Vaud*.

Jérôme Frachebourg
Directeur Général

Jean-Marc Lance
Directeur de la Division prévention

Edition :

Etablissement d'assurance contre l'incendie et les éléments naturels du canton de Vaud
Division Prévention
Av. Général Guisan 56
CH-1009 Pully
+41 58 721 23 51
alarmeip2016@eca-vaud.ch
octobre 2016

Edition :


Etablissement d'assurance contre l'incendie et les éléments naturels du canton de Vaud
Division Prévention
Av. Général Guisan 56
CH-1009 Pully
+41 58 721 23 51
alarmeip2016@eca-vaud.ch
octobre 2016

Directive pour le canton de Vaud

Ce document décrit le modèle de transmission des alarmes automatiques issues d'installations de détection et d'extinction incendie à destination du Centre de Traitement des Alarmes (« CTA ») du canton de Vaud.

Comme il s'appuie sur les normes suisses et européennes relatives aux systèmes de transmission d'alarmes de tous types (incendie, intrusion, contrôle d'accès, alarme sociale,...), le modèle associé peut s'appliquer également à la transmission d'alarmes de tout type (effraction, techniques en particulier) vers des centres officiels ou non officiels. Par conséquent, un transmetteur utilisé pour l'alarme incendie peut également transmettre d'autres alarmes (utilisation mixte).

Ce document concerne les centres officiels d'urgence suivants :

VD 	Centre de Traitement des Alarmes (CTA – 118)

Version 2.2 – Août 2016

Cette version remplace et annule toutes les précédentes.

Sommaire

1	Domaine d'application	7
2	Références normatives	7
3	Définitions - abréviations	8
3.1	AE – Equipement d’annonce	8
3.2	ARC – Centre de réception des alarmes	8
3.3	AS – Système d’alarme	8
3.4	ATS – Système de transmission d’alarme	8
3.5	ATSN - réseau de services de transmission d'alarme	9
3.6	ATP - Voie de transmission d'alarme (« Alarm Transmission Path »)	9
3.7	CTA – Centre de traitement des alarmes (incendie, hold-up, alarmes techniques)	9
3.8	Centre de réception des dérangements	9
3.9	Centre de télésurveillance de l'ATS, centre de télésurveillance de transmission d'alarme	9
3.10	MCT – Emetteurs-récepteurs de centre de télésurveillance	10
3.11	Organisation d’alarmes & levée de doute	10
3.12	RCT – Transmetteur du centre de réception (récepteur)	10
3.13	SPT – Transmetteur du bâtiment surveillé (transmetteur)	11
3.14	UTC – temps universel coordonné (ou Universal Time Coordinated)	11
4	Objet	12
4.1	Modèle de transmission	12
4.2	Utilisateurs prévus	12
4.3	Structure du document	13
5	Exigences relatives à la classification des bâtiments (affectation des objets) en fonction de la « Valeur de risque de prévention incendie »	14
5.1	Méthodologie retenue	14
5.2	Tableau associant la « Valeur de risque prévention incendie » et les configurations d’ATS exigées	14
6	Exigences relatives au système	15
6.1	Exigences générales	15
6.2	Exigences système	16
6.3	Performances	17
6.4	Sécurisation des messages	18
6.5	Acquittement de la transmission	18
6.6	Alarmes générées par l'ATS	18
6.7	Disponibilité	18
6.8	Sécurité	19
6.9	Vérification de performance	19
6.10	Documentation	20
7	Exigences relatives au transmetteur (SPT)	21

7.1	Exigences générales.....	21
7.2	Exigences fonctionnelles	25
7.3	Documentation	27
7.4	Boîtier et protection contre la fraude – exigences relatives à la protection contre la fraude	27
7.5	Performances / Tests et essais effectués	28
8	Exigences relatives au récepteur (RCT).....	28
8.1	Exigences générales.....	29
8.2	Exigences fonctionnelles	29
8.3	Documentation	33
8.4	Performances / Tests et essais effectués	34
9	Exigences relatives aux protocoles de transmission et de communication.....	36
9.1	Exigences générales.....	36
9.2	Exigences fonctionnelles selon TS 50136-9 / IEC 60839-7-8	37
9.3	Exigences fonctionnelles selon ANSI/SIA DC-09 : 2007 ou supérieure	42
10	Annexe « Classification de la valeur du risque prévention incendie en fonction de l'affectation des objets »	46

1 Domaine d'application

La présente Directive décrit le modèle de transmission des alarmes automatiques issues d'installations obligatoires de détection et d'extinction incendie à destination du Centre de Traitement des Alarmes (« CTA ») du canton de Vaud. En se basant sur les normes nationales, européennes et internationales en vigueur, elle définit les exigences relatives au fonctionnement, à la sécurité et à la fiabilité des systèmes de transmission d'alarme.

Elle s'applique au canton de Vaud et à son centre officiel de réception des alarmes incendie, le CTA. Elle spécifie tous les signaux émis de la centrale de détection située dans le bâtiment surveillé, transmis et finalement réceptionné au CTA.

Son application garantit non seulement la communication entre le bâtiment surveillé et le CTA, mais également une implémentation uniforme et une interopérabilité des équipements.

2 Références normatives

Cette directive se réfère aux documents suivants, indispensables à son application correcte :

Désignation	Réf.	Description
SNEN 50136-1 // IEC 60839-5-1	[1]	Systèmes d'alarmes – Systèmes et équipement de transmission d'alarme – Partie 1: Exigences générales pour les systèmes de transmission d'alarme
SNEN 50136-2 // IEC 60839-5-2	[2]	Systèmes d'alarme – Systèmes et équipements de transmission d'alarme – Partie 2: Exigences pour les transmetteurs des locaux surveillés
SNEN 50136-3 // IEC 60839-5-3	[3]	Systèmes d'alarme – Systèmes et équipements de transmission d'alarme – Partie 3: Exigences pour les transmetteurs du centre de réception (RCT)
SNEN 50518-1 : 2013* SNEN 50518-2 : 2013* SNEN 50518-3 : 2013*	[4]	Centre de contrôle et de réception d'alarme - Partie 1: Exigences pour l'emplacement et la construction Partie 2: Exigences techniques Partie 3 : Procédures et exigences de fonctionnement
TS 50136-7	[7]	Systèmes d'alarmes - Systèmes et équipements de transmission d'alarme - Partie 7 : Guide d'application
TS 50136-9 // IEC 60839-7-8 TS	[9]	Systèmes d'alarmes - Systèmes et équipements de transmission d'alarme - Partie 9 : Exigences pour le protocole commun de transmission d'alarme utilisant le protocole Internet
SNEN 54-21	[20]	Systèmes de détection et d'alarme incendie - Partie 21 : dispositif de transmission de l'alarme feu et du signal de dérangement
Directives SES, Edition 1.01.2015	[30]	Directives techniques de l'Association Suisse des Constructeurs de Systèmes de Sécurité pour les installations de détection incendie – Chapitre 2 (Alimentation électrique des ECS) et Chapitre 18 (Exigences envers les systèmes de transmission d'alarme et de dérangement (ATS)) en particulier
Norme ANSI/SIA DC-09:2007 ou supérieure, (ANSI/SIA DC-09 :2013 en l'état)	[40]	Security Industry Association – SIA Digital Communication Standard – Internet Protocol Event Reporting

Norme ANSI/SIA DC-03	[41]	Security Industry Association – SIA Digital Communication Standard – “SIA format” Protocol for Alarm System Communications
Norme ANSI/SIA DC-05	[42]	Security Industry Association – SIA Digital Communication Standard – “Contact ID” Protocol for Alarm System Communications
AEAI – Directives de protection incendie 2015	[50]	Assurance qualité en protection incendie, en particulier l’AEAI 12-15
LSDIS – janvier 2011	[60]	Loi sur le Service de défense contre l’incendie et de secours (<i>RSV 963.15</i>) et son règlement d’application (<i>RSV 963.15.1</i>)
LPIEN – janvier 2009	[61]	Loi sur la prévention des incendies et des dangers résultant des éléments naturels (LPIEN, 963.11) et son règlement d’application (RLPIEN, avril 2004, 963.11.1)

* Et leur évolution en un seul document (SNEN 50518 : 201x).

Les éventuelles restrictions aux normes et autres directives sont mentionnées explicitement dans ce document.

3 Définitions - abréviations

3.1 AE – Equipement d’annonce

Système utilisé par l’ARC pour traiter les alarmes.

3.2 ARC – Centre de réception des alarmes

Entité organisée ayant pour mission la réception et le traitement des alarmes.

3.3 AS – Système d’alarme

Equipements techniques permettant de détecter une alarme de différent type : incendie, effraction, techniques,..). L’AS est installé dans le bâtiment alors considéré comme « surveillé ».

Pour les alarmes feu, le système de détection ou d’extinction (aussi connu sous l’acronyme SDAI, ou appelé « centrale ») doit correspondre aux directives de protection incendie (AEAI et SES).

L’ECA ne met pas de système de détection ou d’extinction à disposition. Ils sont donc fournis exclusivement par des entreprises agréées qui les installent et en assurent la configuration.

3.4 ATS – Système de transmission d’alarme

Equipements d’envoi (SPT), de réception (RCT) et de transmission des alarmes issues de l’AS, ainsi que des signaux de surveillance des voies de transmission.

Un réseau de transmission dédié n’est pas nécessaire à la transmission des alarmes. En principe, l’ECA ne fournit pas de prestations de transmission. La pérennité des réseaux de transmission dépend exclusivement des opérateurs de télécommunication, ou de fournisseurs de prestations assimilés. En conséquence, le choix de ce prestataire est libre mais peut dépendre du transmetteur comme du protocole utilisé.

Suivant la catégorie d’ATS utilisé, la transmission d’alarme doit s’effectuer selon deux voies de transmission physiquement séparées (qui n'utilisent pas d'infrastructures communes à un moment

donné) ; côté SPT et RCT, cela signifie qu'il est nécessaire de recourir aux services de plusieurs opérateurs de télécommunication, dont les infrastructures réseau sont distinctes physiquement (obligatoire côté SPT et côté RCT).

3.5 ATSN - réseau de services de transmission d'alarme

Un ATSN est défini comme un groupe d'ATS de la même catégorie.

Note à l'article: un ATSN est constitué d'un ou plusieurs ATS de la même catégorie, fonctionnant sous la surveillance du même centre de gestion et de télésurveillance.

3.6 ATP - Voie de transmission d'alarme (« Alarm Transmission Path »)

Route suivie par un message d'alarme entre un AS individuel et son AE associé.

Note à l'article: l'ATP débute au niveau de l'interface entre l'AS et le SPT et finit au niveau de l'interface entre le RCT et l'AE. Dans le cadre des notifications et de la surveillance le sens inverse peut aussi être utilisé. Se référer à la Figure 2 (l'ATP est défini du point B au point E).

3.7 CTA – Centre de traitement des alarmes (incendie, hold-up, alarmes techniques)

Le CTA est le centre officiel de réception d'alarmes (ARC) destinées aux Services de Défense Incendie et Secours (SDIS) et à certains Services au sein de la Direction générale de l'environnement (DGE) et du Service de la sécurité civile et militaire (SSCM).

Il assure la réception d'alarmes en rapport direct avec la défense incendie, le secours, les événements naturels et l'atteinte aux personnes, aux biens et à l'environnement (cf. chapitre V du règlement de la LSDIS). Des alarmes techniques ne sont en principe traitées que si elles sont associées à la protection incendie (alarmes gaz, pré alarme,...). Les alarmes doivent donc y être transmises directement et exclusivement. Elles sont généralement suivies d'une intervention appropriée et initiée par le CTA.

3.8 Centre de réception des dérangements

Un centre de réception des dérangements est un ARC qui reçoit et traite les critères de dérangements relatifs au fonctionnement des AS, ATS et AE : perte de connexion, batterie faible, etc.

Sa classification doit correspondre aux spécifications de [4].

3.9 Centre de télésurveillance de l'ATS, centre de télésurveillance de transmission d'alarme

Centre de télésurveillance dans lequel s'effectue le contrôle de l'état et du fonctionnement d'un ou plusieurs systèmes de transmission d'alarme (ATS). Il peut gérer et contrôler les équipements d'alarmes.

Note 1: Un centre de télésurveillance peut être un centre distinct ou faire partie d'un centre de réception d'alarme.

3.10 MCT – Emetteurs-récepteurs de centre de télésurveillance

Equipement de transmission d'alarme (ATE) au sein du système de transmission d'alarme (ATS), qui fournit des informations de télésurveillance et de gestion de l'état de l'équipement et des réseaux de transmission d'alarmes (« données de monitoring » ou de contrôle).

Note 1 : l'émetteur-récepteur du centre de télésurveillance peut être situé dans le centre de réception d'alarme (ARC) ou dans un centre distinct. Si le MCT est situé dans l'ARC, alors les exigences opérationnelles de la série de normes EN 50518 (voir [4]) sont à appliquer. Dans le second cas, il est de bonne pratique d'appliquer les mêmes exigences opérationnelles que celles contenues au sein de la série de norme EN 50518.

Note 2 : l'abréviation « MCT » est dérivée du terme anglais développé correspondant « Monitoring Center Transceiver ».

Note 3 : les 3 types de centres peuvent correspondre à des entités indépendantes ou regroupées suivant les configurations (partiellement ou totalement regroupées).

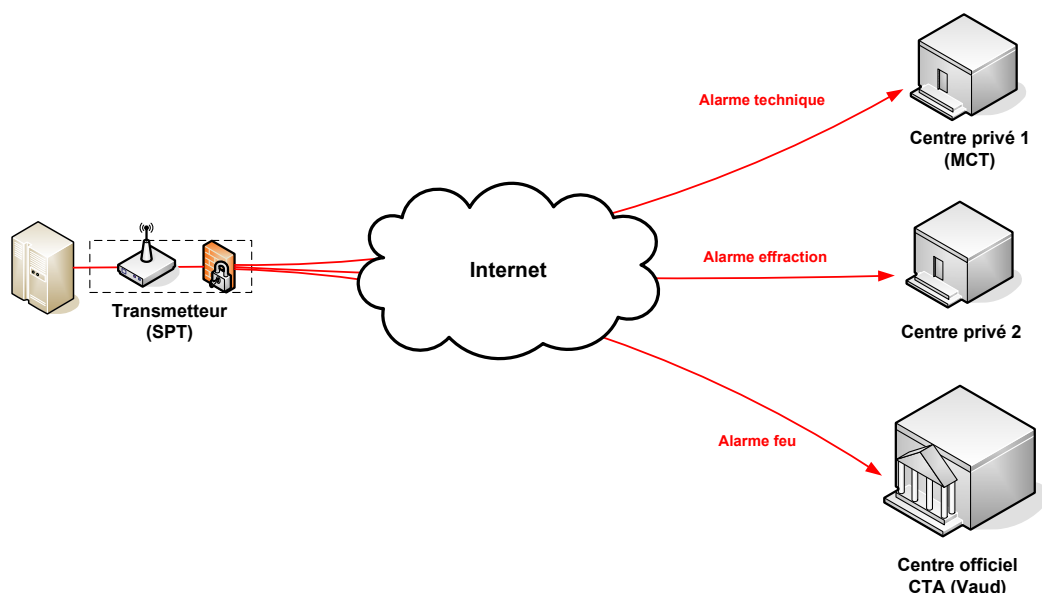


Figure 1 : Principe de la de transmission d'alarmes sécurisées dans le canton de Vaud.

3.11 Organisation d'alarmes & levée de doute

La « levée de doute » est l'opération consistant à vérifier la matérialité d'un événement ayant provoqué le déclenchement d'une alarme: feu, intrusion, etc. Elle permet de visualiser à distance l'objet protégé et/ou de constater sans équivoque le caractère illicite de l'événement déclencheur (contre-appel et dialogue téléphonique, interphonie; transmission d'images et de sons, etc.). L'ensemble des vérifications et la concordance des informations sont effectués par une organisation d'alarmes spécifique.

3.12 RCT – Transmetteur du centre de réception (récepteur)

Equipement raccordé à l'AE permettant de réceptionner les signaux émis des SPTs (transmetteurs).

L'ECA est responsable du fonctionnement permanent de ses RCTs.

3.13 SPT – Transmetteur du bâtiment surveillé (transmetteur)

Equipement raccordé à l'AS permettant la transmission des signaux et alarmes. Pour se raccorder au CTA, le SPT doit être agréé par l'ECA.

L'ECA ne met pas de SPT à disposition des exploitants mais accorde une subvention spéciale au sens de [61]. Les terminaux d'exploitants sont donc fournis exclusivement par des entreprises spécialisées qui les installent et en assurent la configuration ainsi que la maintenance.

3.14 UTC – temps universel coordonné (ou Universal Time Coordinated)

UTC est une échelle de temps adoptée comme base du temps civil international par la majorité des pays du globe. UTC est une échelle de temps comprise entre le « Temps atomique international » ou TAI qui est stable mais déconnecté de la rotation de la Terre et le Temps universel (TU), directement lié à la rotation de la Terre et donc lentement variable. Le terme «coordonné» indique que le **Temps Universel Coordonné** est en fait identique au temps atomique international dont il a la stabilité et l'exactitude à un nombre entier de secondes près, ce qui lui permet de **coller au temps universel à moins de 0,9 s près**.

4 Objet

L'objet de cette directive consiste à définir les exigences et spécifications permettant à des transmetteurs conformes installés dans des objets surveillés à établir des communications sécurisées avec les récepteurs du CTA. D'autre part, elle a pour objectif d'uniformiser cette liaison et le format des messages transmis.

Ce document définit une solution sécurisée ouverte (non propriétaire) basée sur des normes mondiales et nationales relatives aux systèmes et équipements de transmission d'alarmes.

4.1 Modèle de transmission

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

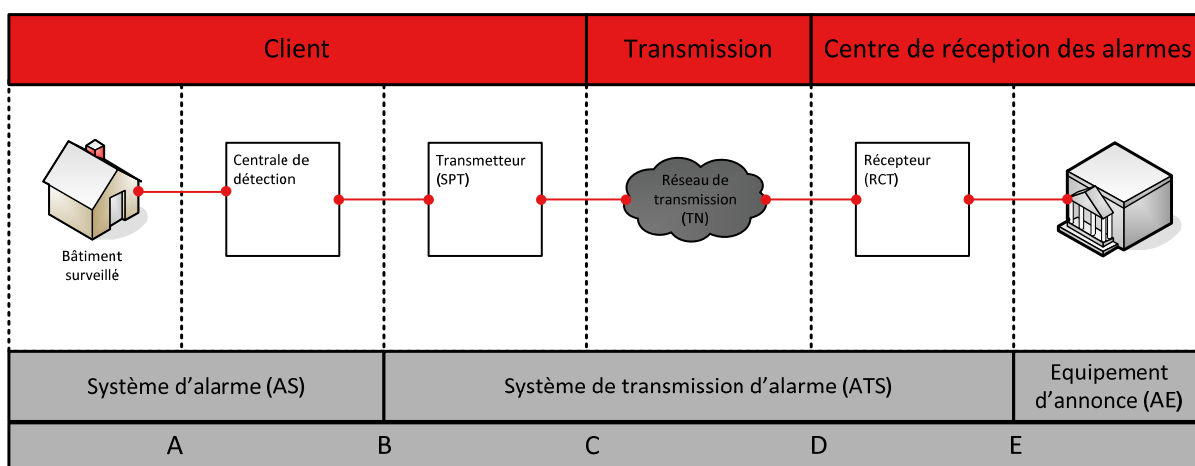


Figure 2 : Principe de la de transmission sécurisée – Se réfère à [1], figure 1.

La transmission sécurisée définie dans ce document commence au point B et se termine au point E. Une transmission sécurisée signifie qu'un message (dans le cas présent 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'au moins une voie de transmission dédiée, à l'intérieur de laquelle l'information est chiffrée et n'a subi aucune modification en cours de transmission.

4.2 Utilisateurs prévus

La présente directive s'adresse aux utilisateurs suivants :

- Prestataires de service de transmission d'alarme, y compris les opérateurs de réseaux ;
- Exploitants de centrales de réception d'alarmes ;
- Opérateurs de réseaux de télécommunication ;
- Fabricants d'équipements de transmetteur et/ou récepteur d'alarme ;
- Installateurs d'équipements de transmetteur et/ou récepteur d'alarme ;
- Propriétaires de bâtiments surveillés (à titre informatif uniquement).

Cette liste n'est pas exhaustive.

4.3 Structure du document

Cette directive est structurée de manière analogue aux normes citées ci-dessus, soit :

1. Le chapitre 1 présente le domaine d'application
2. Le chapitre 2 cite les références normatives en rapport
3. Le chapitre 3 liste les définitions et abréviations utilisées au sein de ce document
4. Le chapitre 4 présente l'objet de cette directive
5. Le chapitre 5 présente la méthodologie retenue pour la classification des bâtiments (affectation des objets) selon AEAI 2015.
6. Les chapitres 6 à 9 décrivent les exigences relatives à cet objet, soit :
 - a. Exigences fonctionnelles du système (chapitre 6)
 - b. Exigences relatives au transmetteur ou SPT (chapitre 7)
 - c. Exigences relatives au transmetteur du centre de réception d'alarmes ou RCT (chapitre 8)
 - d. Exigences relatives au protocole de transmission (chapitre 9).
7. Le chapitre 10 contient l'annexe décrivant, pour chaque affectation d'un objet, la valeur du « risque prévention incendie » associé. Ce chapitre s'appuie sur le chapitre 5 susmentionné.

Les exigences sont décrites sous forme de tableaux, avec la logique suivante :

N°	Réf norme	Description	Valid. produit
1	[1] 5.1	La configuration logique d'un ATS	<input type="checkbox"/>

Annotations :

- Numéro de l'exigence. (pointe vers la cellule N°)
- Référence à la liste des normes, directives et autres documents mentionnés au chapitre 2 de cette directive. (pointe vers la cellule Réf norme)
- Libellé de l'exigence. (pointe vers la cellule Description)
- Possibilité d'autocontrôle pour le lecteur, quant à la compatibilité de son produit par rapport à l'exigence formulée. (pointe vers la cellule Valid. produit)

Notes :

1. Les produits agréés par le CTA sont régulièrement annoncés sur le site web de l'ECA.
2. Les **installations volontaires** suivent les mêmes exigences que celles relatives aux **installations obligatoires** telles que décrites dans cette directive, en fonction de la classification du risque leurs correspondant.

5 Exigences relatives à la classification des bâtiments (affectation des objets) en fonction de la « Valeur de risque de prévention incendie »

5.1 Méthodologie retenue

D'une manière générale, les mesures relatives à la phase d'exploitation des bâtiments sont fixées dans la directive AEAI 12-15. Plus spécifiquement, des **chargés de sécurité en protection incendie** doivent être désignés et formés lorsque la nature et la gravité du danger d'incendie, le nombre d'occupants, le caractère ou l'importance de l'exploitation l'exigent. La nécessité d'un chargé de sécurité incendie dans un bâtiment est donc directement **liée au risque incendie de ce bâtiment en phase d'exploitation**. En conséquence, l'ECA, en tant qu'autorité de protection incendie selon la LSDIS et la LPIEN, a décidé que le critère "nécessité d'un chargé de sécurité en protection incendie" constitue la base principale de l'évaluation de la "valeur de risque Prévention", la classification secondaire tenant compte de l'importance donnée à la protection des personnes et/ou la valeur particulière du bâtiment, en lien avec le patrimoine cantonal.

Par conséquent, pour le canton de Vaud, l'ECA fixe le risque d'un bâtiment de 1 à 4 selon la nécessité d'avoir un chargé de sécurité incendie dans ledit bâtiment (selon AEAI 12-15, [50]) et l'importance donnée à la protection des personnes et/ou la valeur particulière du bâtiment. Le détail de cette classification se trouve dans le tableau annexé (chapitre 10 de cette directive).

5.2 Tableau associant la « Valeur de risque prévention incendie » et les configurations d'ATS exigées

N°	Réf norme	Description																				
1	[1] 5.2.1, Tableau 1	<p>Le tableau ci-dessous résume les exigences de l'ECA pour le canton de Vaud :</p> <table border="1"> <thead> <tr> <th></th> <th>DP2</th> <th>DP4</th> <th>Organisation d'alarmes</th> </tr> </thead> <tbody> <tr> <td>Valeur de risque Prévention 1</td> <td>obligatoire</td> <td>-</td> <td>obligatoire</td> </tr> <tr> <td>Valeur de risque Prévention 2</td> <td>obligatoire</td> <td>-</td> <td>obligatoire</td> </tr> <tr> <td>Valeur de risque Prévention 3</td> <td>-</td> <td>obligatoire</td> <td>obligatoire</td> </tr> <tr> <td>Valeur de risque Prévention 4</td> <td></td> <td>obligatoire</td> <td>obligatoire</td> </tr> </tbody> </table> <p>Tableau 1 : Valeur de risque prévention incendie par affectation et configurations d'ATS exigées.</p> <p>Notes :</p> <ol style="list-style-type: none"> 1) Pour les affectations dont les Valeurs de risque prévention Incendie sont égales à 1 ou 2, la catégorie DP2 est obligatoire (exigence minimum). Dans les deux cas de figure, le Client informe l'ECA par écrit de son installation (mode auto déclaratif). 2) Pour les affectations dont les Valeurs de risque prévention incendie sont égales à 3 ou 4, la catégorie DP4 est obligatoire et les règles suivantes s'appliquent : <ol style="list-style-type: none"> a. Avec une Valeur égale à 3, le mode « obligatoire » est auto déclaratif, le Client devant informer l'ECA par écrit de son installation. b. Avec la même valeur égale à 4, le Client doit soumettre son installation pour validation à l'ECA et apporter la preuve de sa bonne mise en place. 		DP2	DP4	Organisation d'alarmes	Valeur de risque Prévention 1	obligatoire	-	obligatoire	Valeur de risque Prévention 2	obligatoire	-	obligatoire	Valeur de risque Prévention 3	-	obligatoire	obligatoire	Valeur de risque Prévention 4		obligatoire	obligatoire
	DP2	DP4	Organisation d'alarmes																			
Valeur de risque Prévention 1	obligatoire	-	obligatoire																			
Valeur de risque Prévention 2	obligatoire	-	obligatoire																			
Valeur de risque Prévention 3	-	obligatoire	obligatoire																			
Valeur de risque Prévention 4		obligatoire	obligatoire																			

6 Exigences relatives au système

6.1 Exigences générales

La configuration logique d'un ATS doit être celle indiquée à la Figure 3 de cette directive. La fonction d'un ATS est de fournir un support fiable et sûr depuis l'interface B jusqu'à l'interface E pour la transmission des alarmes.

N°	Réf norme	Description	Valid. produit																		
2	[1] 5.1	<p>La configuration logique d'un ATS doit être celle indiquée à la Figure 3. La fonction d'un ATS est de fournir un support fiable et sûr depuis l'interface B jusqu'à l'interface E pour la transmission des alarmes.</p> <p>Figure 3 : Principe de la de transmission sécurisée pour le canton de Vaud</p>	<input type="checkbox"/>																		
3	[1] 5.2	<p>Pour le canton de Vaud, deux catégories d'ATS sont appliquées par l'ECA, soit DP2 et DP4, selon le degré de performance requis (voir N°10, §6.3).</p> <p>Les catégories DP2 et DP4 nécessitent chacune deux voies de transmission d'alarme (ATP) physiquement séparées.</p> <p>Pour les catégories DP2 et DP4, le binôme recommandé est Internet comme voie primaire, le réseau mobile GSM (GPRS ou plus rapide) ou UMTS (HSDPA ou plus rapide) comme voie secondaire, voir Figure 3.</p> <p>D'autres binômes, combinaison des technologies retenues ci-dessus, sont admis, tant que la condition des voies de transmission physiquement séparées est respectée et que les exigences de disponibilités des catégories concernées sont tenues (voir N°18, §6.7).</p> <p>Aucune catégorie personnalisée C n'est acceptée par l'ECA.</p> <table border="1"> <thead> <tr> <th>Configuration d'ATS appliquées par l'ECA</th> <th>DP2</th> <th>DP4</th> </tr> </thead> <tbody> <tr> <td>Interface réseau primaire de SPT</td> <td style="text-align: center;">O</td> <td style="text-align: center;">O</td> </tr> <tr> <td>Interface réseau secondaire de SPT</td> <td style="text-align: center;">O</td> <td style="text-align: center;">O</td> </tr> <tr> <td>RCT secondaire</td> <td style="text-align: center;">O</td> <td style="text-align: center;">O</td> </tr> <tr> <td>Interface réseau primaire de RCT</td> <td style="text-align: center;">O</td> <td style="text-align: center;">O</td> </tr> <tr> <td>Interface réseau secondaire de RCT</td> <td style="text-align: center;">O</td> <td style="text-align: center;">O</td> </tr> </tbody> </table> <p>« O » signifie Obligatoire, « F » signifie Facultatif</p> <p>Tableau 2 : configurations d'ATS appliquées par le canton de Vaud.</p>	Configuration d'ATS appliquées par l'ECA	DP2	DP4	Interface réseau primaire de SPT	O	O	Interface réseau secondaire de SPT	O	O	RCT secondaire	O	O	Interface réseau primaire de RCT	O	O	Interface réseau secondaire de RCT	O	O	<input type="checkbox"/>
Configuration d'ATS appliquées par l'ECA	DP2	DP4																			
Interface réseau primaire de SPT	O	O																			
Interface réseau secondaire de SPT	O	O																			
RCT secondaire	O	O																			
Interface réseau primaire de RCT	O	O																			
Interface réseau secondaire de RCT	O	O																			
4	[1] 5.3	<p>La transmission doit s'effectuer sur les réseaux locaux téléphoniques et/ou de données et/ou de distribution électrique et/ou de télévision par câble et/ou radio publiques câblés (TN1) et non câblés (TN2).</p>																			

6.2 Exigences système

N°	Réf norme	Description	Valid. produit												
5	[1] 6.1	L'ATS doit assurer la communication entre un ou plusieurs AS de l'objet surveillé et un ou plusieurs RCTs d'un ou plusieurs AE. En effet, l'objet surveillé peut avoir plusieurs systèmes de sécurité (détection incendie, détection effraction, surveillance d'installations techniques,...) qui peuvent utiliser le même SPT. De plus, le SPT peut envoyer des signaux à un ou plusieurs AE. Ce dernier peut avoir plusieurs RCTs. Pour le canton de Vaud, le centre officiel de réception des alarmes feu est le CTA.	<input type="checkbox"/>												
6	[1] 6.2	Les liaisons de transmission peuvent être partagées par d'autres équipements, applications et/ou services, pour autant que la transmission d'alarme ne soit pas perturbée et que les exigences de ce document soient respectées. Le transmetteur peut être raccordé sur le réseau interne de l'entreprise, pour autant que ce dernier puisse se connecter au récepteur.	<input type="checkbox"/>												
7	[1] 6.2.4	<p>Pour le canton de Vaud, l'ECA publie une liste des entreprises agréées fournissant des services et produits de transmission pour le raccordement au CTA. L'ATS doit avoir une capacité suffisante pour éviter tout encombrement et permettre la transmission des signaux d'alarme tout en garantissant la conformité avec les exigences du Tableau 3 ci-après pour les catégories obligatoires DP2 et DP4.</p> <p>L'ECA assure que le nombre de systèmes d'alarmes (AS) pouvant être connectés au CTA permet de garantir la conformité avec ces mêmes exigences.</p> <p>Toute voie de communication prise séparément doit continuer à satisfaire aux exigences du Tableau 3 ci-dessous :</p> <table border="1" data-bbox="371 1261 1345 1424"> <thead> <tr> <th>Délais de transmission acceptés par l'ECA</th> <th>DP2</th> <th>DP4</th> </tr> </thead> <tbody> <tr> <td>Moyenne arithmétique de toutes les transmissions</td> <td>20s</td> <td>10s</td> </tr> <tr> <td>95 % pour toutes les transmissions</td> <td>30s</td> <td>15s</td> </tr> <tr> <td>Délai de transmission maximum acceptable</td> <td>60s</td> <td>30s</td> </tr> </tbody> </table> <p>Tableau 3 : délais de transmission acceptés par l'ECA.</p>	Délais de transmission acceptés par l'ECA	DP2	DP4	Moyenne arithmétique de toutes les transmissions	20s	10s	95 % pour toutes les transmissions	30s	15s	Délai de transmission maximum acceptable	60s	30s	<input type="checkbox"/>
Délais de transmission acceptés par l'ECA	DP2	DP4													
Moyenne arithmétique de toutes les transmissions	20s	10s													
95 % pour toutes les transmissions	30s	15s													
Délai de transmission maximum acceptable	60s	30s													
8	[1] 6.2.5	<p>Les RCTs des centres de réception doivent être protégés contre des accès intempestifs et/ou des attaques de refus de service (DDoS – Distributed Denial of Service) provenant du réseau de transmission. De même, les transmetteurs agréés doivent être protégés contre les accès intempestifs. De la sorte, toute donnée malveillante reçue par une interface de réseau de transmission n'a pas d'influence sur le fonctionnement de l'équipement de transmission de l'alarme (SPT, RCT) ou sur le fonctionnement d'une quelconque autre interface de réseau de transmission. Ceci s'applique même si le taux de données malveillantes atteint la capacité d'une seule interface, rendant l'interface elle-même inopérante.</p> <p>Lorsque la performance de l'ATS est affectée par une attaque de refus de service, un signal de dérangement doit être généré selon les exigences de surveillance et de temps de report de dérangement de la catégorie obligatoire applicable (DP2 ou DP4).</p>	<input type="checkbox"/>												

6.3 Performances

N°	Réf norme	Description	Valid. produit
9	[1] 6.3.2	La moyenne arithmétique du délai de transmission d'alarme et la valeur de 95 % des mesures de celui-ci, ne doivent pas excéder les valeurs stipulées dans le Tableau 3 pour la catégorie concernée (DP2 ou DP4). Tout délai de transmission excédant le délai maximum admissible selon ce tableau implique un dérangement du système de transmission.	<input type="checkbox"/>
10	[1] 6.3.3.3 [30] 18.4, 18.6	<p>Contrôle de bout en bout de l'ATS : afin de respecter les temps de report donnés dans la norme, la surveillance de l'ATS doit s'effectuer par « polling » (transmission de messages spécifiques depuis le SPT, pour contrôler que les voies de transmission avec les RCTs sont bien présentes).</p> <p>Pour le canton de Vaud, les catégories d'ATS DP2 et DP4 sont applicables (se référer au §5.2).</p> <p>La catégorie DP4 implique des pollings <u>minimaux</u> relatifs à la surveillance de la connectivité toutes les 90 secondes pour la voie primaire et toutes les 5 heures pour la voie secondaire (lorsque la voie primaire est fonctionnelle).</p> <p>La catégorie DP2 implique des pollings <u>minimaux</u> de surveillance de la connectivité toutes les 30 minutes pour la voie primaire et toutes les 25 heures pour la voie secondaire (lorsque la voie primaire est fonctionnelle).</p> <p>En cas de rupture de la voie primaire, le contrôle par la voie secondaire doit se faire selon la périodicité de la voie primaire.</p> <p>Un transmetteur <u>qui ne reçoit plus de quittance</u> depuis l'une de ses cibles le signale par une alarme locale. Ce statut est défini comme suit :</p> <ul style="list-style-type: none"> • Catégorie DP2 : plus de 3 pollings consécutifs perdus • Catégorie DP4 : plus de 13 pollings consécutifs perdus <p>Se référer au tableau 1 au sein de la spécification technique [7] pour les détails relatifs à la détermination des valeurs susmentionnées.</p> <p><u>Note</u> : l'autorité compétente se réserve le droit d'exiger une fréquence de polling plus rapide en cas d'utilisation de commandes à distances – avec des SPTs « bidirectionnels* » – ou lors d'autres applications particulières le nécessitant (en termes de sécurité) ».</p> <p>* Signifie ici « pouvant recevoir et traiter des commandes ».</p>	<input type="checkbox"/>
11	[1] 6.3.3.4 [30] 18.6	<p>Connexions du transmetteur du centre de réception d'alarme (RCT) à l'équipement d'annonce (AE): le RCT surveille en permanence la connexion à l'AE (polling également). En cas de défaillance de la liaison, un signal de dérangement est enregistré et présenté à l'AE et aux RCTs correspondants ou au centre de télésurveillance MCT. Le temps de report du signal de dérangement satisfait aux exigences du temps de report des catégories DP2 ou DP 4 associées (voir Tableau 5 à l'exigence 37).</p>	<input type="checkbox"/>

6.4 Sécurisation des messages

N°	Réf norme	Description	Validation produit
12	[1] 6.4	Aucun événement ne doit occasionner une perte de message, en particulier une défaillance d'alimentation, une erreur ou réinitialisation logicielle ou matérielle ou toute autre panne.	<input type="checkbox"/>

6.5 Acquittement de la transmission

N°	Réf norme	Description	Validation produit
13	[1] 6.5	Chaque information envoyée par le SPT doit être acquittée (positivement ou négativement) par les RCTs du moment qu'elle est délivrée à l'AE.	<input type="checkbox"/>

6.6 Alarmes générées par l'ATS

N°	Réf norme	Description	Validation produit
14	[1] 6.6 [30] 18.6	Toutes les alarmes et défaillances (de voie) générées par l'ATS doivent être reportées à l'AE et/ou à l'AS (voir tableaux 13 et 4 – respectivement – de cette directive).	<input type="checkbox"/>

6.7 Disponibilité

N°	Réf norme	Description	Validation produit
15	[1] 6.7.1	La disponibilité du système (SPT + réseau + RCT) de transmission est enregistrée au niveau du CTA et peut être fournie à tout moment si nécessaire.	<input type="checkbox"/>
16	[1] 6.7.2	Redondance/Duplication : pour le canton de Vaud, l'ATS doit être complètement redondant. En cas de panne, le système doit automatiquement utiliser l'interface alternative, la voie secondaire, etc.	<input type="checkbox"/>
17	[1] 6.7.3	L'ATS est considéré comme indisponible dans les situations suivantes : <ul style="list-style-type: none"> - Lors de dérangements de l'ATS empêchant la transmission d'une alarme. - Lors de maintenance si aucun autre dispositif n'est fourni. 	<input type="checkbox"/>
18	[1] 6.7.5	La disponibilité de l'ATS ne doit pas être inférieure à 99.8% pour la catégorie DP4 , ou à 99.0% au minimum pour la catégorie DP2 (valeur recommandée : 99.8%). Cette disponibilité de l'ATS est calculée par le CTA, bout-en-bout soit du SPT au RCT, sur chaque période de sept jours. La durée de la disponibilité est mise à disposition de l'exploitant raccordé, à sa demande.	<input type="checkbox"/>
19	[1] 6.7.6	La disponibilité annuelle de l'ATSN ne doit pas être inférieure à 99.9% pour la catégorie DP4 , ou à 99.5% pour la catégorie DP2 , pour tous les ATS de la même catégorie.	<input type="checkbox"/>

6.8 Sécurité

N°	Réf norme	Description	Validation produit
20	[1] 6.8.1	Toutes les données de l'ATS (fonctions et gestion) doivent être chiffrées et hachées avec des clés de minimum 128 bits. De plus, au minimum une fois par semaine, des changements automatiques réguliers de clés aléatoires doivent être implémentés <u>pour les nouvelles installations uniquement</u> , avec le protocole de communication TS 50136-9 (selon chapitre 9.2). Cette exigence s'applique aux catégories DP2 et DP4.	<input type="checkbox"/>
21	[1] 6.8.1	Toutes les méthodes de chiffrement et de hachage doivent être documentées, faire partie du domaine public, testées et validées.	<input type="checkbox"/>
22	[1] 6.8.2	Sécurité de substitution : pour la catégorie DP4, la protection contre une substitution non autorisée du SPT par un équipement identique ou de simulation sur l'ATS doit être assurée. Pour la catégorie DP2, aucune protection particulière n'est exigée. Chaque SPT et RCT doit avoir un code unique, via un nombre suffisant de clés.	<input type="checkbox"/>
23	[1] 6.8.3	Sécurité des informations : pour la catégorie DP4, la protection des informations transmises par l'ATS doit être assurée par des mesures pour empêcher la lecture non autorisée et pour détecter la modification non autorisée des informations transmises. Pour la catégorie DP2, aucune protection particulière n'est exigée.	<input type="checkbox"/>

6.9 Vérification de performance

N°	Réf norme	Description	Validation produit
24	[1] 7.2	La vérification des performances d'un système de transmission d'alarme nécessite : <ul style="list-style-type: none"> a) une vérification destinée à déterminer que le fonctionnement de base du système est conforme aux exigences de la présente Directive et à toutes les normes qui y sont associées; ceci doit inclure l'essai destiné à établir que les alarmes sont transmises et que l'ATS est surveillé. b) une vérification supplémentaire périodique telle qu'exigée pour établir ou confirmer la disponibilité de l'ATS. 	<input type="checkbox"/>
25	[1] 7.3	Pour vérifier la performance d'un ATSN, tous les ATS de la catégorie DP4, respectivement DP2, doivent être pris en compte. Cela s'applique sans restriction dans le canton de Vaud.	<input type="checkbox"/>
26	[1] 7.4	Délai de transmission : la transmission correcte des alarmes doit être vérifiée, notamment la transmission des alarmes associées à la surveillance de l'ATS. Le délai nécessaire à la transmission d'une alarme doit être conforme aux exigences du Tableau 3 selon §6.2 (N°7).	<input type="checkbox"/>

N°	Réf norme	Description	Validation produit
27	[1] 7.5	<p>Intervalle de vérification : la vérification de performance d'un ATS décrite dans les Tableaux 3 et 5 doit être effectuée en continu.</p> <p>Les résultats de la vérification sur chaque ATS et ATSN doivent être analysés en continu sur des périodes successives de trois mois, aussi bien pour les catégories DP2 que DP4.</p>	<input type="checkbox"/>
28	[1] 7.6.1	<p>Disponibilité : l'enregistrement de tous les dérangements et de toutes les vérifications de performance effectuées sur tous les ATS et ATSN est conservé et enregistré par le CTA. Ces enregistrements incluent :</p> <ul style="list-style-type: none"> a) l'heure et la date auxquelles le dérangement a été identifié b) l'heure et la date auxquelles la solution a été mise en oeuvre et le système ramené à un fonctionnement normal. <p>Les enregistrements sont conservés pendant au moins trois ans au sein du CTA.</p> <p>Des enregistrements de disponibilité de l'ATS et de l'ATSN sont fournis par le CTA à l'exploitant sur demande.</p>	<input type="checkbox"/>
29	[1] 7.6.2	<p>Vérification des enregistrements : les enregistrements sont accessibles auprès du CTA à toute vérification par le représentant d'un organisme de certification accrédité ou le représentant d'une autre organisation indépendante.</p>	
30	[1] 7.6.3	<p>Calculs de disponibilité de l'ATSN : la somme des temps de dérangement est, pour tous les dérangements et pour chaque catégorie, calculée par période d'une année. Le nombre d'ATS déployés apparaît à minuit le dernier jour de la période d'une année. La disponibilité annuelle du système est la moyenne arithmétique des disponibilités hebdomadaires pendant 52 semaines successives.</p> <p>Les résultats et les calculs sont conservés pendant au moins 3 ans au CTA.</p>	

6.10 Documentation

N°	Réf norme	Description	Validation produit
31	[1] 8	<p>Le CTA maintient une documentation suffisante pour la planification, l'installation, la mise en service, l'entretien et le fonctionnement de l'ATS. La présentation des instructions de l'ATE doit refléter les niveaux d'accès des différents types d'utilisateurs. La documentation inclut les propriétés relatives aux catégories d'ATS DP2 et DP4 selon les Tableaux 1 à 9 et le §6.8 de [1].</p>	<input type="checkbox"/>

7 Exigences relatives au transmetteur (SPT)

Ce chapitre spécifie les exigences matérielles générales relatives au fonctionnement, à la fiabilité, à la résilience, à la sécurité et à la sûreté des transmetteurs de locaux surveillés (SPT) installés dans des locaux surveillés et utilisés dans les systèmes de transmission d'alarme (ATS) du canton de Vaud. Un transmetteur de locaux surveillés peut être un dispositif autonome ou constituer une partie intégrée à un système d'alarme.

Les exigences spécifiques aux applications et relatives au raccordement du SPT à des systèmes d'alarme relatifs à l'incendie sont données dans la série EN 54, en particulier [20].

7.1 Exigences générales

N°	Réf norme	Description	Validation produit
32	[2] 5.1	Le SPT doit être capable de recevoir des alarmes d'un ou plusieurs AS et de transmettre les alarmes à un ou plusieurs RCTs par l'intermédiaire d'au moins deux ATP distincts, en conformité avec les exigences des catégories d'ATS DP2 et DP4.	<input type="checkbox"/>
33	[2] 5.2	<p>Niveaux d'accès : pour le canton de Vaud, quatre niveaux d'accès permettant de catégoriser la capacité des utilisateurs à accéder aux fonctions du SPT, sont définis :</p> <ul style="list-style-type: none">• <i>Niveau 1</i> : accès aux fonctions, indications et notifications disponibles à tout individu sans authentification;• <i>Niveau 2</i> : accès aux informations concernant l'état opérationnel du SPT. Le niveau d'accès 2 peut également autoriser l'accès aux essais fonctionnels de base et à la gestion des autres utilisateurs de niveau d'accès 2;• <i>Niveau 3</i> : fonctions de maintenance et de mise en service, accès dans le but de modifier la configuration du SPT, par exemple modifications du logiciel, ajout, suppression ou remplacement de composants ou autres opérations qui peuvent, directement ou indirectement, avoir un effet nuisible sur les fonctions du SPT ;• <i>Niveau 4</i> : l'accès pour mettre à jour le logiciel et les fonctions en lecture seule. <p>L'accès aux fonctions de niveau 2, 3 et 4 fait l'objet d'une autorisation du fournisseur au moyen d'une clé ou d'un code sécurisé de même niveau de sécurité.</p> <p>L'accès au niveau 3 est autorisé par un utilisateur disposant d'un accès de niveau 2. De même, un accès au niveau 4 est autorisé par un utilisateur disposant d'un accès de niveau 3. Il s'agit d'une autorisation valable une fois faisant partie d'un contrat de niveau de service (chaque changement donne lieu à une autorisation unique).</p> <p>Les accès aux niveaux 2, 3 et 4 sont obtenus à distance en fournissant une autorisation, équivalente à une clé de 1'000'000 combinaisons.</p> <p>Si le fournisseur fournit des clés par défaut, la mise en service du SPT n'est pas possible sans préalablement changer ces clés, par exemple pendant l'installation. Il ne doit pas être possible de lire une clé quelconque fournissant une autorisation d'accès aux niveaux 2, 3 ou 4.</p>	<input type="checkbox"/>

			DP2	DP4	
		ATP primaire Temps de report de dérangement	30 min.	90 s.	
		ATP Secondaire Période maximale lorsque l'ATP primaire est fonctionnelle	25 h.	5 h.	
		Autre ATP Période maximale lorsque l'ATP primaire est défaillante	30 min.	90 s.	<input type="checkbox"/>
		Temps de report de dérangement de l'ATS	60 min.	3 min.	
<p>Tableau 5 : temps de report de dérangement maximum.</p> <p>La documentation du fournisseur (fabricant) doit clairement préciser le processus de signalisation des dérangements de l'ATS à l'AS.</p>					
38	[2] 5.7	<p>Interface avec l'AS :</p> <ol style="list-style-type: none"> 1. Les connexions à l'AS doivent être surveillées conformément à [1]. Se référer dans ce but à l'exigence n°10. 2. La durée maximale de détection d'une défaillance de l'interface et de la génération de l'alarme correspondante doit satisfaire aux exigences de l'application associée et ne doit pas dépasser le temps de report tel que défini dans le Tableau 7 ci-dessus pour la catégorie d'ATS appropriée. 3. Au minimum, le SPT dispose d'une interface sérielle ou parallèle (selon l'annexe de [2]) pour le raccordement avec l'AS. 4. En complément au point 3 ci-dessus, le SPT peut disposer d'interfaces avec l'AS plus évoluées et plus performantes, permettant, par exemple d'améliorer la granularité, la précision ou la redondance de l'information transmise. 5. Dans ce sens, le fournisseur documente les spécifications de <u>toutes</u> les interfaces du SPT avec l'AS. 			<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
39	[2] 5.8	<p>Surveillance de la ou des interface(s) de réseau de transmission – signalisation des dérangements :</p> <ol style="list-style-type: none"> 1. La documentation du fabricant/fournisseur doit décrire le processus de surveillance et de signalisation des dérangements de l'interface réseau vers l'AS. 2. Les exigences selon tableau 4 ci-dessus sont satisfaites pour la catégorie DP2, respectivement la catégorie DP4, selon les temps de report du tableau 5 (ci-dessus également). 3. Pour les catégories DP2 et DP4, tout dérangement sur l'une des interfaces de réseau de transmission doit être signalé au RCT par l'ATP restant dans les temps spécifiés dans le tableau 4 ci-dessus. 			<input type="checkbox"/> <input type="checkbox"/>
40	[30] 18.3, 9.2 [2] 5.9	<p>Alimentation du SPT : Le transmetteur des locaux surveillés (SPT) doit être alimenté par l'alimentation électrique du système de détection et d'alarme incendie (SDAI) ou par une alimentation électrique séparée. L'alimentation électrique doit avoir au moins la même durée que l'alimentation de secours de l'AS, soit selon [30].</p> <p>Pour les catégories DP2 et DP4, si la voie primaire et la voie secondaire sont exploitées via des réseaux informatiques redondants, les parties</p>			<input type="checkbox"/> <input type="checkbox"/>

N°	Réf norme	Description	Validation produit																											
43	[2] 6.1.3	<p>Exigences pour le fonctionnement en forçage de la transmission: Lorsqu'une alarme est reçue en provenance de l'AS, le SPT doit transmettre cette alarme au RCT.</p> <p>Le SPT ne doit pas acquitter l'alarme à destination de l'AS avant d'avoir reçu un acquittement de la part du RCT. Lorsque le SPT reçoit un acquittement de la part du RCT, cet acquittement doit être transmis à l'AS.</p>	<input type="checkbox"/> <input type="checkbox"/>																											
44	[2] 6.2	<p>Alarmes du SPT : le SPT doit être capable de générer et de transmettre aux RCTs les alarmes spécifiées au Tableau 8 ci-après :</p> <table border="1"> <thead> <tr> <th rowspan="2">#</th> <th colspan="3">Alarmes produites par le SPT et transmises au RCT</th> </tr> <tr> <th>Alarmes</th> <th>DP2</th> <th>DP4</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Défaillance et rétablissement de la source d'alimentation principale du SPT</td> <td style="text-align: center;">○</td> <td style="text-align: center;">○</td> </tr> <tr> <td>2</td> <td>Défaillance et rétablissement de la source d'alimentation alternative du SPT</td> <td style="text-align: center;">○</td> <td style="text-align: center;">○</td> </tr> <tr> <td>3</td> <td>Défaillance et rétablissement de l'interconnexion de l'AS au SPT</td> <td style="text-align: center;">○</td> <td style="text-align: center;">○</td> </tr> <tr> <td>4</td> <td>Défaillance et rétablissement de l'ATP principal</td> <td style="text-align: center;">○</td> <td style="text-align: center;">○</td> </tr> <tr> <td>5</td> <td>Défaillance et rétablissement de l'ATP secondaire</td> <td style="text-align: center;">○</td> <td style="text-align: center;">○</td> </tr> </tbody> </table> <p>« ○ » signifie obligatoire.</p> <p>Tableau 8 : Alarmes produites par le SPT et transmises au RCT.</p> <p>NOTES :</p> <ol style="list-style-type: none"> Les exigences concernant la transmission des défaillances et des rétablissements de la source d'alimentation principale et/ou alternative du SPT ne s'appliquent qu'aux SPT dotés d'une alimentation électrique dédiée. Si le SPT génère des alarmes autres que celles définies dans le Tableau 6, ces alarmes doivent être décrites dans la documentation du fournisseur. 	#	Alarmes produites par le SPT et transmises au RCT			Alarmes	DP2	DP4	1	Défaillance et rétablissement de la source d'alimentation principale du SPT	○	○	2	Défaillance et rétablissement de la source d'alimentation alternative du SPT	○	○	3	Défaillance et rétablissement de l'interconnexion de l'AS au SPT	○	○	4	Défaillance et rétablissement de l'ATP principal	○	○	5	Défaillance et rétablissement de l'ATP secondaire	○	○	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
#	Alarmes produites par le SPT et transmises au RCT																													
	Alarmes	DP2	DP4																											
1	Défaillance et rétablissement de la source d'alimentation principale du SPT	○	○																											
2	Défaillance et rétablissement de la source d'alimentation alternative du SPT	○	○																											
3	Défaillance et rétablissement de l'interconnexion de l'AS au SPT	○	○																											
4	Défaillance et rétablissement de l'ATP principal	○	○																											
5	Défaillance et rétablissement de l'ATP secondaire	○	○																											
45	[2] 6.3, [1] 6.8.2	<p>Sécurité de substitution : pour la catégorie DP4 uniquement, le fabricant doit fournir une déclaration descriptive de la méthodologie qu'il utilise pour assurer la conformité à l'exigence N°22.</p> <table border="1"> <thead> <tr> <th>Exigence de sécurité de substitution des SPTs</th> <th>DP4</th> </tr> </thead> <tbody> <tr> <td>Protection de substitution</td> <td style="text-align: center;">○</td> </tr> </tbody> </table> <p>Tableau 9 : Exigence de sécurité de substitution des SPTs.</p>	Exigence de sécurité de substitution des SPTs	DP4	Protection de substitution	○	<input type="checkbox"/>																							
Exigence de sécurité de substitution des SPTs	DP4																													
Protection de substitution	○																													
46	[2] 6.4, [1] 6.8.3	<p>Sécurité de l'information : pour la catégorie DP4 uniquement, le fabricant doit fournir une déclaration descriptive de la méthodologie qu'il utilise pour assurer la conformité à l'exigence N°23.</p> <table border="1"> <thead> <tr> <th>Exigence de sécurité des informations</th> <th>DP4</th> </tr> </thead> <tbody> <tr> <td>Sécurité des informations</td> <td style="text-align: center;">○</td> </tr> </tbody> </table> <p>Tableau 10 : Exigence de sécurité des informations.</p>	Exigence de sécurité des informations	DP4	Sécurité des informations	○	<input type="checkbox"/>																							
Exigence de sécurité des informations	DP4																													
Sécurité des informations	○																													

7.5 Performances / Tests et essais effectués

N°	Réf norme	Description	Validation produit																																																									
50	[2] 9.1 à 9.4.16.4 inclus	<p>Pour le canton de Vaud, les SPTs relatifs aux catégories DP2 et DP4 doivent satisfaire à tous les tests du chapitre 9 de [2], selon les exigences et les procédures de tests y spécifiées. Le tableau ci-après synthétise la situation :</p> <table border="1" data-bbox="368 450 1345 495"> <tr> <td>Catégorie de SPT :</td> <td>DP2 <input type="checkbox"/></td> <td>DP4 <input type="checkbox"/></td> </tr> </table> <table border="1" data-bbox="368 524 1345 1512"> <thead> <tr> <th><i>Libellé de l'exigence</i></th> <th><i>N° de la directive</i></th> <th><i>Validation</i></th> </tr> </thead> <tbody> <tr> <td>Niveaux d'accès</td> <td>33</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Accès à distance</td> <td>34</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Téléchargement montant et descendant</td> <td>35</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Stockage des paramètres</td> <td>36</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Signalisation des dérangements de l'ATS et de l'ATP à l'AS</td> <td>37</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Interface avec l'AS</td> <td>38</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Surveillance interface(s) de réseau de transmission – signalisation des dérangements</td> <td>39</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Alimentation du SPT</td> <td>40</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Journal des événements</td> <td>41</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Mode de fonctionnement des acquittements – « pass-through » ou – « store-and-forward »</td> <td>42</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Exigences « pass-through » pour le fonctionnement « en forçage de la transmission » / Exigences « enregistrement et transmission »</td> <td>43</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Alarmes du SPT</td> <td>44</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Sécurité de substitution</td> <td>45</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Sécurité de l'information</td> <td>46</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Documentation du SPT</td> <td>47</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Marquage et identification</td> <td>48</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Boîtier et protection contre la fraude</td> <td>49</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> </tbody> </table> <p>Tableau 11 : Synthèse des tests relatifs aux exigences à satisfaire par le SPT.</p>	Catégorie de SPT :	DP2 <input type="checkbox"/>	DP4 <input type="checkbox"/>	<i>Libellé de l'exigence</i>	<i>N° de la directive</i>	<i>Validation</i>	Niveaux d'accès	33	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Accès à distance	34	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Téléchargement montant et descendant	35	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Stockage des paramètres	36	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Signalisation des dérangements de l'ATS et de l'ATP à l'AS	37	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Interface avec l'AS	38	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Surveillance interface(s) de réseau de transmission – signalisation des dérangements	39	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Alimentation du SPT	40	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Journal des événements	41	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Mode de fonctionnement des acquittements – « pass-through » ou – « store-and-forward »	42	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> OK <input type="checkbox"/> NOK	Exigences « pass-through » pour le fonctionnement « en forçage de la transmission » / Exigences « enregistrement et transmission »	43	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> OK <input type="checkbox"/> NOK	Alarmes du SPT	44	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Sécurité de substitution	45	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Sécurité de l'information	46	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Documentation du SPT	47	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Marquage et identification	48	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Boîtier et protection contre la fraude	49	<input type="checkbox"/> OK <input type="checkbox"/> NOK	<input type="checkbox"/>
Catégorie de SPT :	DP2 <input type="checkbox"/>	DP4 <input type="checkbox"/>																																																										
<i>Libellé de l'exigence</i>	<i>N° de la directive</i>	<i>Validation</i>																																																										
Niveaux d'accès	33	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Accès à distance	34	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Téléchargement montant et descendant	35	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Stockage des paramètres	36	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Signalisation des dérangements de l'ATS et de l'ATP à l'AS	37	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Interface avec l'AS	38	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Surveillance interface(s) de réseau de transmission – signalisation des dérangements	39	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Alimentation du SPT	40	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Journal des événements	41	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Mode de fonctionnement des acquittements – « pass-through » ou – « store-and-forward »	42	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Exigences « pass-through » pour le fonctionnement « en forçage de la transmission » / Exigences « enregistrement et transmission »	43	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Alarmes du SPT	44	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Sécurité de substitution	45	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Sécurité de l'information	46	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Documentation du SPT	47	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Marquage et identification	48	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										
Boîtier et protection contre la fraude	49	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																																										

8 Exigences relatives au récepteur (RCT)

Ce chapitre spécifie les exigences matérielles générales relatives au fonctionnement, à la fiabilité, à la résilience, à la sécurité et à la sûreté des transmetteurs du centre de réception (RCT) installés dans l'ARC et utilisés dans les systèmes de transmission d'alarme (ATS) du canton de Vaud. Ces exigences permettent de garantir la compatibilité avec les catégories d'ATS appliquées dans le canton de Vaud, soit DP2 et DP4.

Le RCT a pour fonction de surveiller les ATP, de recevoir les messages d'alarme, de transmettre les messages d'alarme vers un ou plusieurs AE et d'envoyer des accusés de réception aux SPT.

Le transmetteur du centre de réception (RCT) peut être soit un élément intégré d'équipement de réception/d'annonce, soit un dispositif autonome. Dans les deux cas, les exigences au sein de cette directive doivent être respectées.

8.1 Exigences générales

N°	Réf norme	Description	Validation produit
51	[3] 5.2	Classification des RCTs : La documentation du RCT doit décrire pour quelles catégories d'ATS le RCT est conforme aux exigences, en particulier, pour le canton de Vaud, sa conformité avec les exigences des catégories d'ATS DP2 et DP4.	<input type="checkbox"/>

8.2 Exigences fonctionnelles

N°	Réf norme	Description	Validation produit
52	[3] 6.1	Le RCT doit assurer la communication entre un ou plusieurs AE et un ou plusieurs SPT et surveiller l'(les) interface(s) avec un ou plusieurs AE. Le RCT doit surveiller les ATS.	<input type="checkbox"/> <input type="checkbox"/>
53	[3] 6.2	<p>Niveaux d'accès : pour le canton de Vaud, quatre niveaux d'accès permettant de catégoriser la capacité des utilisateurs à accéder aux fonctions des RCTs, sont définis :</p> <ul style="list-style-type: none"> • <i>Niveau 1</i> : accès aux indications ; • <i>Niveau 2</i> : accès à l'état opérationnel des RCTs et aux fonctions de mise en service ; • <i>Niveau 3</i> : fonctions de maintenance et accès dans le but de modifier la configuration des RCTs, notamment les données spécifiques au site et autres opérations qui peuvent, directement ou indirectement, avoir un effet nuisible sur les fonctions des RCTs ; • <i>Niveau 4</i> : accès aux mises à jour logicielles et paramètres en lecture seule. <p>Ces 4 niveaux d'accès s'appliquent uniquement à un accès logique (pas à un accès physique).</p> <p>L'accès à toutes les fonctions doit faire l'objet d'une autorisation au moyen d'une clé.</p> <p>Les niveaux d'accès 2, 3 et 4 doivent utiliser des comptes personnalisés pour obtenir une traçabilité.</p> <p>Un utilisateur de niveau 4 doit obtenir une autorisation par un utilisateur disposant d'un accès de niveau 3. Cette autorisation peut être permanente ou limitée dans le temps.</p> <p>L'accès à tous les niveaux doit faire l'objet d'une autorisation au moyen d'une clé. Le mécanisme de la clé doit pouvoir fournir au moins 1'000'000 clés différentes.</p> <p>S'il est possible de tenter d'avoir un accès plus de 3 fois au cours d'une période de 60 secondes, les RCTs doivent avoir la capacité de retarder des</p>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

		<p>tentatives répétées. Après la troisième tentative, un délai d'au moins 90 s doit être respecté entre chaque nouvelle tentative.</p> <p>Si le fournisseur transmet des clés par défaut, il ne doit pas être possible d'effectuer la mise en service des RCTs sans préalablement changer ces clés, par exemple pendant l'installation.</p> <p>L'accès à distance doit nécessiter une connexion sécurisée et satisfaire aux exigences de sécurité des données telles que spécifiées sous 6.8. Le tableau 12 ci-dessous résume les accès logiques autorisés selon les niveaux d'accès.</p> <table border="1" data-bbox="368 553 1337 1111"> <thead> <tr> <th>Niveau d'accès</th> <th>Niveau 1</th> <th>Niveau 2</th> <th>Niveau 3</th> <th>Niveau 4</th> </tr> </thead> <tbody> <tr> <td>Consulter les indications du RCT</td> <td>A</td> <td>A</td> <td>A</td> <td>A</td> </tr> <tr> <td>Modifier la configuration du RCT</td> <td>NA</td> <td>NA</td> <td>A</td> <td>NA</td> </tr> <tr> <td>Consulter la configuration du RCT</td> <td>NA</td> <td>A</td> <td>A</td> <td>A</td> </tr> <tr> <td>Mettre en/hors service le SPT</td> <td>NA</td> <td>A</td> <td>A</td> <td>NA</td> </tr> <tr> <td>Consulter le journal des événements / alarmes du RCT</td> <td>NA</td> <td>A</td> <td>A</td> <td>A</td> </tr> <tr> <td>Modifier le logiciel du RCT</td> <td>NA</td> <td>NA</td> <td>NA</td> <td>A</td> </tr> <tr> <td>Modifier les utilisateurs et/ou droits d'utilisateur</td> <td>NA</td> <td>NA</td> <td>A</td> <td>NA</td> </tr> <tr> <td>Modifier et/ou supprimer des entrées dans le journal des événements</td> <td>NA</td> <td>NA</td> <td>NA</td> <td>NA</td> </tr> </tbody> </table> <p>Où : « A = Autorisé », « NA = Non Autorisé ».</p> <p>Tableau 12 : Niveaux d'accès – Accès logique aux fonctions.</p> <p>Une fermeture de session automatique de sessions d'accès à distance doit être activée après une période d'inactivité. La période d'inactivité doit être configurable.</p>	Niveau d'accès	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Consulter les indications du RCT	A	A	A	A	Modifier la configuration du RCT	NA	NA	A	NA	Consulter la configuration du RCT	NA	A	A	A	Mettre en/hors service le SPT	NA	A	A	NA	Consulter le journal des événements / alarmes du RCT	NA	A	A	A	Modifier le logiciel du RCT	NA	NA	NA	A	Modifier les utilisateurs et/ou droits d'utilisateur	NA	NA	A	NA	Modifier et/ou supprimer des entrées dans le journal des événements	NA	NA	NA	NA	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Niveau d'accès	Niveau 1	Niveau 2	Niveau 3	Niveau 4																																												
Consulter les indications du RCT	A	A	A	A																																												
Modifier la configuration du RCT	NA	NA	A	NA																																												
Consulter la configuration du RCT	NA	A	A	A																																												
Mettre en/hors service le SPT	NA	A	A	NA																																												
Consulter le journal des événements / alarmes du RCT	NA	A	A	A																																												
Modifier le logiciel du RCT	NA	NA	NA	A																																												
Modifier les utilisateurs et/ou droits d'utilisateur	NA	NA	A	NA																																												
Modifier et/ou supprimer des entrées dans le journal des événements	NA	NA	NA	NA																																												
54	[3] 6.3	<p>Téléchargement de logiciel: le téléchargement d'un logiciel entrant ou sortant d'un RCT est uniquement autorisé au niveau d'accès approprié, tel que défini ci-dessus, à l'exigence n°53.</p>	<input type="checkbox"/>																																													
55	[3] 6.4	<p>Stockage des paramètres et données : une coupure d'alimentation (suivie de son rétablissement) ou un redémarrage du logiciel ne doit pas entraîner de perte de configuration, de journal et de messages d'alarme sécurisés. Le RCT doit revenir automatiquement à son fonctionnement normal dans tous les cas de figure.</p>	<input type="checkbox"/>																																													
56	[1] 6.6 [3] 6.5, [30] 18.6	<p>Surveillance et signalisation des dérangements de l'ATP et de l'ATS : les défaillances de l'ATS et/ou de l'ATP doivent être signalées par les RCTs à l'AE conformément au Tableau 13 ci-dessous.</p> <table border="1" data-bbox="368 1861 1337 2011"> <thead> <tr> <th>Alarme / Rapport d'alarme des RCTs à l'AE</th> <th>DP2</th> <th>DP4</th> </tr> </thead> <tbody> <tr> <td>Défaillance / Dérangement de l'ATP</td> <td>F</td> <td>F</td> </tr> <tr> <td>Défaillance / Dérangement de l'ATS</td> <td>O</td> <td>O</td> </tr> </tbody> </table> <p>« O » signifie Obligatoire, « F » signifie Facultatif.</p> <p>Tableau 13 : Rapport d'alarme des RCTs à l'AE.</p>	Alarme / Rapport d'alarme des RCTs à l'AE	DP2	DP4	Défaillance / Dérangement de l'ATP	F	F	Défaillance / Dérangement de l'ATS	O	O	<input type="checkbox"/>																																				
Alarme / Rapport d'alarme des RCTs à l'AE	DP2	DP4																																														
Défaillance / Dérangement de l'ATP	F	F																																														
Défaillance / Dérangement de l'ATS	O	O																																														

		<p><u>Note</u> : pour le canton de Vaud, il convient que la méthode de report d'alarme de toutes les voies ayant échoué vers l'AE soit un message de « défaillance de voie primaire d'ATS » et de « défaillance d'autre voie d'ATS » et/ou un message "toutes voies défaillantes". La méthode de report doit être documentée par le CTA.</p> <p>La documentation du fournisseur (fabricant) doit clairement préciser le signal de notification.</p>	<input type="checkbox"/>												
57	[3] 6.6 [1] 6.6	<p>Interface avec l'(les) AE :</p> <ol style="list-style-type: none"> L'(les) interface(s) avec l'(les) AE doi(ven)t être surveillée(s) conformément au Tableau 5. Le temps de report de la défaillance de connexion doit être inférieur ou égal au temps de report de l'ATS avec la catégorie la plus élevée ou 60 s, la plus courte des valeurs étant retenue, soit : <ul style="list-style-type: none"> Pour la catégorie DP2, le temps de report maximum est 60s. Pour la catégorie DP4, le temps de report maximum est 60s également. En cas de défaillance de l'interface, un signal de dérangement doit être généré et un évènement doit être consigné. Le fournisseur documente les spécifications de l'(des) interface(s) à l'AE et la manière dont le signal de dérangement est présenté et consigné 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
58	[3] 6.7	<p>Signalisation des dérangements :</p> <ol style="list-style-type: none"> Le RCT doit disposer d'un moyen pour signaler les dérangements lorsque l'un des dérangements suivants se produit : <ul style="list-style-type: none"> défaillance de l'interface de l'AE ; défaillance de l'interface du réseau de transmission ; défaillance du système du RCT. Le fournisseur doit spécifier, dans la documentation du RCT, comment ces dérangements sont signalés. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
59	[3] 6.8	<p>Enregistrement d'évènements :</p> <p>Pour qu'un RCT soit compatible avec les exigences du canton de Vaud, une fonction de journalisation doit être fournie pour permettre de constituer une piste d'audit et de résoudre les problèmes.</p> <ol style="list-style-type: none"> Les évènements spécifiés dans le Tableau 14 doivent être enregistrés pour les catégories DP2 et DP4 de RCT. <table border="1" data-bbox="368 1818 1337 2018"> <thead> <tr> <th colspan="3">Événements à enregistrer</th> </tr> <tr> <th>#</th> <th>Événement</th> <th>Identification des utilisateurs</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Message d'alarme depuis l'ATS</td> <td>N/A</td> </tr> <tr> <td>2</td> <td>Défaillance et rétablissement de l'(des) interface(s) de l'AE</td> <td>N/A</td> </tr> </tbody> </table>	Événements à enregistrer			#	Événement	Identification des utilisateurs	1	Message d'alarme depuis l'ATS	N/A	2	Défaillance et rétablissement de l'(des) interface(s) de l'AE	N/A	<input type="checkbox"/> <input type="checkbox"/>
Événements à enregistrer															
#	Événement	Identification des utilisateurs													
1	Message d'alarme depuis l'ATS	N/A													
2	Défaillance et rétablissement de l'(des) interface(s) de l'AE	N/A													

		<table border="1"> <tr> <td>3</td> <td>Défaillance et rétablissement de l'(des) interface(s) du réseau de transmission</td> <td>N/A</td> </tr> <tr> <td>4</td> <td>Modifications à la configuration du RCT</td> <td>O</td> </tr> <tr> <td>5</td> <td>Mise sous tension ou réinitialisation</td> <td>O</td> </tr> <tr> <td>6</td> <td>Toute modification du logiciel</td> <td>O</td> </tr> <tr> <td>7</td> <td>Modifications de la date et de l'heure</td> <td>O</td> </tr> <tr> <td>8</td> <td>Accès au RCT</td> <td>O</td> </tr> <tr> <td>9</td> <td>Modifications des utilisateurs et/ou droits d'utilisateur</td> <td>O</td> </tr> </table> <p>« O » signifie obligatoire, « N/A » signifie « Non Applicable ».</p> <p>Tableau 14 : classification de l'enregistrement des événements – événements à enregistrer.</p> <p>NOTE : l'enregistrement de l'identification des utilisateurs est seulement obligatoire si l'évènement est déclenché par une intervention des utilisateurs.</p> <p>2. Le journal des événements peut être stocké à l'extérieur du RCT. <input type="checkbox"/></p> <p>3. Les moyens d'enregistrement des événements doivent être non volatils. Les entrées de journal doivent être conservées pendant au moins 3 ans. Le fournisseur doit spécifier dans sa documentation la procédure à suivre. <input type="checkbox"/></p> <p>4. Les événements datant de plus de 3 ans peuvent être supprimés. <input type="checkbox"/></p> <p>5. Le journal doit enregistrer, outre l'évènement lui-même, la date et l'heure auxquelles l'évènement s'est produit. La résolution temporelle doit être d'au minimum 1 s et doit avoir une précision de ± 5 s selon le temps universel coordonné. <input type="checkbox"/></p> <p>6. Le RCT doit comporter un moyen de synchroniser la date et l'heure selon l'UTC (temps universel coordonné ou <i>UTC</i>). Le fournisseur doit spécifier dans sa documentation la procédure à suivre concernant la synchronisation de l'heure selon l'UTC. <input type="checkbox"/></p> <p>7. Le RCT peut utiliser les fuseaux horaires locaux. <input type="checkbox"/></p> <p>8. Pour optimiser le stockage des événements, si des événements répétitifs successifs identiques se produisent au cours d'une période de 12 heures, il n'est alors nécessaire d'enregistrer que le premier et le dernier événement. Dans ce cas, le nombre d'évènements identiques doit être enregistré. <input type="checkbox"/></p>	3	Défaillance et rétablissement de l'(des) interface(s) du réseau de transmission	N/A	4	Modifications à la configuration du RCT	O	5	Mise sous tension ou réinitialisation	O	6	Toute modification du logiciel	O	7	Modifications de la date et de l'heure	O	8	Accès au RCT	O	9	Modifications des utilisateurs et/ou droits d'utilisateur	O	
3	Défaillance et rétablissement de l'(des) interface(s) du réseau de transmission	N/A																						
4	Modifications à la configuration du RCT	O																						
5	Mise sous tension ou réinitialisation	O																						
6	Toute modification du logiciel	O																						
7	Modifications de la date et de l'heure	O																						
8	Accès au RCT	O																						
9	Modifications des utilisateurs et/ou droits d'utilisateur	O																						
60	[3] 6.9.1, 6.9.2	<p>Modes de fonctionnement (« pass-through » ou forçage de la transmission) : le mode de fonctionnement dit « pass-through » (ou « forçage de la transmission ») est recommandé pour les RCTs du canton de Vaud. Le mode « store-and-forward » (ou « enregistrement et transmission ») est, toutefois, toléré pour autant que toutes les exigences selon [3], 6.9.2, soient garanties, les preuves correspondantes, ainsi que les certifications mentionnées au N°42, devant être soumises à l'Autorité Compétente pour approbation.</p> <p>Le fournisseur doit confirmer dans la documentation du produit le mode de fonctionnement proposé.</p>	<input type="checkbox"/> <input type="checkbox"/>																					

61	[3]. 6.9.3	<p>Exigences pour le fonctionnement en forçage de la transmission : lorsqu'une alarme est reçue en provenance du SPT, les RCTs doivent transmettre cette alarme à l'(aux) AE.</p> <p>Les RCTs ne doivent pas acquitter l'alarme à destination du SPT avant d'avoir reçu un acquittement de la part d'au moins un AE. Lorsque les RCTs reçoivent un acquittement de la part d'un ou de plusieurs AE, cet acquittement doit être transmis au SPT.</p>	<input type="checkbox"/> <input type="checkbox"/>				
62	[3] 6.10	<p>Déni de service : le fournisseur des RCTs doit déclarer, dans sa documentation, la méthodologie qu'il utilise pour assurer la conformité à l'exigence n°8 de cette directive.</p>	<input type="checkbox"/>				
63	[3] 6.11, [1] 6.8.3	<p>Sécurité de l'information : pour la catégorie DP4 uniquement, le fournisseur doit fournir une déclaration descriptive de la méthodologie qu'il utilise pour assurer la conformité à l'exigence N°23, en particulier pour assurer la communication du SPT et l'accès à distance.</p> <table border="1"> <thead> <tr> <th>Exigence de sécurité des informations</th> <th>DP4</th> </tr> </thead> <tbody> <tr> <td>Sécurité des informations</td> <td>Obligatoire</td> </tr> </tbody> </table> <p>Tableau 15 : Exigence de sécurité des informations.</p> <p>Aucune exigence particulière n'est exigée pour la catégorie DP2.</p>	Exigence de sécurité des informations	DP4	Sécurité des informations	Obligatoire	<input type="checkbox"/>
Exigence de sécurité des informations	DP4						
Sécurité des informations	Obligatoire						
64	[3] 6.12, [1] 6.8.2	<p>Sécurité de substitution : pour la catégorie DP4 uniquement, le fournisseur doit fournir une déclaration descriptive de la méthodologie qu'il utilise pour assurer la conformité à l'exigence N°22.</p> <table border="1"> <thead> <tr> <th>Exigence de sécurité de substitution des SPTs</th> <th>DP4</th> </tr> </thead> <tbody> <tr> <td>Protection de substitution</td> <td>Obligatoire</td> </tr> </tbody> </table> <p>Tableau 16 : Exigence de sécurité de substitution.</p>	Exigence de sécurité de substitution des SPTs	DP4	Protection de substitution	Obligatoire	<input type="checkbox"/>
Exigence de sécurité de substitution des SPTs	DP4						
Protection de substitution	Obligatoire						
65	[3] 6.13	<p>Redondance des RCTs : pour le canton de Vaud, les RCTs doivent être conformes aux exigences de redondance selon exigence n°2 de la directive (voir Tableau 2 selon N°3, §5.2).</p>	<input type="checkbox"/>				

8.3 Documentation

N°	Réf norme	Description	Validation produit
66	[3] 6.14	<p>Documentation du RCT: La documentation relative au RCT doit être concise, complète et sans équivoque. Elle doit être suffisante pour permettre une installation, une mise en service et une maintenance fonctionnelles du RCT. Les informations fournies doivent être suffisantes pour permettre l'intégration des RCTs dans un ATS.</p> <p>La documentation du RCT doit inclure, au moins, les éléments suivants :</p> <ul style="list-style-type: none"> - le nom du fabricant et du fournisseur ; - la description du matériel ; - la norme à laquelle le composant est déclaré conforme ; - le nom ou la marque de l'organisme de certification ; 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

		<ul style="list-style-type: none"> - le nombre maximum de SPT pouvant être connectés pour les catégories DP2, respectivement DP4 ; - le nombre maximum d'AE pouvant être connectés ; - le nombre maximum d'interfaces du réseau de transmission ; - le nombre maximum d'alarmes pouvant être traitées par seconde ; - les catégories d'ATS pour lesquelles le RCT convient ; - les exigences d'alimentation électrique du RCT ; - une confirmation du mode demandé de fonctionnement des acquittements, selon exigences n°42 et n°43. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
67	[3] 6.15	<p>Marquage et identification :</p> <p>Le RCT doit être marqué avec les informations suivantes :</p> <ul style="list-style-type: none"> - le nom du fabricant ou du fournisseur ; - les catégories d'ATS pour lesquelles le RCT convient ; - le numéro de série. <p>Le marquage doit être lisible, durable et sans équivoque.</p> <p>Si le RCT n'utilise pas un matériel dédié (à savoir le RCT est une solution logicielle), le logiciel doit pouvoir afficher les marquages/identifications requis.</p>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

8.4 Performances / Tests et essais effectués

N°	Réf norme	Description	Validation produit																																							
68	[3] 7.3.1 à 7.3.19 inclus	<p>Pour le canton de Vaud, les RCTs relatifs aux catégories DP2 et DP4 doivent satisfaire à tous les tests décrits au chapitre 7 de la norme [3], selon les exigences et les procédures de tests y spécifiées. Le tableau ci-après synthétise la situation :</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Catégorie de RCT :</td> <td style="width: 25%;">DP2 <input type="checkbox"/></td> <td style="width: 25%;">DP4 <input type="checkbox"/></td> </tr> <tr> <td style="background-color: #e0e0e0;">Libellé de l'exigence</td> <td style="background-color: #e0e0e0;">N° de la directive</td> <td style="background-color: #e0e0e0;">Validation</td> </tr> <tr> <td>Traitement des signaux d'alarme</td> <td>52</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Niveaux d'accès</td> <td>53</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Téléchargement de logiciel</td> <td>54</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Stockage des paramètres et données spécifiques à l'utilisateur</td> <td>55</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Signalisation d'une défaillance de l'ATS pour un ATS à double voie</td> <td>56</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Interface(s) avec l'(les) AE</td> <td>57</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Signalisation des dérangements</td> <td>58</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Enregistrement d'évènements</td> <td>59</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Résolution et synchronisation d'horloge</td> <td>59, points 5 et 6</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Conservation du journal</td> <td>59, point 3</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> <tr> <td>Méthodes d'optimisation de stockage des évènements</td> <td>59, point 8</td> <td><input type="checkbox"/> OK <input type="checkbox"/> NOK</td> </tr> </table>	Catégorie de RCT :	DP2 <input type="checkbox"/>	DP4 <input type="checkbox"/>	Libellé de l'exigence	N° de la directive	Validation	Traitement des signaux d'alarme	52	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Niveaux d'accès	53	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Téléchargement de logiciel	54	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Stockage des paramètres et données spécifiques à l'utilisateur	55	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Signalisation d'une défaillance de l'ATS pour un ATS à double voie	56	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Interface(s) avec l'(les) AE	57	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Signalisation des dérangements	58	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Enregistrement d'évènements	59	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Résolution et synchronisation d'horloge	59, points 5 et 6	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Conservation du journal	59, point 3	<input type="checkbox"/> OK <input type="checkbox"/> NOK	Méthodes d'optimisation de stockage des évènements	59, point 8	<input type="checkbox"/> OK <input type="checkbox"/> NOK	<input type="checkbox"/>
Catégorie de RCT :	DP2 <input type="checkbox"/>	DP4 <input type="checkbox"/>																																								
Libellé de l'exigence	N° de la directive	Validation																																								
Traitement des signaux d'alarme	52	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																								
Niveaux d'accès	53	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																								
Téléchargement de logiciel	54	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																								
Stockage des paramètres et données spécifiques à l'utilisateur	55	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																								
Signalisation d'une défaillance de l'ATS pour un ATS à double voie	56	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																								
Interface(s) avec l'(les) AE	57	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																								
Signalisation des dérangements	58	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																								
Enregistrement d'évènements	59	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																								
Résolution et synchronisation d'horloge	59, points 5 et 6	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																								
Conservation du journal	59, point 3	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																								
Méthodes d'optimisation de stockage des évènements	59, point 8	<input type="checkbox"/> OK <input type="checkbox"/> NOK																																								

	Identification des utilisateurs des entrées de journal	59, note	<input type="checkbox"/> OK <input type="checkbox"/> NOK	
	Mode de fonctionnement – « pass-through » ou « store-and-forward »	60	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> OK <input type="checkbox"/> NOK	
	Exigences pour le fonctionnement en « forçage de la transmission » ou « enregistrement et transmission »	61	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> OK <input type="checkbox"/> NOK	
	Déni de service	62	<input type="checkbox"/> OK <input type="checkbox"/> NOK	
	Sécurité de l'information	63	<input type="checkbox"/> OK <input type="checkbox"/> NOK	
	Sécurité de substitution	64	<input type="checkbox"/> OK <input type="checkbox"/> NOK	
	Redondance du RCT	65	<input type="checkbox"/> OK <input type="checkbox"/> NOK	
	Documentation du RCT	66	<input type="checkbox"/> OK <input type="checkbox"/> NOK	
	Marquage et identification	67	<input type="checkbox"/> OK <input type="checkbox"/> NOK	
Tableau 17 : Synthèse des tests relatifs aux exigences à satisfaire par le RCT.				

9 Exigences relatives aux protocoles de transmission et de communication

Pour que le SPT et le RCT puissent communiquer entre eux, ces deux équipements doivent utiliser le même protocole de **transmission d'alarme** (c'est-à-dire parler « la même langue »). L'objectif est que les SPTs et RCTs de différents fournisseurs puissent être **interopérables**. A cet effet, un protocole mondial et très sécurisé est spécifié dans [9]. La directive du canton de Vaud s'y réfère et renvoie au contenu très technique de ce document. Seules les exigences principales sont rappelées ci-après, sous 9.2 en particulier. Un second protocole, l'ANSI/SIA DC-09, est également présenté sous 9.3 car la directive du canton de Vaud s'y réfère également (voir Tableau 18, ci-après).

L'**IP** (protocole Internet) est défini comme protocole de **transmission** de base incontournable pour la transmission sécurisée des alarmes.

Au niveau du **langage**, les protocoles de **transmission d'alarme** en vigueur dans le canton Vaud utilisant l'IP et leurs exigences respectives sont décrits ci-après.

9.1 Exigences générales

Le tableau ci-dessous résume les exigences générales relatives au protocole de **transmission d'alarme** utilisé en fonction du type d'ouvrage.

N°	Réf norme	Description	Validation produit																				
69	[9], [40], [41], [42]	<p>Le tableau ci-dessous résume les exigences de l'ECA pour le canton de Vaud :</p> <table border="1"> <thead> <tr> <th></th> <th>Autres protocoles</th> <th>ANSI/SIA DC-09 :2007 et suivante (Version 2013)</th> <th>TS 50136-9 ** / IEC 60839-7-8 TS Ed.1</th> </tr> </thead> <tbody> <tr> <td>Valeur de risque Prévention 1 et 2, installations existantes au 31.12.2016</td> <td>Accepté pendant la phase transitoire (jusqu'à fin 2018)</td> <td>-----</td> <td>-----</td> </tr> <tr> <td>Valeur de risque Prévention 1 et 2, nouvelles installations* dès le 1.01.2017</td> <td>-----</td> <td>Obligatoire *** (minimum requis)</td> <td>Recommandé ***</td> </tr> <tr> <td>Valeur de risque Prévention 3 et 4, installations existantes au 31.12.2016</td> <td>Accepté pendant la phase transitoire (jusqu'à fin 2018)</td> <td>Accepté jusqu'à fin 2020</td> <td>Obligatoire dès le 1.01.2021</td> </tr> <tr> <td>Valeur de risque Prévention 3 et 4, nouvelles installations* dès le 1.01.2017</td> <td>-----</td> <td>-----</td> <td>Obligatoire</td> </tr> </tbody> </table> <p>** Dans l'attente de l'officialisation de ce protocole normalisé, l'introduction d'autres protocoles normalisés demeure réservée.</p> <p>*** Les évolutions rapides en matière de sécurité informatique peuvent conduire au remplacement du protocole DC-09 par un protocole présentant une sécurité supérieure. C'est pourquoi, il est recommandé d'utiliser le TS 50136-9.</p> <p>Tableau 18 : protocole de transmission d'alarme utilisant le protocole Internet, en fonction du type d'ouvrage.</p> <p>*Note : l'exigence pour les nouvelles installations s'applique également en cas de travaux importants (mises à l'enquête via la CAMAC), ou de rénovations et de révisions sur des installations techniques existantes (détection, extinction).</p> <p>Toutes les nouvelles installations ou les remplacements d'installations existantes dès le 1.01.2017 devront disposer de transmetteurs d'alarmes supportant soit le protocole de transmission d'alarmes ANSI/SIA DC-09, soit le TS 50136-9 (selon Tableau 18).</p> <p>Les alarmes transmises sont encapsulées dans les 2 protocoles susmentionnés ; les trames des alarmes sont au format SIA DC-03 ([41]) ou SIA DC-05 ([42]). Les éventuelles données additionnelles aux alarmes doivent être encapsulées <u>directement</u> dans l'un des 2 protocoles de transmission d'alarmes susmentionnés (et non pas en SIA DC-03 ou en SIA DC-05).</p>		Autres protocoles	ANSI/SIA DC-09 :2007 et suivante (Version 2013)	TS 50136-9 ** / IEC 60839-7-8 TS Ed.1	Valeur de risque Prévention 1 et 2, installations existantes au 31.12.2016	Accepté pendant la phase transitoire (jusqu'à fin 2018)	-----	-----	Valeur de risque Prévention 1 et 2, nouvelles installations* dès le 1.01.2017	-----	Obligatoire *** (minimum requis)	Recommandé ***	Valeur de risque Prévention 3 et 4, installations existantes au 31.12.2016	Accepté pendant la phase transitoire (jusqu'à fin 2018)	Accepté jusqu'à fin 2020	Obligatoire dès le 1.01.2021	Valeur de risque Prévention 3 et 4, nouvelles installations* dès le 1.01.2017	-----	-----	Obligatoire	<input type="checkbox"/>
	Autres protocoles	ANSI/SIA DC-09 :2007 et suivante (Version 2013)	TS 50136-9 ** / IEC 60839-7-8 TS Ed.1																				
Valeur de risque Prévention 1 et 2, installations existantes au 31.12.2016	Accepté pendant la phase transitoire (jusqu'à fin 2018)	-----	-----																				
Valeur de risque Prévention 1 et 2, nouvelles installations* dès le 1.01.2017	-----	Obligatoire *** (minimum requis)	Recommandé ***																				
Valeur de risque Prévention 3 et 4, installations existantes au 31.12.2016	Accepté pendant la phase transitoire (jusqu'à fin 2018)	Accepté jusqu'à fin 2020	Obligatoire dès le 1.01.2021																				
Valeur de risque Prévention 3 et 4, nouvelles installations* dès le 1.01.2017	-----	-----	Obligatoire																				

73	[9] 5.2.3, 5.2.4.	Format des messages : <ol style="list-style-type: none"> 1. A l'exception du « Connection handle », tout le reste du message est chiffré, avec le chiffrement négocié lors de la mise en service. 2. Assignment du « Connection handle » : le processus d'assignation correspond à celui défini au chapitre 5.2.4. de la spécification technique [9]. 	<input type="checkbox"/> <input type="checkbox"/>
74	[9] 5.2.5.2	SPT Device ID (identifiant du SPT) : <ol style="list-style-type: none"> 1. Identifiant fixe, unique, en lecture seule, pendant toute la durée de vie du SPT (par ex. le numéro de série du SPT). 2. Se trouve dans la base de données SPTs, dans les RCTs. 3. Cet identifiant est créé lors de la fabrication du SPT. Il doit être communiqué au CTA pour être configuré dans les RCTs. 4. L'unicité de l'identifiant est assurée par l'un des principes définis sous 5.2.5.2 de [9]. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
75	[9] 5.2.5.3	RCT Device ID (identifiant du RCT) : <ol style="list-style-type: none"> 1. Identifiant unique, dans le RCT, inchangé pendant toute la durée de vie du RCT. 2. Est « rendu disponible » au SPT lors de la phase de mise en service. 	<input type="checkbox"/> <input type="checkbox"/>
76	[9] 5.2.6	Identifiants des messages : les identifiants des messages correspondent à ceux du tableau 4 de [9].	<input type="checkbox"/>
77	[9] 5.2.8	Numéros de séquences : le processus décrit sous 5.2.8 de [9] est implémenté.	<input type="checkbox"/>
78	[9] 5.2.9	Flags : des commandes à distance peuvent être incluses dans les messages de réponses, au moyen de flags selon 5.2.9 sous [9].	<input type="checkbox"/>
79	[9] 5.3	Longueur des messages et bits de bourrage (« padding ») : <ol style="list-style-type: none"> 1. La longueur des messages correspond à 5.3.2 de [9] 2. Le « Padding » correspond à 5.3.1 de [9] 	<input type="checkbox"/> <input type="checkbox"/>
80	[9] 5.4, 6.4.10, 6.4.11	Hachage : <ol style="list-style-type: none"> 1. Le RCT doit supporter <u>toutes</u> les méthodes de hachage (validation des messages) mentionnées au tableau 6 de [9]. 2. Le SPT doit supporter <u>au minimum</u> le SHA-256 (méthode par défaut retenue par le canton de Vaud). 3. Les méthodes de hachage correspondent à 6.4.10 et 6.4.11 de [9]. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
81	[9] 5.5.1, 6.4.6 à 6.4.9	Chiffrement (« Cryptage ») : <ol style="list-style-type: none"> 1. La méthode de chiffrement est négociée lors de la mise en service. 2. Le RCT doit supporter <u>toutes</u> les méthodes de chiffrement mentionnées au tableau 7 de [9]. Voir 6.4.6 et 6.4.7 de [9] pour les types de message à utiliser lors de cette mise en service. 3. En-dehors de la mise en service, le SPT doit supporter <u>au minimum</u> l'AES-128 (méthode par défaut retenue par le canton de Vaud). 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

		<p>4. La clé de chiffrement n'est valable que pour une seule connexion entre le SPT et les RCTs ; par conséquent, les RCTs doivent conserver la trace de toutes les clés utilisées par le SPT pour se connecter à eux.</p> <p>5. Le mode de fonctionnement à utiliser avec l'AES est le CBC (<i>Cipher Block Chaining</i>) comme spécifié dans NIST (publication spéciale 800-38A - édition 2001). Le vecteur d'initialisation est constitué de zéros uniquement.</p>	<input type="checkbox"/> <input type="checkbox"/>
82	[9] 5.5.2	<p>Echange de clés :</p> <p>1. La durée de vie de la clé est déterminée par le nombre de paquets transmis. Pour garantir la sécurité, les clés sont mises à jour régulièrement par les RCTs (« déclencheurs »), tous les N paquets transmis avec succès (utilise le compteur de séquence des RCTs comme référence) ; N est une valeur envoyée par les RCTs au SPT pendant la phase de première mise en service.</p> <p>2. Pour renforcer la sécurité, un échange de clé doit être déclenché par les RCTs au moins une fois par semaine ou au moins tous les $2^{16} = 65\ 536$ paquets transmis avec succès (selon la première provenance).</p> <p>3. En plus, tant le RCT que le SPT peuvent invoquer les échanges de clés supplémentaires.</p> <p>4. Pour éviter que le RCT et le SPT se désynchronisent lorsque un message d'alarme est transmis exactement en même temps qu'une session d'échanges de clés, le RCT doit conserver la clé relative à la session précédente, jusqu'à que la première transmission d'un paquet avec la nouvelle clé de session est quittancée positivement.</p>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
83	[9] 5.6	<p>Délais d'attente et tentatives (« timeouts & retries ») : les délais d'attente (suite auxquels un message sera retransmis) augmentent à chaque nouvelle tentative, tel que défini dans RFC793 (adaptation à la capacité de réseau disponible).</p> <p>L'objectif est de s'adapter à l'état de congestion du réseau : plus le réseau est chargé, plus la valeur de délai d'attente augmente, essayant ainsi d'éviter une surcharge des RCTs en cas de congestion du réseau.</p> <p>Les règles de 5.6 [9] s'appliquent strictement.</p>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
84	[9] 5.7	<p>Numéro de version : le numéro de version, se trouvant dans l'en-tête du message, est une valeur numérique (1 byte) non signé indiquant la version du protocole effectivement utilisé.</p> <p>Le SPT et les RCTs conviennent mutuellement de la version du protocole à utiliser lors de la phase de mise en service.</p>	<input type="checkbox"/> <input type="checkbox"/>
85	[9] 5.8, 5.2.9	<p>Commandes à distance : pour permettre à un RCT depuis le CTA d'envoyer des commandes à distance (à un SPT) sans dépendre des propriétés des réseaux entre les deux (par exemple, les règles de pare-feu et autres problématiques relatives aux réseaux), un mécanisme pour « encapsuler » les commandes à distance dans les messages de réponses est appliqué. Se référer à 5.2.9 de [9] et au tableau 8 de [9] pour les détails techniques.</p>	

			<input type="checkbox"/>
86	[9] 5.9	Valeurs de démarrage (« initiales », par défaut) : les valeurs du tableau 9 de [9] sont utilisées par le protocole de transmission du canton de Vaud, tant que les variables ne sont pas définies explicitement par des messages de configuration correspondants.	<input type="checkbox"/>
87	[9] 6.x, 6.2.2, 6.2.3, 6.3.1.x, 6.3.2., 6.4.x.	<p>Types de messages :</p> <ol style="list-style-type: none"> 1. Supervision de la voie de transmission : le message de configuration correspond à 6.4.12 de [9]. Un polling régulier entre le SPT et les RCTs et périodique (« heart beat » négocié lors de la mise en service) est en charge de cette supervision. Son format suit les exigences des tableaux 10 et 11 de [9]. 2. Rapports des événements (SPT → RCTs): le message (alarme) de l'événement doit toujours suivre le format des messages des tableaux 12 à 20 de [9]. 3. Format de réponse de l'événement (RCTs → SPT): le message de réponse à l'événement doit suivre le format du tableau 21 de [9]. 4. Messages de configuration : la plupart des paramètres configurables sont uniques dans le SPT (pour chaque RCT en rapport), soit : <ol style="list-style-type: none"> a. Connection Handle b. Device ID - identifiant c. Sélection du chiffrement d. Clé de session e. Hash (hachage) f. La surveillance de voie de transmission d'alarme. <p>Les règles décrites selon 6.4.2 / tableau 22 jusqu'à 6.4.23 / tableau 46 de [9] s'appliquent sans restriction pour le Canton de Vaud.</p> 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
88	[9] 7.1.2, 7.1.3.	<p>Mise en service et configuration de démarrage/connexion :</p> <ol style="list-style-type: none"> 1. La procédure de mise en service a pour but de permettre à l'émetteur-récepteur au sein des locaux surveillés SPT et à ceux au sein des RCTs de s'authentifier mutuellement. 2. 2 options sont possibles pour le canton de Vaud pour l'obtention du 'Master Set' (voir 7.1.3 de [9]), soit: <ol style="list-style-type: none"> a. génération en utilisant un «secret partagé» transmis hors bande (« out-of-band ») (voir 7.1.4.1 & 7.1.4.2 de [9]), ou b. utilisation des certificats X.509 et DTLS pour le RCT et le SPT (option pour le SPT) (voir 7.1.5 de [9]) 3. Quel que soit le mécanisme retenu ci-dessus pour l'obtenir, la clé principale est ensuite utilisée pour chiffrer, en utilisant l'AES256, l'échange des autres paramètres. Elle est également utilisée (par le protocole « en cours») pour établir la clé (s) de session. 4. La clé principale est une clé de 256 bits. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

		5. Le flux de messages au cours de la mise en service d'un nouveau SPT suit la procédure présentée au tableau 47 de [9].	<input type="checkbox"/>
89	[9] 7.2	<p>Configuration de la connexion : Lors d'une reconnexion, le 'Master Set' tel que négocié lors de la mise en service sera initialement utilisé pour le chiffrement (cryptage) et l'authentification des messages entre SPT et RCT. Les premières étapes consistent à demander de nouveaux paramètres de session pour les communications à suivre.</p> <p>Pendant la phase de configuration de la connexion, les paramètres suivants sont définis dans l'ordre ci-dessous, soit:</p> <ol style="list-style-type: none"> 1) Version du protocole mutuellement convenue entre le SPT et le RCT, 2) Sélection du chiffrement; 3) Clé de session; 4) Hash; 5) La surveillance de la voie de transmission d'alarme. <p>Le flux de messages pendant le démarrage de la connexion (pour obtenir les paramètres de la session) suit la procédure présentée dans le tableau 48 de [9].</p>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
90	[9] annexe A	Codes de résultats, de quittancements: le tableau A.1 de l'annexe A de [9] s'applique sans restriction pour le Canton de Vaud.	<input type="checkbox"/>
91	[9] annexe B	Identificateurs de protocoles : le tableau B.1 de l'annexe B de [9] s'applique sans restriction pour le Canton de Vaud.	<input type="checkbox"/>
92	[9] annexe C	« Secret partagé » : le formatage du « secret partagé » et son « checksum » sont définis selon l'annexe C et s'appliquent sans restriction pour le Canton de Vaud.	<input type="checkbox"/>

102	[40] version 2013, Annexe C	Les procédures d'autocontrôles informatives selon l'annexe C de [40] sont obligatoires pour le canton de Vaud.	<input type="checkbox"/>
103	[40] version 2013, Annexe F	Le contenu informatif de l'annexe F de [40] est obligatoire pour le canton de Vaud.	<input type="checkbox"/>
104	[40] version 2013, Annexe I	Les commandes à distances proposées à titre informatif à l'annexe I de [40] sont recommandées pour le canton de Vaud. L'ECA peut imposer ces commandes, selon la syntaxe proposée, lors d'applications spécifiques (réseaux d'eau,...).	<input type="checkbox"/>

10 Annexe « Classification de la valeur du risque prévention incendie en fonction de l'affectation des objets »

L'objectif de cette annexe est de décrire la méthodologie utilisée pour classer les objets raccordés en fonction d'une "valeur de risque prévention". Cette classification sert de base à la DDIS pour une évaluation sous l'angle opérationnel ("valeur de risque intervention").

Sous réserve de cas particuliers, la "valeur de risque prévention" est établie selon les critères suivants:

Affectation	Autres critères	Valeur de risque prévention
Hébergement type EMS, hôpital, home	> 20 personnes ou ≤ 20 personnes	4
Hébergement type hôtel, pension	> 100 personnes	3
	≤ 100 personnes	2
Surface de vente	> 2'400 m ²	3
	≤ 2'400 m ²	1 ou 2
Local recevant du public	> 300 personnes	3
	≤ 300 personnes	1 ou 2
Parking	-	1
Immeuble d'habitation	-	1 ou 2
Bâtiment industriel, administratif, scolaire, d'artisanat ou de stockage	> 10'000 m ²	3
	≤ 10'000 m ²	1
Entreposage ou manipulation de grandes quantités de matières dangereuses, et/ou assujettissement à l'OPAM	-	3

Tableau 19 : valeur de risque prévention en fonction du type d'ouvrage (affectation).

D'une manière générale, les mesures relatives à la phase d'exploitation des bâtiments sont fixées dans la directive AEAI 12-15. Plus spécifiquement, des **chargés de sécurité** en protection incendie doivent être désignés et formés lorsque la nature et la gravité du danger d'incendie, le nombre d'occupants, le caractère ou l'importance de l'exploitation l'exigent (voir affectations ci-dessus). La nécessité d'un chargé de sécurité incendie dans un bâtiment est donc directement liée au risque incendie de ce bâtiment en phase d'exploitation. En conséquence, l'ECA, en tant qu'autorité compétente, a décidé que le critère "nécessité d'un chargé de sécurité en protection incendie" constitue la base principale de l'évaluation de la "valeur de risque Prévention" (un chargé de sécurité devant être désigné pour un bâtiment avec risque de prévention égal à 3 ou 4, ce qui n'est pas le cas pour un bâtiment avec risque de prévention égal à 1 ou 2). La classification secondaire, soit le choix entre 3 ou 4, respectivement entre 1 ou 2, tient compte

de l'importance donnée à la protection des personnes et/ou la valeur particulière du bâtiment, en lien avec le patrimoine cantonal.

Le tableau ci-dessous synthétise la situation :

Valeur de risque Prévention	Chargé de sécurité ?	Risque pour protection des personnes ou valeur particulière du bâtiment ?
1	NON	NON
2		OUI
3	OUI	NON
4		OUI

Tableau 20 : valeur de risque prévention en fonction de la présence d'un chargé de sécurité.
