Réseau de transport d'électricité

ANNEXE D
Exigences de sécurité imposées par RTE pour le raccordement d'un client au réseau RMS cRPT

Contrat RR/RC

TABLE DES MATIERES

1. Objet du document

Le présent document édicte les règles de sécurité que doivent respecter les clients pour se raccorder au réseau RMS cRPT. Ces règles de sécurité répondent à deux objectifs :

- Protéger le réseau RMS cRPT et les flux qui circulent sur ce réseau, et, par conséquent, la sûreté du système électrique ;
- Protéger les clients en leur garantissant un bon niveau de sécurité du réseau de télécommunications auquel ils se connectent.

2. Définitions

Dans ce document, le terme « client » est une personne morale qui possède un ou plusieurs points de raccordement au réseau RMS cRPT.
Le terme « site client » est employé pour désigner un site géographique, placé sous la responsabilité d'un client, et sur lequel se trouve un point de raccordement au réseau RMS cRPT.
Le terme « réseau local cRPT » est employé pour désigner un réseau local, situé sur le site client, et sur lequel sont connectés les équipements d'interface avec RTE listés au paragraphe suivant.
Le terme « exploitant » est employé pour désigner l'entité chargée de garantir le maintien en condition opérationnelle et de sécurité des équipements connectés au réseau local cRPT.

3. Description de l'architecture, équipements concernés

Le réseau RMS cRPT est un réseau IP privé, de propriété RTE (une partie des supports sont des fibres optiques propriété de RTE, le reste est supporté par un IP VPN opérateur). Il est utilisé pour des échanges bidirectionnels entre RTE et ses clients. Ces échanges sont les suivants :

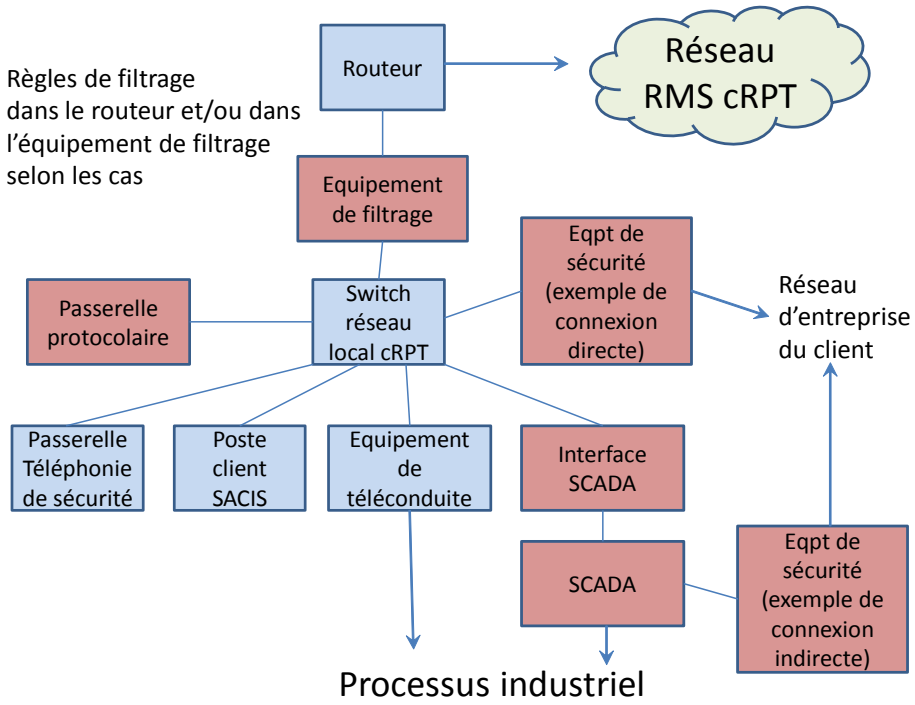
- Téléphonie de sécurité entre les dispatchings de RTE et les clients,
- Système d'alerte et de sauvegarde,
- Echanges de téléconduite (télémesures, télésignalisations, télécommandes, télévaleurs de consigne, téléréglages).

Sur chaque site client se trouvent tout ou partie des équipements suivants :

- Routeur(s) RMS
- Equipement de filtrage
- Réseau(x) local, switch(s)
- Passerelle pour la téléphonie de sécurité
- Poste client du Système d'alerte et de sauvegarde
- Equipement de téléconduite
- Equipement d'interface avec le SCADA de conduite des installations du client
- Passerelle protocolaire ayant pour but de convertir les protocoles de téléconduite utilisés avec RTE (104 ou TASE2) en protocole propre au client destiné à

échanger avec des applications de son réseau d'entreprise (un data historian, par exemple)

Le schéma suivant illustre cette architecture de raccordement.



Selon les clients, tous les équipements ne sont pas présents systématiquement ; les seuls équipements présents dans tous les cas sont le routeur et le switch. En amont du routeur (nuage « Réseau RMS cRPT » sur le schéma), il y a en général d'autres équipements sur le site client (modems, équipements optiques,…), appartenant à RTE ou à l'opérateur de télécommunications. Ces équipements ne sont pas concernés par les règles de sécurité ci-dessous et ne sont donc pas représentés.

En ce qui concerne **la limite de propriété** : tous les équipements sont propriété du client, à l'exception du routeur qui est propriété de RTE lorsque le site n'est pas une centrale de production.
En ce qui concerne **l'exploitation**, les équipements en rouge sur le schéma sont exploités par le client. Les équipements en bleu peuvent être exploités par RTE dans le cas où le client en a sous-traité la maintenance à RTE.
Lorsque RTE exploite le routeur (qu'il en soit propriétaire ou pas), il y intègre des règles de filtrage. Quand le routeur est exploité par le client, celui-ci peut implémenter des règles de filtrage dans le routeur ou dans l'équipement de filtrage facultatif.

4. Exigences sur l'architecture de raccordement du client au réseau RMS cRPT

Exigence D-1 : Les équipements listés au paragraphe C doivent se situer sur le réseau local cRPT. Si le client souhaite connecter[1] sur ce réseau local un équipement non listé au paragraphe C, même temporairement, il doit en faire la demande à RTE.

Si un client a raccordé sur le réseau local cRPT un équipement sans l'autorisation de RTE, RTE peut exiger son retrait[2]. En cas de défaut d'exécution, RTE peut aller jusqu'à déconnecter le site client afin de garantir la sécurité du réseau RMS cRPT. Dans ce cas, RTE ne sera redevable d'aucune compensation financière, pénalités ou autres, et le client ne sera pas rémunéré pour les services système non rendus pendant la durée de cette déconnexion. Ces dispositions financières s'appliquent aussi aux autres cas de déconnexion du réseau RMS cRPT (Cf. paragraphes F et H).

Exigence D-2 : Toute connexion, directe ou indirecte, entre le réseau local cRPT et le réseau d'entreprise du client doit se faire au travers d'un équipement de sécurité[3], pour lequel :

- Le client doit gérer les règles de filtrage implémentées dans cet équipement de sécurité de manière à interdire tout flux non autorisé sur le réseau local cRPT ;
- Le client doit collecter les logs sécurité de cet équipement de sécurité afin de surveiller, a minima en heures ouvrées, d'éventuelles tentatives d'intrusion sur le réseau local cRPT.

Exigence D-3 : Aucun flux d'information ne doit être échangé directement entre le(s) réseau(x) d'entreprise du client et le réseau RMS cRPT au travers du réseau local cRPT : les équipements présents sur le réseau local cRPT doivent être les seuls équipements qui peuvent dialoguer avec le(s) réseau(x) d'entreprise du client.

En complément des exigences précédentes, RTE recommande que les routeurs d'accès au réseau RMS cRPT et, s'ils sont distincts, les équipements de filtrage définis au paragraphe F, soient physiquement protégés contre tout accès non autorisés, en étant localisés dans des locaux accessibles uniquement aux personnes habilitées.

5. Exigences sur les flux de données

RTE définit les types de flux de données nécessaires aux fonctions listées au paragraphe C et les transmet au client. Les flux autorisés sont différents pour chaque client. RTE les définit donc au cas par cas en fonction des systèmes présents sur le réseau local cRPT du client. Les flux autorisés peuvent également évoluer dans le temps.

[1] Il s'agit ici d'une connexion numérique

[2] Cette règle admet cependant une exception : le client est autorisé à installer sur le réseau local cRPT des sondes de détection d'intrusion (IDS ou IPS) ou des analyseurs de protocoles.

[3] Désigné sous ce nom sur le schéma du paragraphe C, il y a deux emplacements possibles (connexion directe ou indirecte)

Exigence E-1 : Le client ne doit pas faire transiter d'autres types de flux sur le réseau RMS cRPT que ceux autorisés par RTE.

Exigence E-2 : Le client ne doit pas utiliser le réseau RMS cRPT pour d'autres besoins que les échanges avec les dispatchings de RTE. En particulier, un client ne doit pas utiliser le réseau RMS cRPT pour des échanges de données entre ses propres sites.

6. Règles de sécurité du point d'accès au réseau RMS cRPT

Le client peut mettre en place un filtrage des flux qui transitent depuis son site vers le réseau RMS cRPT, dans le but de garantir le respect des exigences sur les flux du paragraphe E (filtrage sur les adresses IP source et destination ainsi que sur les ports TCP, par exemple). Le client peut intégrer cet éventuel filtrage dans le routeur RMS s'il en est propriétaire ou dans un équipement dédié[4] s'il souhaite renforcer sa sécurité. Cependant, ce filtrage n'est pas imposé car RTE met en œuvre un filtrage équivalent sur les routeurs RTE du réseau RMS cRPT.

Exigence F-1 : Dans le cas où RTE n'est pas le propriétaire des routeurs RMS du site client, le client doit garantir que le système d'exploitation des routeurs intègre les derniers correctifs de sécurité. Pour ce faire :

- Le client doit intégrer tout correctif de sécurité dans un délai maximal de deux ans après sa publication par l'éditeur. Ceci implique que le client doit upgrader les matériels ou logiciels lorsqu'ils ne sont plus supportés par l'éditeur.
- Le client doit mettre en œuvre un processus de veille sécurité et alerter RTE en cas de publication d'une faille qu'il estime critique.

La décision sur la conduite à tenir est alors prise d'un commun accord entre le client et RTE. En cas de désaccord, RTE jugera si la criticité de la faille justifie la déconnexion temporaire du site client du réseau RMS cRPT en attendant qu'il intègre le correctif.

Exigence F-2 : Dans le cas où RTE n'est pas propriétaire des routeurs RMS du site client, le client doit protéger le compte administrateur des routeurs par une authentification à double facteur ou, à défaut, par un mot de passe :

- qui doit comprendre au moins huit caractères et au moins trois types de caractères différents parmi : lettres majuscules, lettres minuscules, chiffres, caractères spéciaux ;
- et qui doit être changé au moins une fois par an.

Exigence F-3 : Les communications sur le réseau RMS cRPT doivent être chiffrées. Dans le cas où RTE n'est pas propriétaire des routeurs RMS du site client, le client doit configurer le routeur selon les directives de RTE, ce chiffrement étant basé sur une clé partagée choisie par RTE.

[4] Dénommé « équipement de filtrage » sur le schéma du paragraphe C

Si RTE n'est pas l'administrateur des routeurs, à chaque fois que RTE décide de modifier cette clé, le centre de supervision réseau de RTE (le CASTEN), contacte le client afin de planifier la date et l'heure du changement et lui transmettre la nouvelle clé.

Exigence F-4 : Les mots de passe des routeurs et la clé de chiffrement figurent dans la configuration du routeur. Dans le cas où RTE n'est pas propriétaire du routeur, le client doit chiffrer ces informations sensibles avec un algorithme d'une complexité correspondant a minima à l'état de l'art, et qui peut évoluer dans le temps à la demande de RTE.

A la date de publication de ce document, les algorithmes utilisés doivent être :

- Pour les mots de passe : un hachage MD5 ;
- pour la clé de chiffrement : un codage AES basé sur une clé qui ne doit pas figurer dans la configuration du routeur.

7. Dispositif de surveillance

Dans le cas où RTE est propriétaire ou administrateur des routeurs RMS, il se charge de surveiller les logs sécurité des routeurs. S'il le souhaite, le client peut néanmoins demander à RTE de lui mettre à disposition ces logs pour mettre en œuvre sa propre surveillance sécurité. L'architecture pour la connexion du centre opérationnel de sécurité du client à ces routeurs est à la charge du client et doit être définie en commun avec RTE.

Exigence G-1 : Dans le cas où RTE n'est pas administrateur des routeurs RMS du site client, le client doit surveiller a minima les logs de connexion aux routeurs.

Exigence G-2 : Dans tous les cas, le client doit alerter le centre opérationnel de sécurité de RTE lorsqu'il détecte une activité suspecte via ses outils de surveillance.

RTE communique au client les coordonnées de son centre opérationnel de sécurité, joignable a minima en heures ouvrées. Les types d'événements pour lesquels le client doit alerter le centre opérationnel de sécurité de RTE dépendent de la nature des événements que le client surveille. Ils sont par exemple :

- Activité suspecte détectée entre le réseau RMS cRPT et réseau local cRPT du site client, ou l'inverse (détectable dans le cas où le client surveille les logs sécurité du routeur et qu'il y a implémenté des règles de sécurité, ou s'il a installé un équipement de filtrage derrière le routeur) ;
- Activité suspecte entre le réseau local cRPT et le réseau d'entreprise du client, détectable via la surveillance de l'équipement de sécurité (Cf. exigence D-2) si celui-ci existe ;
- Virus détecté, activité malveillante, connexion ou tentative de connexion non autorisée sur les systèmes en interface avec RTE (poste client SACIS, équipement de téléconduite, routeur…), éventuellement détectables selon la nature de la surveillance mise en place par le client sur ces équipements, la seule surveillance

obligatoire est celle de l'exigence G-1, dans le cas où ce n'est pas RTE qui administre les routeurs ;
- Vol de matériel, indispensable dans le cas des routeurs, afin que RTE modifie aussitôt les clés de chiffrement des communications.

Dans tous les cas, RTE surveille la sécurité du réseau RMS cRPT et doit donc pouvoir contacter le client lorsqu'il détecte un événement sécurité :

Exigence G-3 : Le client doit communiquer à RTE les coordonnées de son autorité de sécurité que RTE doit contacter lorsqu'il détecte sur le réseau RMS cRPT une activité suspecte qui le concerne.

8. Dispositions à prendre en cas d'alerte avérée

Lorsqu'une alerte est détectée par RTE ou par le client, RTE s'autorise à prendre toutes les mesures appropriées pour protéger la sécurité du réseau RMS cRPT, pouvant aller jusqu'à une déconnexion du site client.

Exigence H-1 : Dans le cas où RTE n'est pas l'exploitant des routeurs RMS du site client, ou si une action à distance n'est pas possible, RTE peut demander au client de se déconnecter physiquement du réseau RMS cRPT (débranchement des routeurs). Dans ce cas, c'est le centre opérationnel de sécurité de RTE qui fait la demande au client par téléphone. Le client doit alors rappeler le centre opérationnel de sécurité de RTE (coordonnées téléphoniques définies au paragraphe G) pour faire confirmer l'ordre de déconnexion. La procédure est identique pour la reconnexion.

L'exigence précédente implique que le client doit identifier visuellement un lien physique permettant de couper la connexion par un geste simple à la portée d'un opérateur peu qualifié.

Exigence H-2 : Afin de mener les analyses a posteriori, le client doit fournir au centre opérationnel de sécurité de RTE, sur demande, et sous un délai maximal de deux jours ouvrés, les logs sécurité des routeurs et des éventuels équipements de sécurité[5]. Le client doit tenir à disposition ces logs pendant une durée minimale de 6 mois.

9. Vérification de la conformité

Exigence I-1 : Le client doit fournir à RTE, au moment du raccordement du site, puis à chaque modification des équipements connectés au réseau ou sur demande de RTE :
- le schéma à jour qui représente l'architecture du réseau local cRPT ainsi que tous ses points de connexion avec d'autres parties du Système d'Information du client ;
- une attestation de conformité aux exigences du présent document.

[5] Il s'agit des équipements de filtrage et de sécurité sur le schéma du paragraphe C

Exigence I-2 : Dans le cas où RTE n'est pas l'administrateur du routeur RMS, le client doit informer RTE au moins une fois par an de ses caractéristiques : type de matériel et version logicielle (contrôle du respect de l'exigence F-1).

Exigence I-3 : Sur demande de RTE, le client doit fournir la configuration des équipements de sécurité (contrôle du respect de l'exigence D-2).

FIN DU DOCUMENT