Réseau de transport d'électricité

Exigences de sécurité imposées aux clients de RTE pour le raccordement et l'utilisation du réseau de téléconduite

Indice 1

A – Objet du document

Le présent document édicte les règles de sécurité que doivent respecter les clients pour se raccorder et utiliser le réseau de télécommunications qui supporte les échanges de téléconduite entre RTE et ses clients. Ces règles de sécurité répondent à trois objectifs :

- protéger le réseau de téléconduite et les flux qui circulent sur ce réseau, et, par conséquent, la sûreté du système électrique ;
- protéger les réseaux informatiques des clients en leur garantissant la sécurité du réseau de télécommunications auquel ils se connectent ;
- répondre aux exigences de la loi de programmation militaire 2014-2019 (promulguée le 18 décembre 2013).

Afin de garantir les objectifs ci-dessus, RTE met également en œuvre des mesures de sécurité du même type sur ses propres équipements réseau et sécurité connectés au réseau de téléconduite. Ces règles de sécurité internes à RTE ne sont pas décrites dans ce document, cependant RTE s'engage vis-à-vis de ses clients à prendre les mesures nécessaires. En particulier, RTE se conforme aux exigences réglementaires du secteur énergie.

B - Définitions

Les mots ou groupes de mots utilisés dans la suite de ce document et dont la première lettre est en majuscule ont la signification qui leur est donnée ci-dessous :

- Client : utilisateur du réseau public de transport ou gestionnaire de réseau de distribution qui est responsable vis-à-vis de RTE d'un ou plusieurs Sites raccordés au Réseau de Téléconduite Clients de RTE.
- Réseau de Téléconduite Clients : réseau de télécommunications longue distance qui supporte les échanges de téléconduite, de téléphonie de sécurité et de sauvegarde entre les dispatchings de RTE et les Clients.
- Site ou Site Client : site géographique, placé sous la responsabilité d'un Client, et sur lequel se trouve un point de raccordement au Réseau de Téléconduite Clients.
- Réseau Local de Téléconduite : réseau local, situé sur un Site Client, et sur lequel sont connectés les équipements en interface avec RTE qui sont listés au paragraphe C.

Direction des systèmes d'information et des télécommunications
Tour Marchand
41 rue Berthelot - 92411 COURBEVOIE CEDEX
tel. 01.78.66.50.00 fax. 01.78.66.50.64

- Administrateur (d'un équipement) : entité mandatée par le Client pour mettre en œuvre les modalités relatives au maintien en condition opérationnelle et de sécurité d'un équipement connecté au Réseau Local de Téléconduite, telles que prévues par les présentes règles de sécurité.
- Heures Ouvrées : En jours ouvrés du Client, les horaires de travail dans la journée sont ceux du Client.

C – Description de l'architecture, équipements concernés

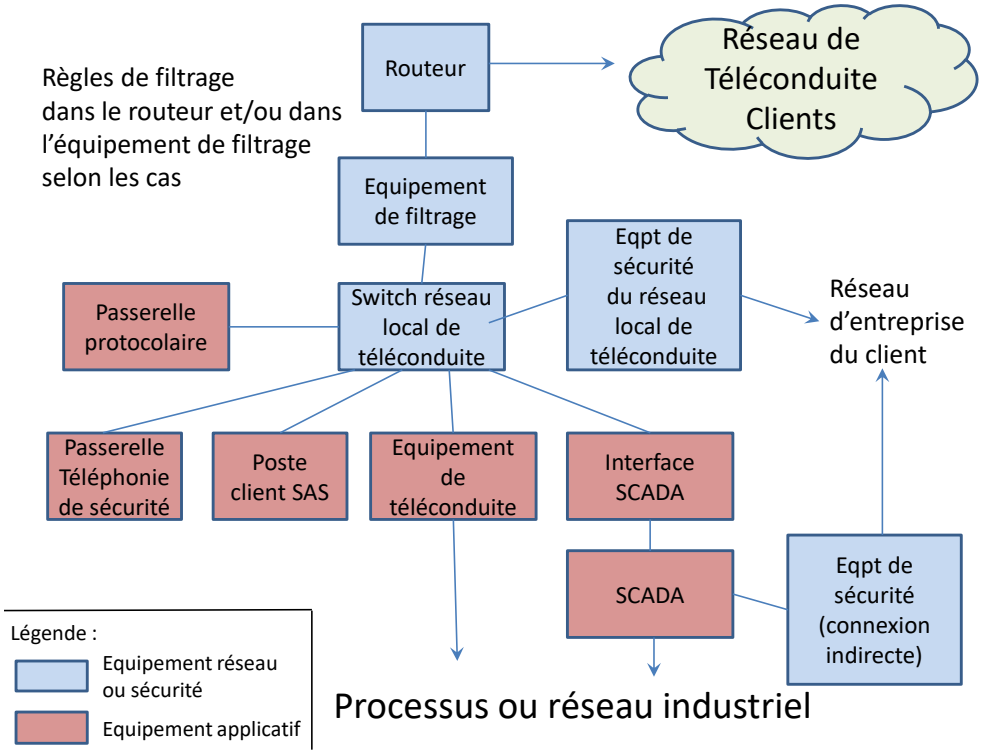
Le Réseau de Téléconduite Clients est un réseau IP privé, de responsabilité RTE. Il est utilisé pour des échanges bidirectionnels entre RTE et ses Clients afin de mettre en œuvre tout ou partie des fonctionnalités suivantes, selon l'éligibilité du Site :

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

Sur chaque Site Client se trouvent tout ou partie des équipements suivants :

- Routeur
- Equipement de filtrage
- Réseau local, switch
- Passerelle pour la téléphonie de sécurité
- Poste client du système d'alerte et de sauvegarde
- Equipement de téléconduite local
- 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)
- Equipement de sécurité destiné à filtrer/sécuriser les échanges avec le réseau d'entreprise du client, s'ils existent. Ce réseau d'entreprise doit être compris comme le (ou les) réseau qui héberge les postes bureautiques ou les systèmes et applications non industrielles.

Le schéma suivant illustre cette architecture de raccordement, dont plusieurs instances peuvent exister sur un seul Site.



Tous les équipements ne sont pas présents systématiquement sur le Site Client ; le seul équipement présent dans tous les cas est le routeur (le switch est toujours présent – fonctionnellement – mais peut être physiquement regroupé avec l'équipement de filtrage). En amont du routeur (nuage « Réseau de Téléconduite Clients » 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.

Tous les équipements sont propriété du Client, à l'exception du routeur[1] qui peut dans certains cas être propriété de RTE.
Lorsque RTE administre le routeur, il y intègre des règles de filtrage. Lorsque le Client administre le routeur, il peut implémenter des règles de filtrage dans le routeur ou dans l'équipement de filtrage facultatif.

D - Exigences sur l'architecture de raccordement au Réseau de Téléconduite Clients

Exigence D-1 : A l'exception du routeur, les équipements listés au paragraphe C doivent se situer sur le Réseau Local de Téléconduite. Si le Client souhaite connecter[2] sur ce réseau local un équipement non listé au paragraphe C, même temporairement, il doit en faire la demande à RTE[3].

[1] Et aussi le switch dans le cas particulier de l'offshore
[2] Il s'agit ici, ainsi que dans la suite du document, d'une connexion numérique
[3] Cette règle admet cependant une exception : le Client est autorisé à installer sur le Réseau Local de Téléconduite des sondes de détection d'intrusion (IDS, IPS) ou des analyseurs de protocoles.

Si un Client a raccordé sur le Réseau Local de Téléconduite un équipement sans l'autorisation de RTE, RTE peut exiger son retrait. En cas de défaut d'exécution, RTE peut déconnecter le Site Client afin de garantir la sécurité du Réseau de Téléconduite Clients, conformément aux modalités définies au paragraphe I.

Exigence D-2 : Toute connexion[2], directe ou indirecte, entre le Réseau Local de Téléconduite et le réseau d'entreprise du Client doit se faire au travers d'un équipement de sécurité[4], 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 de Téléconduite ;
- Le Client doit collecter 24 heures sur 24 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 de Téléconduite.

Exigence D-3 : Aucun flux d'information ne doit être échangé directement entre le(s) réseau(x) d'entreprise du Client et le Réseau de Téléconduite Clients au travers du Réseau Local de Téléconduite : les équipements présents sur le Réseau Local de Téléconduite doivent être les seuls équipements qui peuvent dialoguer avec le(s) réseau(x) d'entreprise du Client.

Exigence D-4 : Les échanges directs (i.e. sans traverser d'équipements de sécurité) avec le réseau industriel du Client sont autorisés, notamment lorsqu'un un SCADA est présent. Cependant, dans le cas où cette connexion directe existe, le réseau industriel ne devra pas être connecté à Internet, même au travers d'un coupe-feu ; les points accès Internet doivent être situés sur le réseau d'entreprise du Client.

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

E - 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 potentiellement différents pour chaque Site. RTE les définit donc au cas par cas selon les fonctions mises en œuvre sur le Site Client. Les flux autorisés peuvent également évoluer dans le temps sous réserve d'accord des deux parties, le document qui définit les flux autorisés est alors mis à jour.

Exigence E-1 : Le Client ne doit pas faire transiter d'autres types de flux sur le Réseau de Téléconduite Clients que ceux autorisés par RTE.

[4] Désigné sous ce nom sur le schéma du paragraphe C, il y a deux emplacements possibles (connexion sur le réseau local de téléconduite ou connexion indirecte)

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

F – Exigences de sécurité sur le point d'accès au Réseau de Téléconduite Clients

Le Client peut mettre en place un filtrage des flux qui transitent depuis son Site vers le Réseau de Téléconduite Clients, 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 s'il en est propriétaire ou dans un équipement dédié[5] 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 de Téléconduite Clients.

Exigence F-1 : Lorsque le Client est le propriétaire des routeurs de son Site, il 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[6].
- Le Client doit mettre en œuvre un processus de veille sécurité et alerter le centre opérationnel de sécurité de RTE en cas de publication d'une faille qu'il estime critique.

En cas publication de faille critique, la décision sur la conduite à tenir et sur les dispositions palliatives est 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 de Téléconduite Clients en attendant qu'il mette en œuvre des mesures appropriées. Cette déconnexion se fait alors selon les modalités définies au paragraphe I.

Exigence F-2 : Les comptes administrateur des routeurs du Site Client doivent être protégés 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 de Téléconduite Clients doivent être chiffrées. Les routeurs du Site Client doivent être configurés selon les directives de RTE, ce chiffrement étant basé sur une clé partagée choisie par RTE.

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

[6] RTE tient à disposition du Client la liste des types de routeurs qui ont fait l'objet de tests de compatibilité.

Chaque fois que RTE décide de modifier cette clé, le centre de supervision réseau de RTE (le CASTEN) contacte le Client ou son Administrateur mandaté pour 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 le routeur. Ces informations sensibles doivent être chiffrées 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 : du SHA 256 ou a minima 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.

Exigence F-5 : Le Client doit prévenir le centre opérationnel de sécurité de RTE sans délai en cas de vol d'un routeur. RTE lancera alors l'opération de modification des clés de chiffrement.

G – Exigences relatives au dispositif de surveillance

Dans le cas où RTE est propriétaire des routeurs, il se charge de surveiller leurs logs sécurité.
Si le Client a besoin d'implémenter une connexion avec les routeurs 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 : Si le Client est propriétaire des routeurs, le Client ou son Administrateur mandaté 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 les jours ouvrés à RTE entre 8h et 17h. 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 de Téléconduite Clients et le Réseau Local de Téléconduite 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 sur le Réseau Local de Téléconduite, 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 de l'outil de sauvegarde, 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 étant celle de l'exigence G-1 ;

- Vol de matériel sur le réseau Local de Téléconduite, obligatoire dans le cas des routeurs (Cf. exigence F-5).

Dans tous les cas, RTE surveille la sécurité du Réseau de Téléconduite Clients 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 pouvoir contacter a minima en Heures Ouvrées lorsqu'il détecte sur le Réseau de Téléconduite Clients une activité suspecte qui le concerne.

H - 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 de Téléconduite Clients, pouvant aller jusqu'à une déconnexion du Site Client.

Exigence H-1 : RTE peut demander[7] au Client de se déconnecter du Réseau de Téléconduite Clients (action sur les routeurs)[8]. 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. Le délai d'exécution est alors de deux heures. 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 facilement.

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[9]. Le Client doit tenir à disposition ces logs pendant une durée minimale de 6 mois.

Dans le cas d'un équipement de sécurité avec connexion indirecte, RTE n'est pas à même d'analyser ses logs sécurité car cet équipement fait transiter des informations qui ne concernent pas RTE. Si une analyse s'avère nécessaire à ce niveau, elle est faite par les experts sécurité du Client, qui en communiquent les résultats au centre opérationnel de sécurité de RTE. Toute analyse effectuée par RTE fait l'objet d'un rapport écrit que RTE s'engage à transmettre au client.

I – Vérification de la conformité et modalités de déconnexion en cas de non-conformité

[7] Uniquement en Heures Ouvrées

[8] En général action logique (shutdown) ou bien action physique, par exemple si une action à distance s'avère impossible

[9] Sur le schéma du paragraphe C, il s'agit de l'équipement de filtrage et de l'équipement de sécurité du réseau local de téléconduite.

Exigence I-1 : Le Client doit fournir à RTE, au moment du raccordement du Site, puis à chaque modification des équipements connectés au Réseau Local de Téléconduite ou sur demande de RTE :

- le schéma à jour qui représente l'architecture du Réseau Local de Téléconduite ainsi que tous ses points de connexion avec d'autres parties du Système d'Information du Client ;
- les coordonnées de son autorité de sécurité ;
- le cas échéant, les coordonnées de l'Administrateur mandaté pour mettre en œuvre les exigences de sécurité conformément aux modalités décrites ci-dessus ;
- une attestation de conformité aux exigences du présent document.

Exigence I-2 : Dans le cas où RTE n'est pas propriétaire du routeur, le Client ou son Administrateur mandaté 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 donner accès à RTE à la configuration des équipements de sécurité (dans l'objectif de contrôle ponctuel du respect de l'exigence D-2).

En cas d'écart par rapport aux exigences du présent document, le Client se rapproche de RTE pour analyser conjointement la consistance de l'écart ainsi que les moyens organisationnels et techniques mis en œuvre pour pallier cet écart. RTE analyse les conséquences de l'écart sur la sécurité du Réseau de Téléconduite Clients.
Lorsque le non-respect d'une exigence par le Client porte atteinte à la sécurité du Réseau de Téléconduite Clients, RTE peut refuser le raccordement du Site Client au Réseau de Téléconduite Clients ou déconnecter le Site Client du Réseau de Téléconduite Clients après une mise en demeure restée infructueuse à l'issue d'un délai de 3 mois. Toutefois, ce délai peut être réduit par la mise en demeure, en fonction de la nature de l'inexécution et des risques induits sur le Réseau de Téléconduite Clients. Dans cette hypothèse, le délai sera indiqué dans la mise en demeure qui sera adressée par télécopie et confirmée par lettre recommandée avec demande d'avis de réception.
Dans le cas où le Client est déconnecté du Réseau de Téléconduite eu égard au non-respect d'une exigence, RTE ne sera redevable d'aucune compensation financière, pénalités ou autres, et le Client supporte toutes les conséquences de cette déconnexion (par exemple en termes de rémunération des services système non rendus pendant la durée de cette déconnexion).

J – Modèle d'attestation de conformité

Attestation de conformité aux exigences de sécurité imposées aux clients de RTE pour le raccordement et l'utilisation du réseau de téléconduite

Le Client *[Nom du Client]* déclare avoir pleinement connaissance et accepter sans réserve les dispositions définies dans le document « Exigences de sécurité imposées pour le raccordement d'un client au réseau de téléconduite » indice *[x]* et dans la documentation technique de référence de RTE. Ces dispositions complètent les prescriptions Système d'Information transmises par RTE dans le cadre du raccordement.

Par la présente attestation, le Client atteste que le(s) site(s) ci-dessous, placé(s) sous sa responsabilité et raccordé(s) au Réseau de Téléconduite Clients de RTE est(sont) conforme(s) aux exigences définies dans ce document :

- *Lister le(s) Site(s) Client*

Le Client peut préciser les moyens organisationnels et techniques mis en œuvre pour répondre à ces exigences.

Le cas échéant, le Client précise les écarts et s'engage sur l'échéance de leur résorption ou s'assure auprès de RTE que les moyens organisationnels et techniques mis en œuvre par le Client permettent de pallier cet écart et de ne pas porter atteinte à la sécurité du Réseau de Téléconduite Clients.

Pour *[Nom du Client]*

Nom – Prénom
Qualité
Signature

Fait à
Le

FIN DU DOCUMENT