



Gestionnaire
du Réseau de Transport d'Electricité

ENJEUX DE SÉCURITÉ DES INFRASTRUCTURES SCADA POUR LE TRANSPORT DE L'ÉLECTRICITÉ

CLUSIF
Paris, 17 avril 2007

Philippe Bedu – Frédéric Lenoir
RTE - Réseau de Transport d'Electricité
www.rte-france.com

Sommaire

- **Présentation de RTE**
- **Gestion de la sécurité du SI à RTE**
- **Le SI temps réel : ouverture sur le reste du SI**
- **Plusieurs niveaux de protection :**
 - **Périmétrique**
 - **Logique**
 - **Physique**
- **Surveillance de la sécurité du SI**

Les missions de RTE

Record de consommation : 86 000 MW
 78000 KM de lignes HT/THT
 2400 Postes de transformations
 46 interconnexions

- **Gestion de l'infrastructure de transport HT/THT**
 RTE exploite et entretient le réseau public de transport et est responsable de son développement, en minimisant le coût pour la collectivité, en veillant à la sûreté du système, des personnes et des biens.

- **Gestion des flux d'énergie**
 RTE gère les flux d'électricité et procède aux ajustements, gère les droits d'accès aux interconnexions internationales en collaboration avec les gestionnaires de réseaux voisins, RTE mobilise les réserves et compense les pertes, procède aux comptages nécessaires et règle les écarts.

- **Garantie de l'accès au réseau de transport**
 RTE conclut des contrats avec les utilisateurs du réseau de transport, sur la base des tarifs d'accès aux réseaux et dans le respect des règles de non-discrimination



Les deux grands métiers de RTE

Le système électrique et la gestion de flux

- l'accès au réseau ;
- la sûreté du système électrique ;
- la maîtrise d'ouvrage du développement du réseau.



Le transport électrique et la gestion du réseau

- la maintenance du réseau ;
- l'ingénierie du développement du réseau.

Gérer les cyber risques des objectifs et des moyens

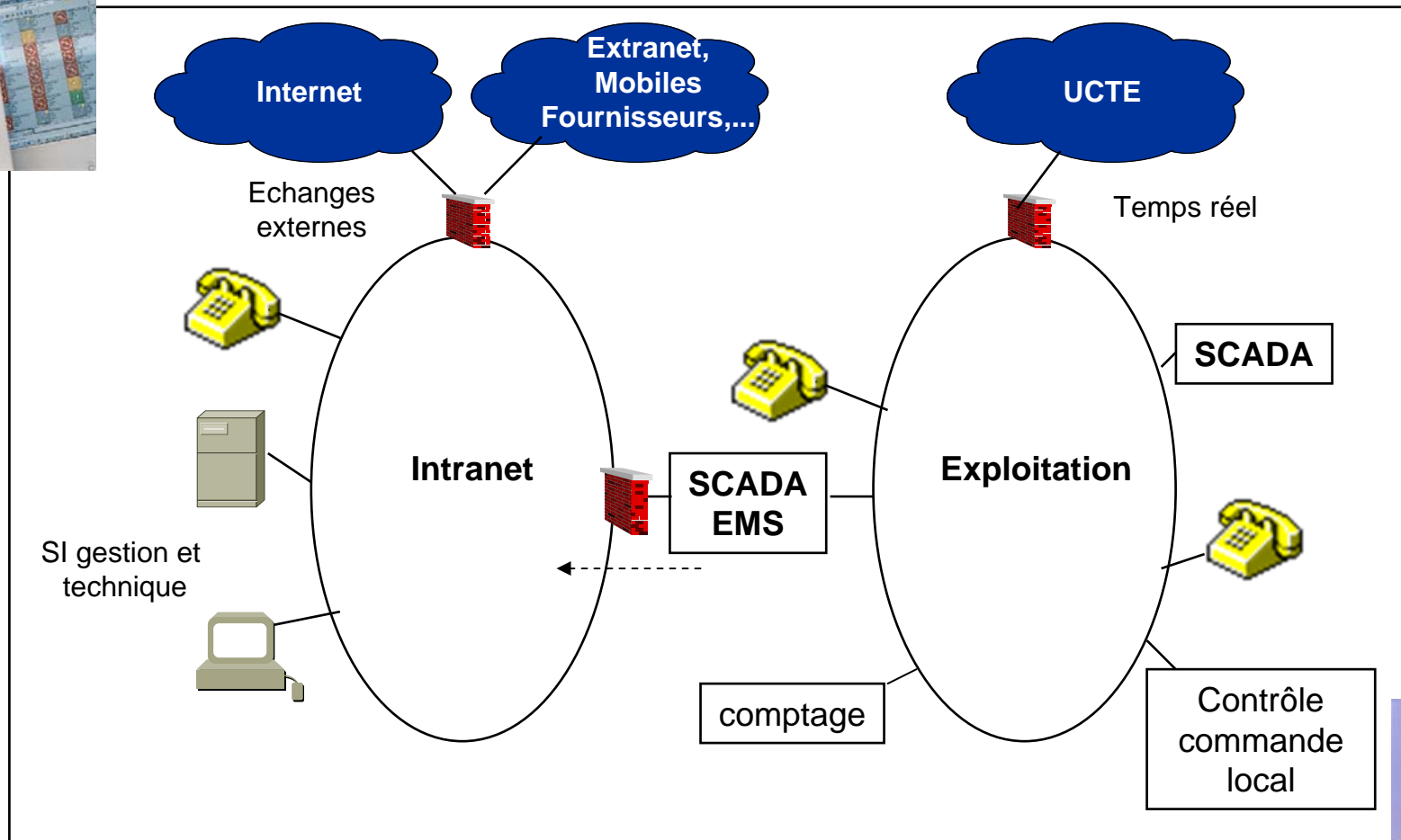
- **Une politique de sécurité SI alignée sur les enjeux de RTE**
 - Aucune plainte, imputable au SI, pour non respect de la confidentialité ou pour discrimination
 - Aucun Événement Sûreté Système imputable au SI ne doit atteindre un niveau de criticité supérieur à « C »*
 - Limiter à un montant maximum annuel les conséquences des dysfonctionnements du SI
- **Une mise en œuvre basée ...**
 - Sur des standards et des bonnes pratiques
 - Sur une analyse et des mesures de maîtrise des risques

(*) sur une échelle de A à F, incident généralisé national

Sécurité SI : analyse et mesures de maîtrise des risques

- **Veille et analyse des risques**
 - Standards, fournisseurs, CERTs (Computer Emergency Response Team), protection des infrastructures critiques ...
- **Mesures techniques**
 - Architecture, ingénierie, Coupe-Feu, cryptage, authentification, audit ...
- **Une organisation pour gérer la sécurité**
 - Responsable Sécurité SI national et local, experts, organisation de crise
- **Sensibilisation des utilisateurs du SI**
- **Sécurité physique**
- **Engagements contractuels, application de la loi**

Une architecture SI en domaines de sécurité pour une défense en profondeur



Une approche classique pour la sécurité du SI industriel

- **Protection du système d'information par des mesures techniques conformes à l'état de l'art, par exemple**
 - dispositifs "coupe-feu" entre les réseaux externes et les réseaux internes.
 - règle du « tout ce qui n'est pas explicitement autorisé est interdit »
 - association par authentification des utilisateurs avec droits d'accès
 - formation et sensibilisation de son personnel aux cyber-risques
 - procédures alternatives en cas de dysfonctionnement de son informatique

- **RTE partage son expérience de la lutte contre les cyber menaces avec**
 - Les industriels fournisseurs de ses systèmes.
 - Des associations professionnelles comme le **CLUSIF** (CLUb de la Sécurité Informatique Français), le **CIGRE** (Conseil International des Grands Réseaux Électriques), l'**UCTE** (Union for the Co-ordination of Transmission of Electricity), etc.
 - Les services de l'État

Protection physique des équipements SCADA

- Les machines SCADA sont placées physiquement dans des zones à **accès renforcé**
- Ces zones à accès renforcé **sont dédiées** aux applications Temps Réel de conduite dont les SCADA sont le noyau central

Réseaux de Télécommunications de sécurité propriétaires

- Des moyens de transmission dédiés à l'usage de RTE pour les flux temps réels
- Réseau d'information administré et supervisé par RTE
- Points d'interconnexion sécurisés par coupe-feu
- Séparation entre Zones de confiance et reste du SI

Administration et supervision de la sécurité

- La sécurité est administrée et supervisée par RTE (possibilité d'isoler si besoin le SI temps réel du reste)
- Supervision des équipements ainsi que des évènements sécurité dans le but de détecter des comportements matériels et flux anormaux