CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

Retour d'expérience RTE suite à Stuxnet

RTE: le Gestionnaire du Réseau de Transport d'Electricité en France

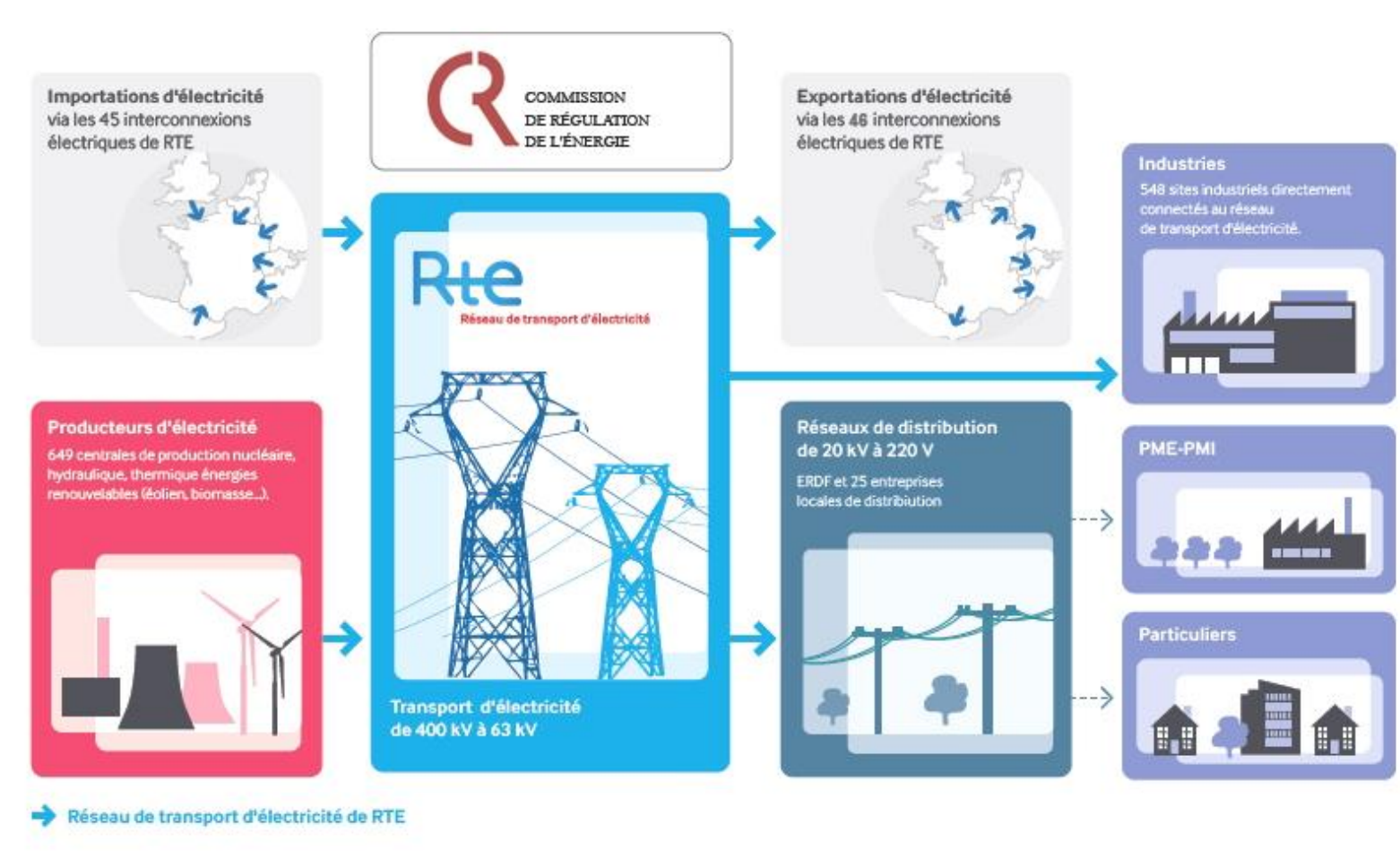
L'électricité ne se stocke pas à l'échelle industrielle et la demande varie très fortement. Pour répondre à ces contraintes, RTE doit être en mesure de fournir un flux tendu d'électricité à chaque instant.

RTE est le garant du bon fonctionnement et de la sûreté du Système Electrique Français.

RTE a pour missions d'exploiter, maintenir et développer le réseau électrique HT et THT (de 63 kV à 400 kV)

- 105 000 km de lignes électriques
- 2 600 postes électriques

Les acteurs du marché de l'électricité

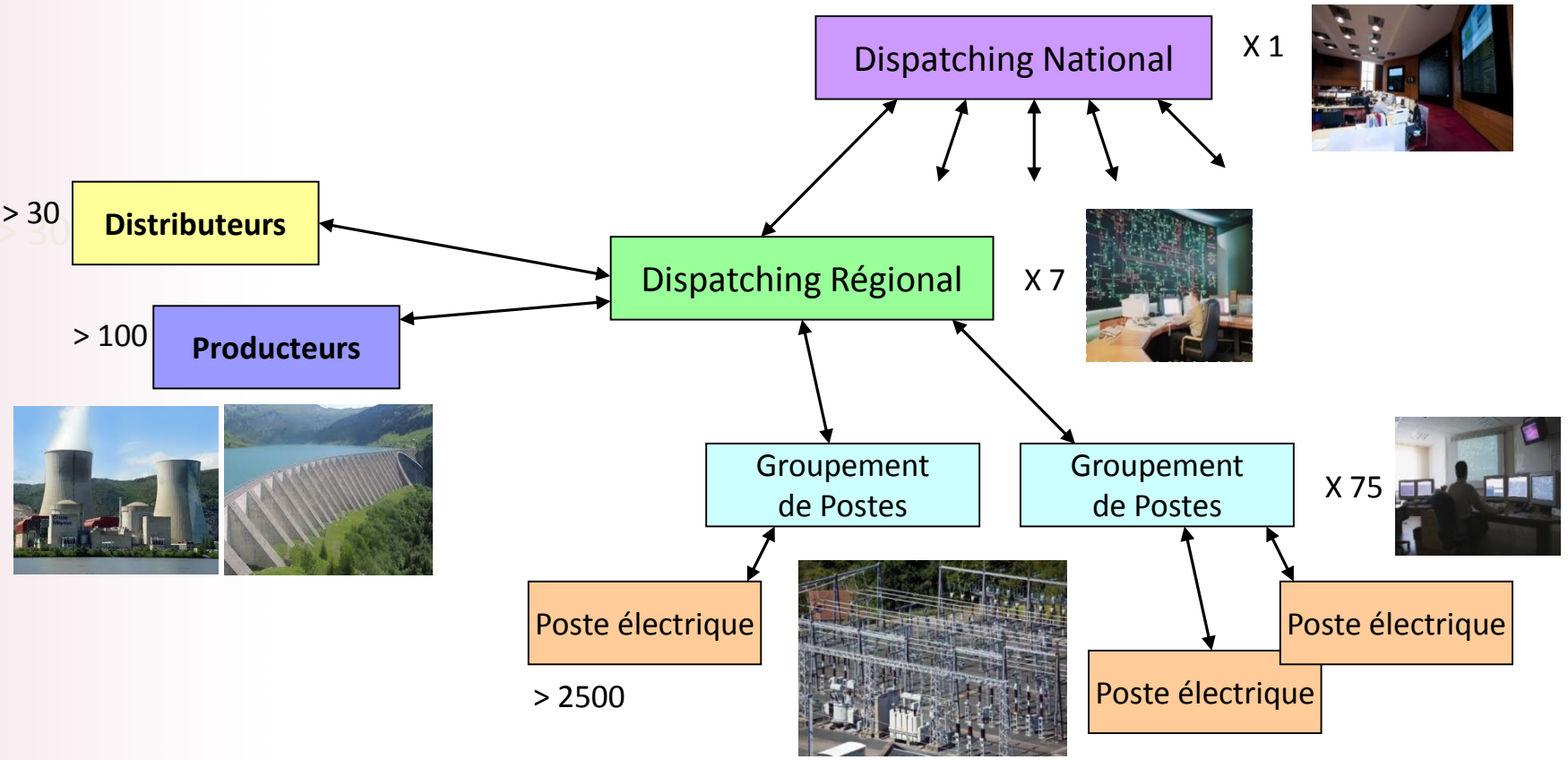


Des fournisseurs d'électricité en concurrence,

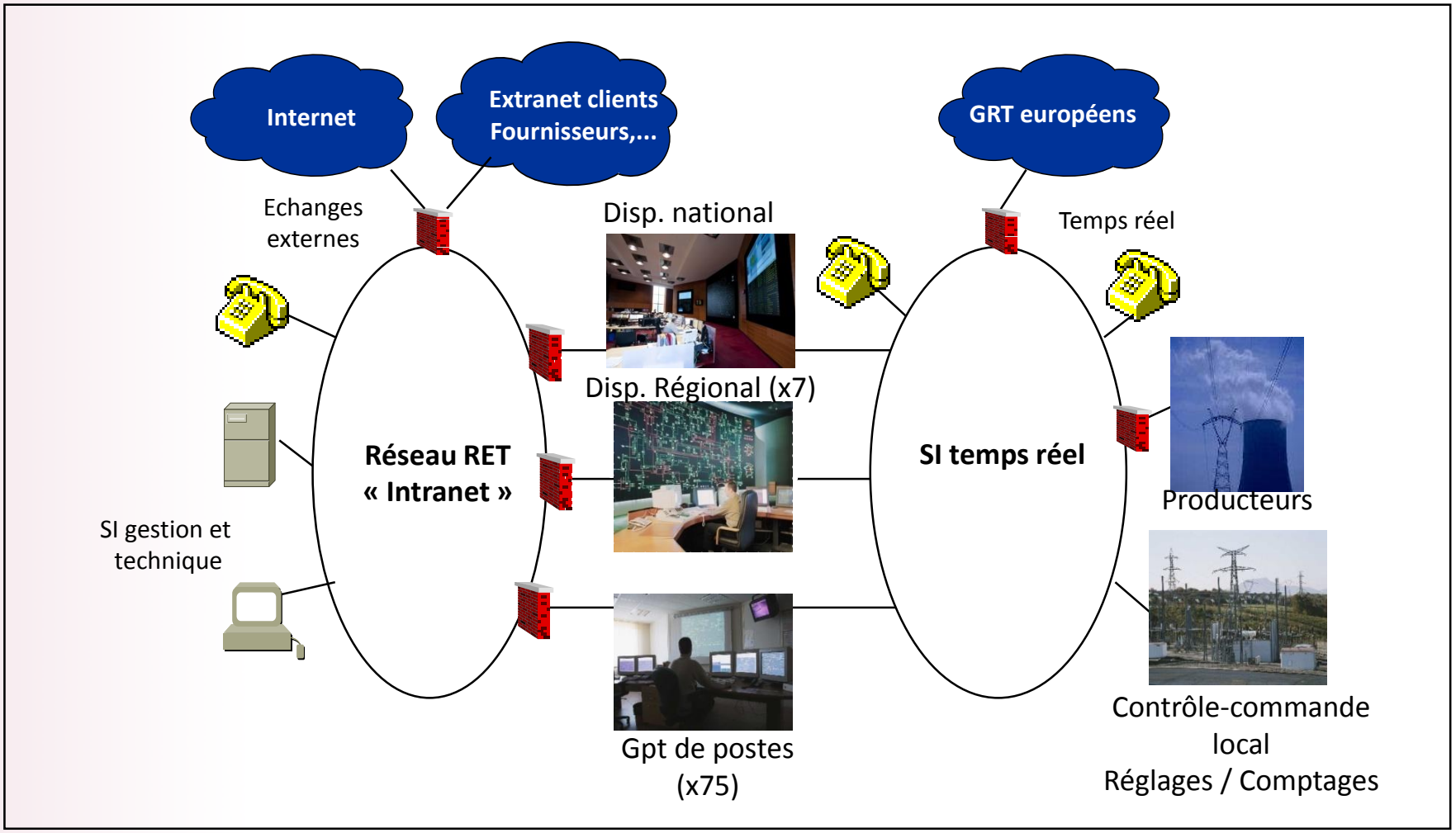
des consommateurs libres de choisir leur fournisseur

Organisation de la conduite du réseau

Une conduite du réseau organisée en quatre niveaux



Une architecture organisée autour d'un SI d'entreprise et d'un SI temps réel



Un contrôle commande (conduite, protection et reprise de service du poste) reposant sur plusieurs paliers technologiques…

Avant 1975 : palier Ariane pour tous les niveaux de tension lorsqu'il y avait peu de contraintes d'élimination des défauts
Technologie électromécanique à base de relais

1975 : palier Briseis pour les postes 400kV pour accueillir sur le réseau les centrales nucléaires
Technologie électronique

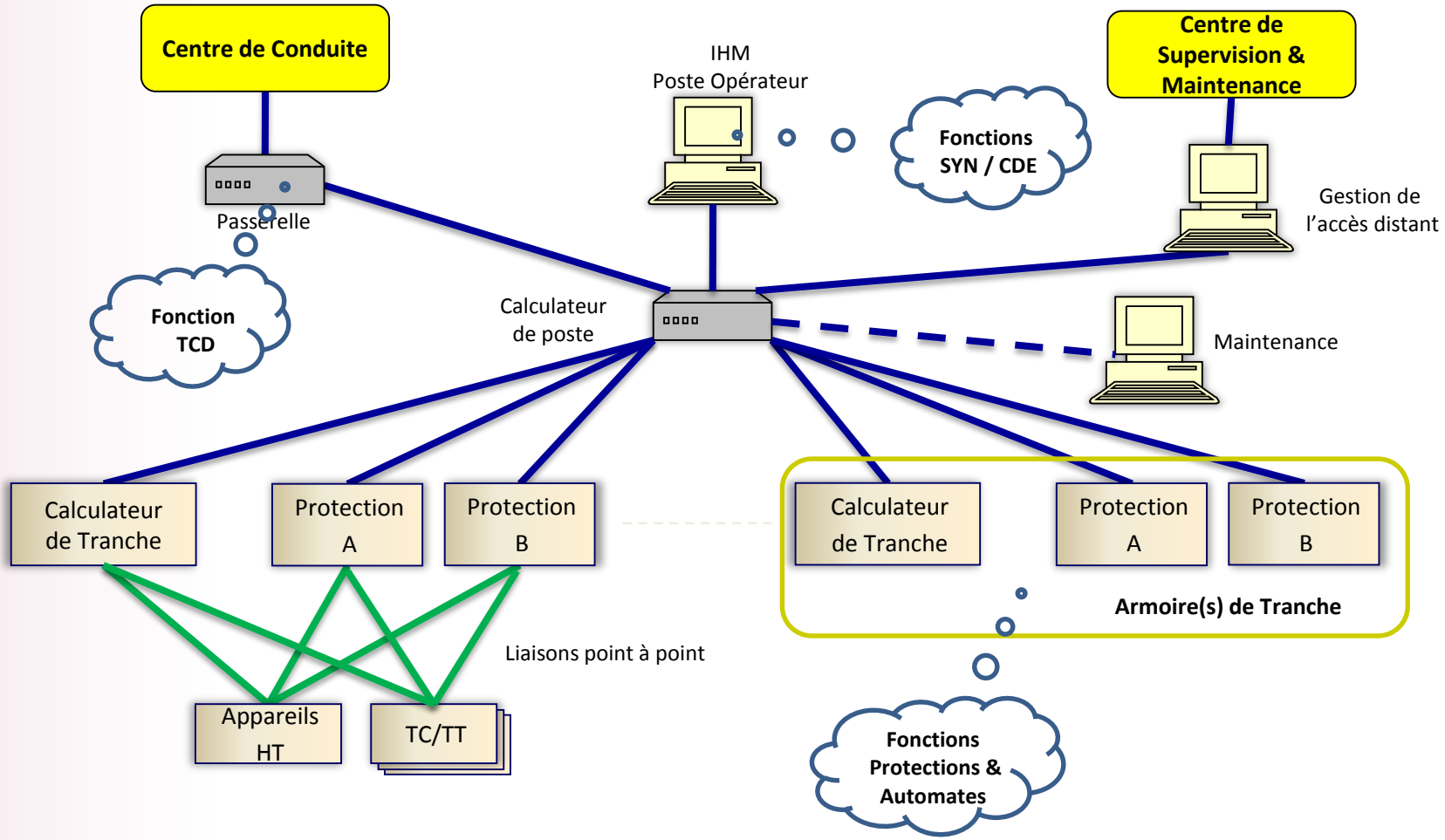
1983 : palier Cynthia pour les postes 225kV et HT afin de tenir compte des nouvelles contraintes des réseaux régionaux
Technologie électronique

… très peu sensibles aux attaques informatiques jusqu'au milieu des années 2000

1986 : palier Daphné pour tous les nouveaux postes:
Pas de changement technologique majeur

2006 : palier Electre destiné remplacer les paliers obsolètes (Briseis et Cynthia) introduisant des nouveaux *systèmes numériques* utilisant des composants matériels et logiciels sur étagère (OS Windows, Switch & routeur Ethernet,…)

Schéma de principe du contrôle-commande numérique



Une intégration de la sécurité informatique prise en compte par RTE au début des années 2000

- sur son SI d'entreprise avec notamment la diffusion d'antivirus sur ses postes de travail, la gestion de patchs sécurité et la surveillance des accès au SI

- sur son SI temps réel au moment du déploiement de SCADA au niveau des Groupements de poste, protégés des agressions par des coupe-feux gérés et supervisés par un centre opérationnel d'administration et de supervision de la sécurité mis en place en 2004

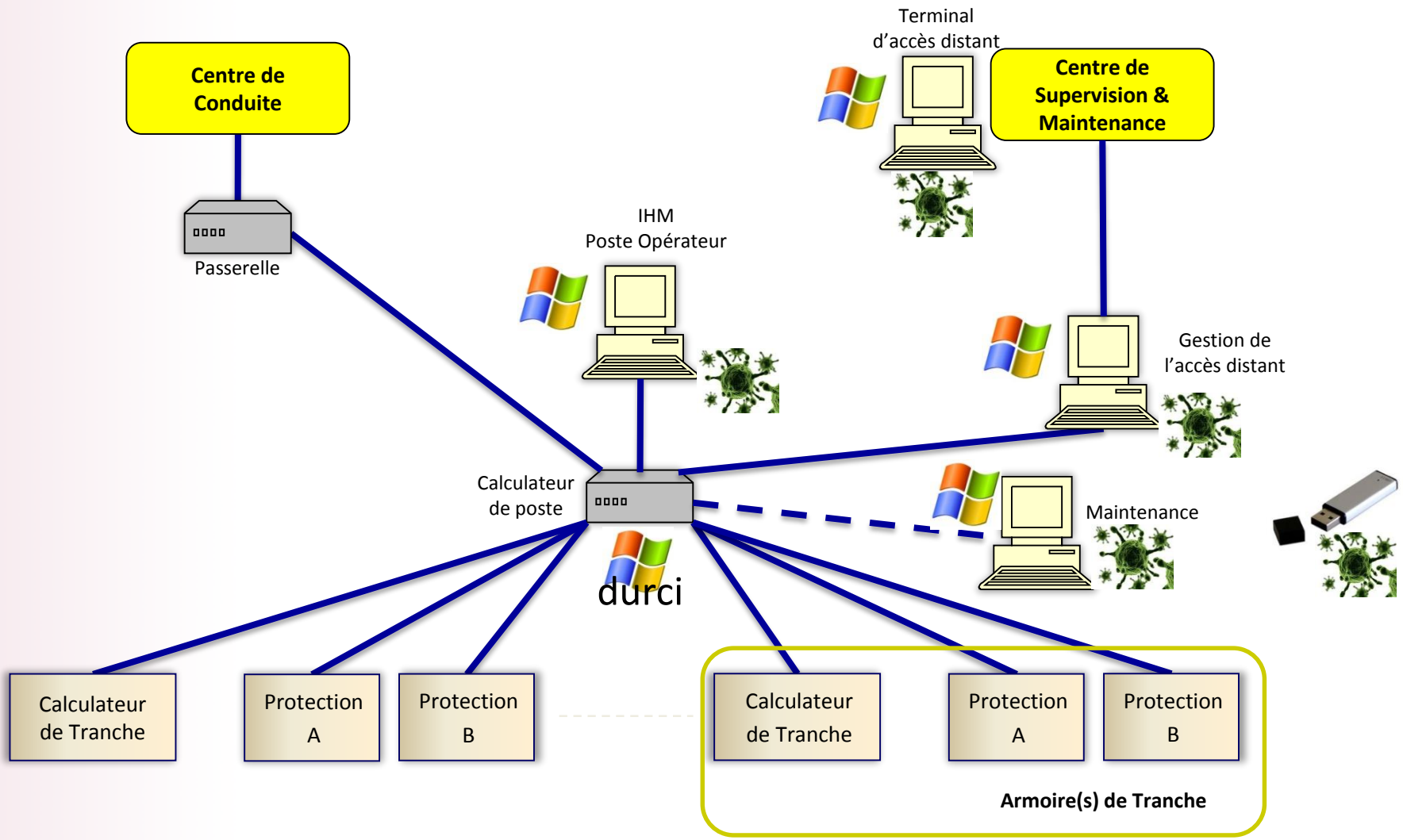
- pour le contrôle commande numérique des postes, le fait que ces systèmes aient été déployés sans lien direct avec l'externe et le SI d'entreprise nous laissait penser qu'ils étaient protégés des cyber-menaces, mais…

… à l'été 2010, l'alerte Stuxnet nous a montré que ce n'était pas le cas et que la cyber-protection de nos postes électriques ressemblait à…

30 juillet 2010: l'alerte Stuxnet

- 30/07/2010 : Siemens alerte RTE de l'infection de certains de ses SCADA d'un virus dangereux
- Aout 2010: Campagne de détection virale sur tous les contrôle-commande numériques de RTE
- Septembre 2010: Bilan de la campagne
  - ☺ Absence du virus Stuxnet
  - ☹ 20% des PC liés au contrôle-commande numérique sont infectés par d'autres virus, tous les constructeurs sont touchés
  - 😐 Ces virus étaient inoffensifs

Les machines Windows… et les virus



Les Actions correctives suite à Stuxnet

Automne 2010 : mise en place d'un référentiel sécurité SI Postes Electriques avec entre autres la mise en place d'antivirus là où c'est possible, mais de façon manuelle (une fois par mois, lors de déplacements sur les sites électriques)

2011 : mise en place de contrôles internes pour vérifier l'application du référentiel

2012 : actions de renforcement de la sécurité du SI industriel

- protections anti virales par liste blanche
- processus de veille sécurité du SI industriel pour alerter les équipes chargées du MCO en cas de publication de failles les concernant
- L'adjonction de coupe-feux à l'interface de nos partenaires et de règles de filtrages sur les routeurs du SI industriel

Les évolutions à venir

Pour le contrôle commande numérique des postes

Un plan d'action de sécurisation structurelle du prochain palier

- Dès la phase de conception :
  - point d'accès unique protégé,
  - Antivirus liste blanche,
  - Hardening
- … mais aussi en phase d'exploitation :
  - surveillance temps réel des équipements et réseaux
  - journalisation sécurisée des accès locaux et distants

Pour les télécommunications

Les profondes évolutions de télécommunications à venir à RTE

- font l'objet d'une étude sécurité approfondie
- la sécurité sera administrée et supervisée depuis un centre unique