Club de la sécurité de l'information français

Conférence CLUSIF

SI Industriels en 2017 :
Incidents, enjeux et… parades

Club de la sécurité de l'information français

CLUSIF

Concilier fiabilité et sécurité

Frédéric LENOIR
RTE

frederic.lenoir@rte-france.com

Direction des Systèmes d'Information et Télécommunications

Les SCADA sont vitaux pour le fonctionnement de certains services

Et pourtant, ils disposent de peu de mesures de cyber-protection

il est vrai que pendant des années ces systèmes étaient protégés car pas ou peu ciblés et difficiles à atteindre (château fort). Nouvelle situation et nouveaux impacts ; il est nécessaire d'intégrer les cyber risques sur la sûreté de fonctionnement.

SOMMAIRE

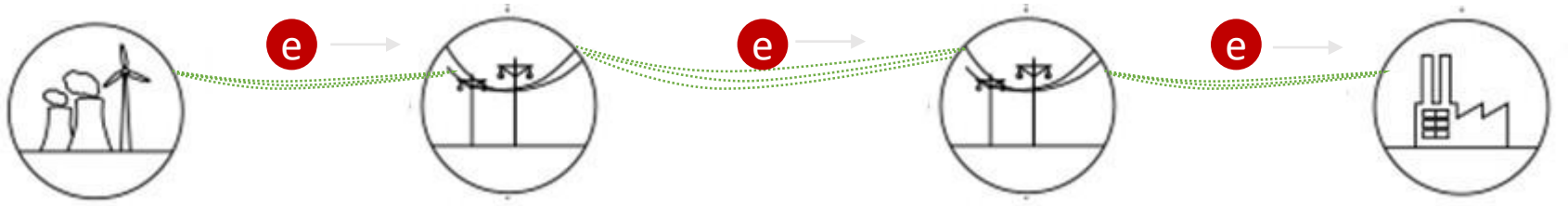
Préambule

Clés de lecture

8 500 salariés

54 Producteurs

260 Consommateurs industriels



P = C au meilleur coût

Part du transport dans la facture d'électricité = 8%

100 000 km de lignes ariennes + souterraines

Presque 3000 postes électriques (RTU)

22 000 km de Fibres Optiques

500 clients Distributeurs

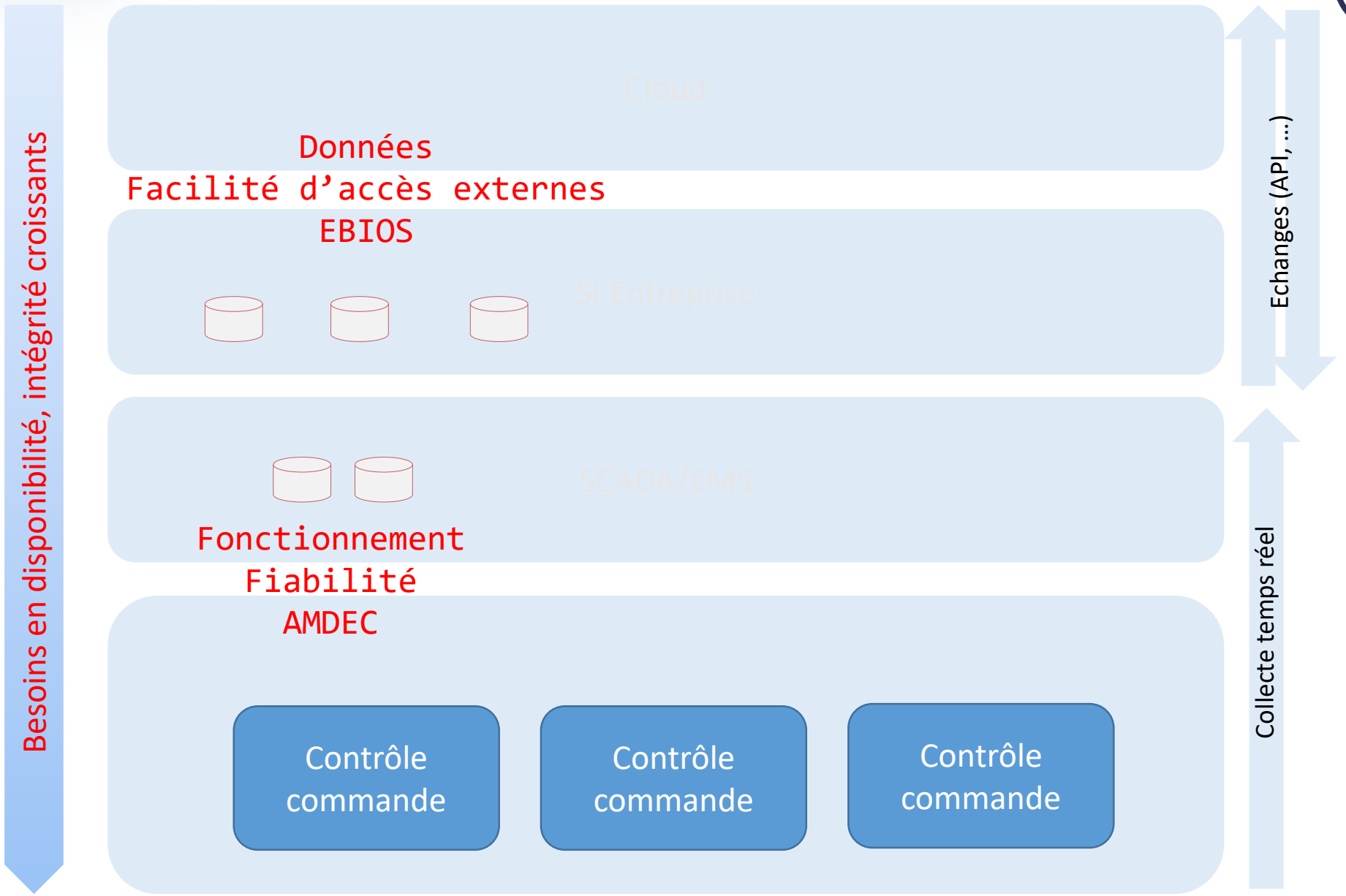
Les grands enjeux de l'Entreprise

- Sûreté de fonctionnement du Réseau Electrique
- Adapter le réseau aux enjeux de demain (énergies vertes, consommation au plus proche de la production…)
- Garantir des Mécanismes d'ajustement Equilibre Offre -Demande innovants

Les grands enjeux sur la Sécurité des SI

- Application de l'arrêté sectoriel du domaine « électricité » de la Loi de Programmation Militaire sur le Périmètre le plus sensible du SI (Systèmes SCADA et Contrôle Commande)
- Cyber Résilience (PRA/PCA)
- Intégrer les cyber-menaces dans les études de sûreté de fonctionnement
- Supervision de la sécurité
- Accès aux données clients (API) depuis l'externe

Objectifs de sécurité



Cas d'analyse de risques

nouvelles architectures SCADA
&
cyber-menaces en hausse
=
RISQUES A REVOIR

Pourquoi une telle étude ?

Trois grandes évolutions…

Centralisation du système SCADA de téléconduite

Évolution des réseaux TCM de Collecte

Environnement plus hostile cyber menaces

Ex : Coûts cyberattaques = 3*Coûts catastrophes naturelles

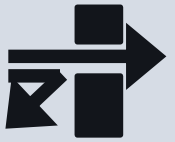
… amènent à re-questionner sur le niveau de risque SI et Télécom pour la téléconduite.

L'étude vise ainsi à :

- Proposer des **mesures** pour garantir a minima un **niveau constant de sûreté** de la téléconduite du réseau électrique
- Identifier les **nouveaux scénarios** (en particulier cyber) entraînant des **durées d'indisponibilité importantes** (supérieures à quelques heures et pouvant atteindre plusieurs semaines) qui ne sont pas pris en compte aujourd'hui

Comment l'augmentation de la cybermenace impacte-t-elle les analyses de sûreté de fonctionnement ?

Comparatif des caractéristiques d'une menace classique et d'une cyberattaque

	 Détection	 Réaction au PRA	 Impact pour l'entreprise
Menace classique (incendie, inondation, etc.)	immédiate et évidente	Une menace non évolutive	Impact pour l'entreprise prédictible à l'avance et lié à la menace
Cyberattaque	Temps de compréhension de l'attaque beaucoup plus long	Augmente la durée de remédiation Si attaque évoluée la menace peut être évolutive (s'adapte à la défense)	Des actions de défense pouvant temporairement augmenter l'impact pour l'entreprise *(isolation de parties du SI, certaines applications sont alors indisponibles)*

Méthodologie

Principe de la méthodologie d'analyse de risques retenue

Définition des scénarios de risques :

Bien support X **Événement redouté** X **Menace**

Identification des actifs impactés

Sélection des menaces EBIOS applicables au contexte

Exemple : Passerelles x Perte logique simultanée de toutes les passerelles de flux entrant des SCADA x Bug logiciel

Scénario de risques

Pour chaque scénario, définition de :

Vraisemblance

Évaluation de la probabilité de réalisation du risque

Impact / Niveau de gravité

Précision des conséquences pour la Téléconduite, évaluation du niveau de gravité dans le temps

Mesures de sécurité

Identification des mesures prévues par les projets et celles envisageables pour réduire le risque

Zoom sur la notion de vraisemblance

Plan de traitement des risques et des risques résiduels

Adapter les échelles de vraisemblance

Nécessité d'adapter les échelles de vraisemblance pour les aspects cyber attaques

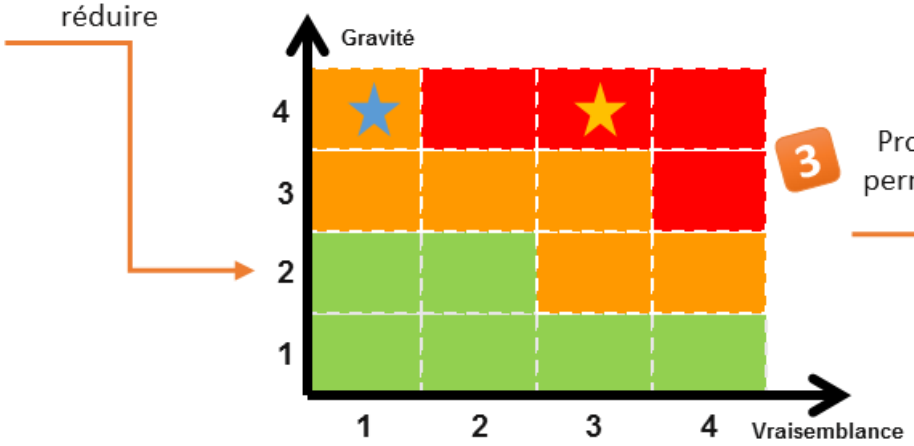
	1 – Très rare	2 – Rare	3 – Occasionnel	4 – Probable
Fréquence d'apparition du risque : événement pouvant arriver	Supérieur à 50 ans	Entre 10 et 50 ans	Entre 1 et 10 ans	Dans l'année
Difficulté de mise en œuvre pour les attaques Cyber	Nécessitant des ressources importantes et une expertise étatique	Nécessitant des ressources spécifiques et une expertise pointue	Nécessitant des ressources et une expertise avancée	Nécessitant des ressources standard et expertise faible

Méthodologie

AMDEC pas adapté aux cyber menaces

Pour chaque scénario de risques (croisement d'un bien support, d'une menace et d'un événement redouté)

1 Identification des mesures prévues dans le cadre des différents projets permettant de le réduire

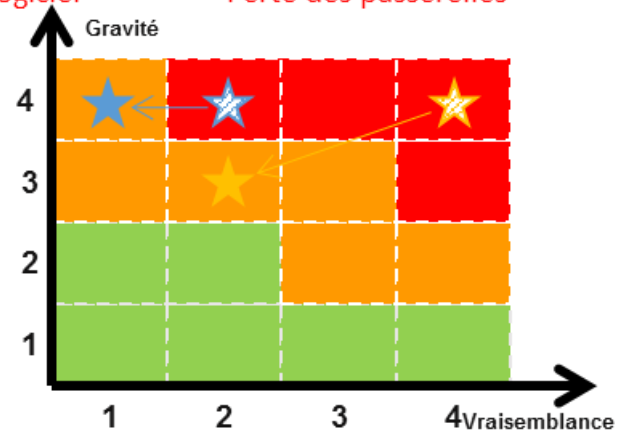


2 Positionnement du scénario de risque après application des mesures prévues

3 Proposition de mesures complémentaires permettant de diminuer le niveau du risque

Exemple 1 : Scada — Incendie — Perte d'une ZR

Exemple 2 : Passerelles 104 — Bug logiciel — Perte des passerelles



4 Positionnement du scénario de risque après application des mesures complémentaires à challenger

Conclusion

Les apports prévisibles de cette analyse de risques

La centralisation des fonctions sensibles accroît certains risques.

➔ pour un même événement, la gravité est plus forte pour un SI centralisé

la centralisation rend plus facile l'adoption de mesures de réduction des risques et en particulier le cloisonnement (administration centralisée) et la surveillance SSI

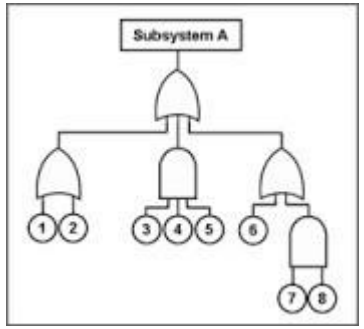
➔ plus aisé de détecter les attaques et de protéger un tel système, ce qui permet in fine de mieux maîtriser le niveau de risque.

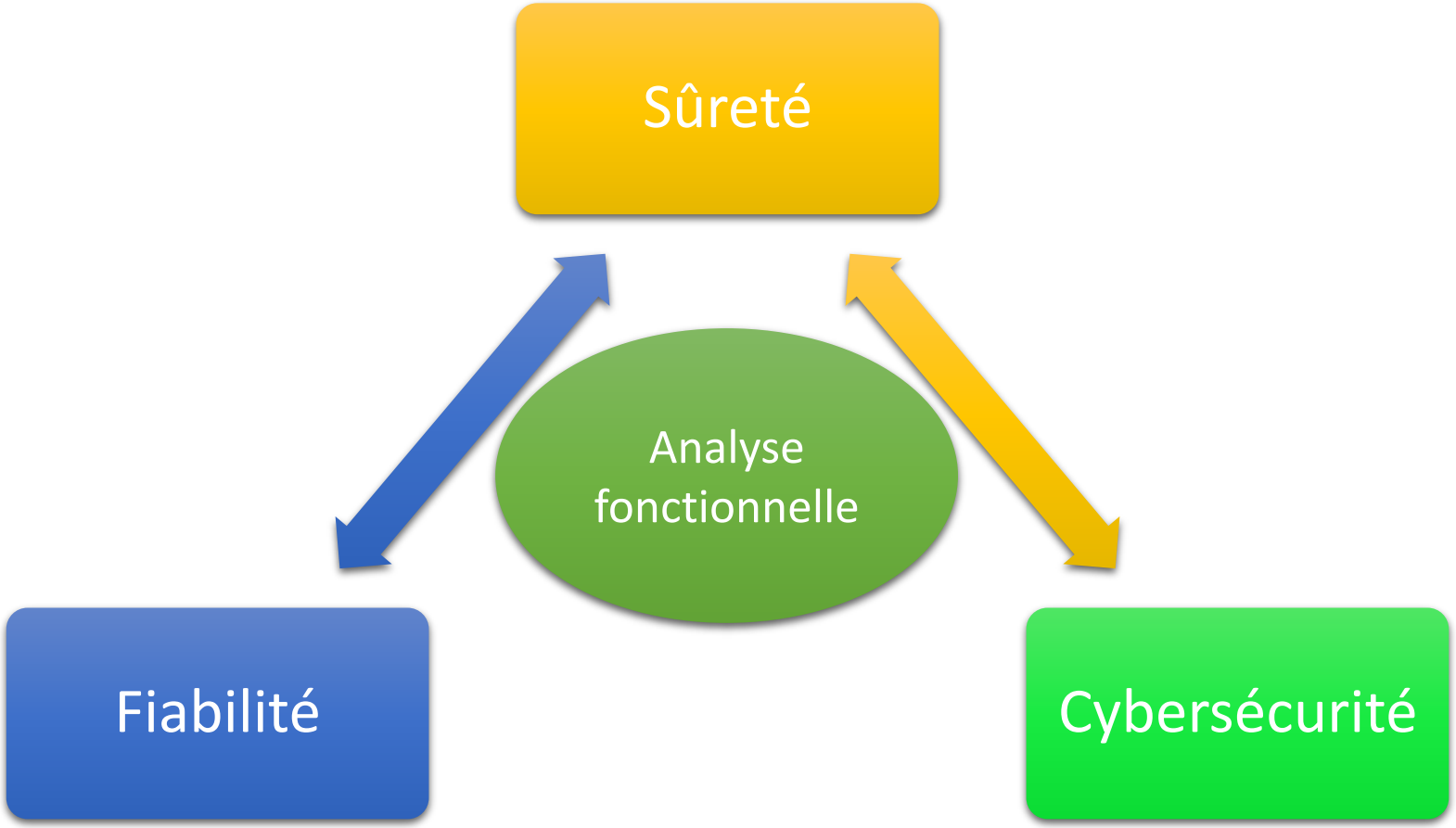
Les apports non soupçonnés « a priori » de cette analyse de risques

Plans de Continuité d'Activité non robustes à des indisponibilités liées aux cyber-attaques

Reconcevoir les PCA et intégrer cette dimension dans les futurs

Et s'il était possible de concilier sûreté et sécurité dans les analyses de risques !




Sûreté
Analyse fonctionnelle
Fiabilité
Cybersécurité

Merci pour votre écoute