Swiss Re

We're smarter together

Au delà des couvertures dommages
Zoom sur les expositions aux cyber-risques

Evénement éolien off-shore, Jimmy Keime, 5 Juin 2018

Sommaire

Pourquoi les parcs éoliens sont concernés par les risques cyber ?

Les parcs éoliens: des systèmes interconnectés

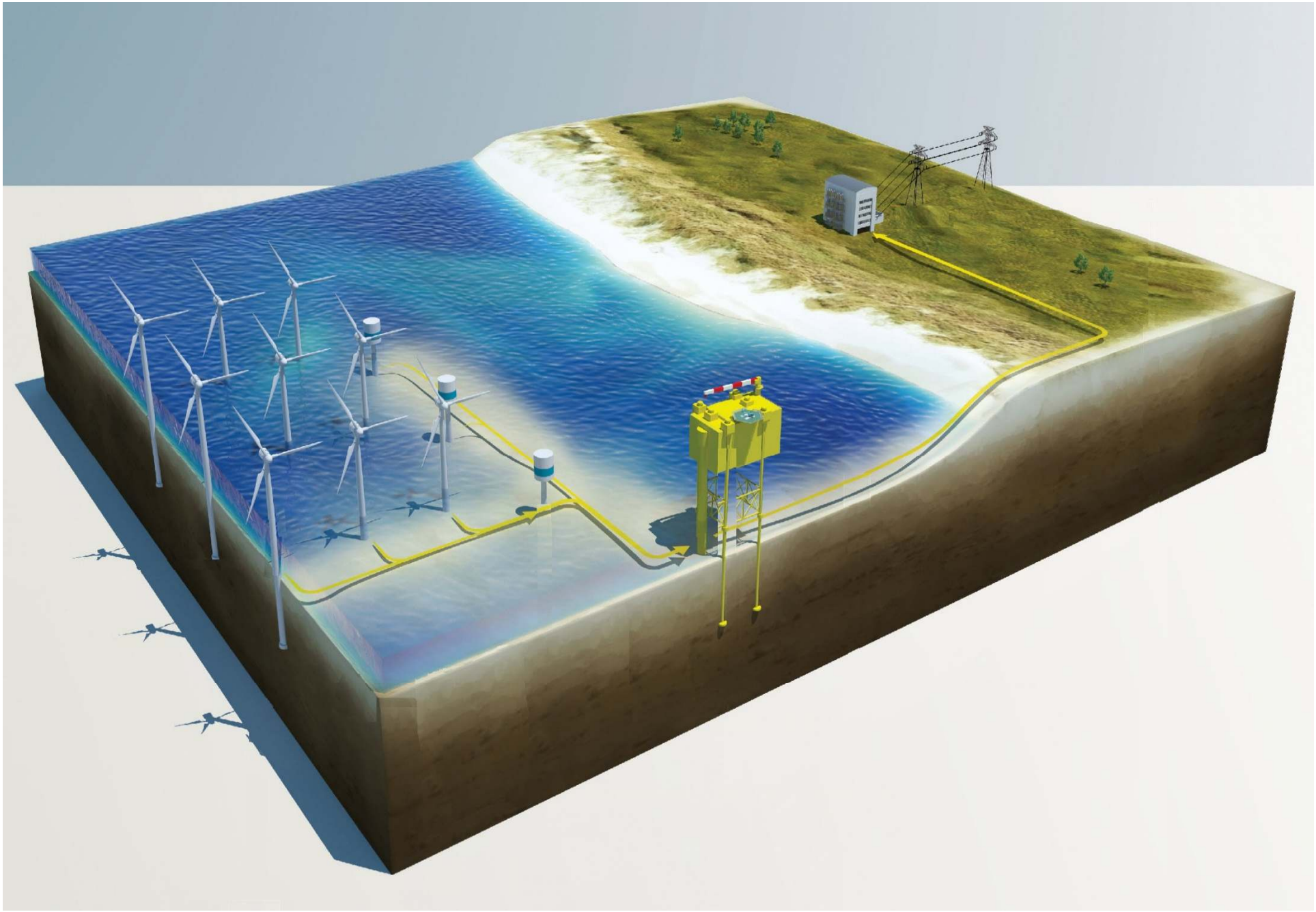
Les éoliennes contiennent de nombreux Industrial Control Systems (ICS) tels que:

- Capteurs
- Commandes

Ces systèmes sont supervisés par des systèmes SCADA (Supervisory Control and Data Acquisition). Ils connectent :

- Les différents ICS pour permettre le contrôle et la supervision d'une éolienne
- Toutes les éoliennes d'un même parc
- La sous-station
- La station météo

Swiss Re



Les éoliennes : des points d'entrés physiques pour des attaques ciblées

- La distribution spatiale des éoliennes rend leur protection plus difficile
- La manière la plus efficace nécessite :
  - Un accès physique à une éolienne
  - Un boitier programmable < 50€
- Pour les parcs les moins protégés, il est très facile de prendre les commandes de toutes les éoliennes présentes sur le même réseau. Il a été démontré les attaques suivantes :
  - Envoi de commandes pour endommager ou stopper les éoliennes
  - Attaques du type « man in the middle » pour intercepter les commandes envoyées par le centre de contrôle

Les SCADA : des centres nerveux connectés

- Les SCADA connectent un ou plusieurs parcs éoliens dans une salle de contrôle et/ou sur internet pour les installations de petites tailles
- Systèmes SCADA connectés et mal protégés = Danger. Exemples :
  - XZERES 442SR : problème de design du serveur permet à un hacker de changer le mot de passe administrateur
  - RLE Nova : mot de passe stocké dans un fichier texte accessible

Quelles peuvent être les conséquences d’attaques cyber sur les parcs éoliens ?

Des conséquences désastreuses

Les 2 principals motivations

Financier

- Extorsion, rançon

Destruction

- Neutraliser, endommager

Des consequences importantes

- Perte d'exploitation
- Perte de données
- Dommage matériel
- Dommage corporel
- Dommage de réputation
- Coûts de notification
- Possibles amendes, sanctions, pénalités
- Extorsion, rançon
- Vol de propriété intellectuelle
- Coûts d'investigations

Les polices TRME et BDM/Dommages couvrent-elles ces risques ?

Des clauses de marché existent...

La majorité des polices TRME, BdM/Dommages contiennent des exclusions marché visant à exclure les risques Cyber

- Institute Cyber Attack Exclusion Clause (CL 380), 10/11/2003
  *Exclut tous préjudices, responsabilité civile ou frais occasionnés, induits ou engendrés directement ou indirectement par l'utilisation ou l'exploitation, **aux fins de causer un préjudice**, d'un ordinateur, système informatique, logiciel, code malveillant, virus ou traitement informatique ou autre système électronique.*
- Electronic Data Clause (NMA 2914 - 2915), 25/01/2001
  Exclut les coûts, les frais de réparation / remplacement, ainsi que les dommages physiques résultant de données ou logiciels perdus / endommagés.
  Couvre les dommages physiques causés par un incendie / une explosion, lorsque l'incendie / l'explosion résulte de données ou de logiciels perdus / endommagés.
- Cyber Non-Aggregation Clause (NMA 2912) / IT Hazards Exclusion Clause (NMA 2928)
  Similaire à NMA 2914-2915, mais avec rachat de l'exclusion Cyber si dommages causés par FLEXA ou des périls naturels.

… mais n'ont pas été testées

- Les clauses sont complexes
- Elles n'ont encore pas été contestées devant un tribunal
- Par exemple :
  - CL380: « aux fins de causer un préjudice » devrait être prouvé

→ Nous devons partir du principe que le Cyber est actuellement couvert

- Une clause d'exclusion spécifique est en cours de rédaction par l'IMIA (International Association of Engineering Insurers) pour palier à ces problèmes « Advanced Cyber Exclusion Clause »
- Devrions nous également proposer une couverture spécifique Cyber ?

Une couverture Cyber sous certaines conditions

Respect des Best Practices existantes, par exemple :

- **ABS** : Cyber Security Implementation for the Marine and Offshore Industries une norme pour la gestion de la cyber sécurité pour les actifs offshore, y compris les exigences pour une certification

Appendix

Institute Cyber Attack Exclusion Clause CL 380, 10/11/2003 - Traduction

1. Sous réserve du paragraphe 2 ci-après, la présente police ne couvre en aucun cas les préjudices, responsabilité civile ou frais occasionnés, induits ou engendrés directement ou indirectement par l'utilisation ou l'exploitation, aux fins de causer un préjudice, d'un ordinateur, système informatique, logiciel, code malveillant, virus ou traitement informatique ou autre système électronique.
2. Si la présente clause est garantie par une police couvrant les risques de guerre, guerre civile, révolution, rébellion, insurrection ou conflit civil en résultant, ou tout acte hostile commis par ou contre une puissance belligérante ou tout acte de terrorisme ou à caractère politique, le paragraphe 1 ne permet pas d'exclure les préjudices (qui sans cela seraient couverts) découlant de l'utilisation d'un ordinateur, système informatique ou logiciel ou tout autre système électronique pour le système de lancement et/ou de guidage et/ou le dispositif de mise à feu de toute arme ou de tout missile.

Prepared by

Jimmy Keime
Senior Engineering Underwriter
Jimmy_Keime@swissre.com

www.swissre.com

We’re smarter together

Swiss Re

Legal notice

The information and opinions contained in the presentation are provided as at the date of the presentation and are subject to change without notice. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the details given. All liability for the accuracy and completeness thereof or for any damage or loss resulting from the use of the information contained in this presentation is expressly excluded. Under no circumstances shall Swiss Re or its Group companies be liable for any financial or consequential loss relating to this presentation.