



Cybersécurité pour vos éoliennes

Continuité opérationnelle dans un monde de l'énergie connecté

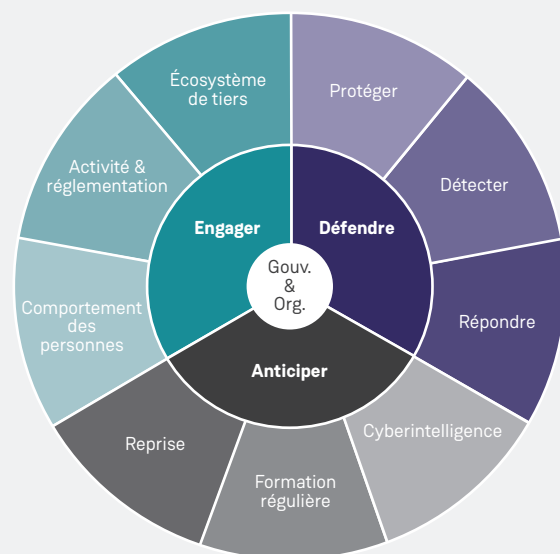
Le secteur de l'énergie est confronté à une nouvelle réalité. À mesure que les systèmes énergétiques deviennent plus connectés, la technologie opérationnelle est de plus en plus ciblée par des cyberattaques.

Les adversaires ne se contentent plus d'obtenir un accès — ils étudient les systèmes de contrôle industriel, cartographiant les boucles de contrôle et les postes de travail d'ingénierie afin de comprendre les processus physiques et de créer, avec précision, des perturbations opérationnelles potentielles. Les accès distants exposés, les identifiants faibles et la visibilité limitée augmentent les risques, faisant de la cybersécurité un élément central des opérations énergétiques résilientes.

Aujourd'hui, la combinaison de la pression réglementaire, de l'augmentation de la connectivité OT et des incidents récents dans l'ensemble du secteur de l'énergie signifie que la fenêtre pour réagir tardivement est en train de se refermer. La cybersécurité est devenue une exigence stratégique pour la continuité opérationnelle — c'est pourquoi agir dès maintenant est essentiel.

Pour les opérateurs énergétiques, la cybersécurité n'est plus seulement une préoccupation informatique — c'est un élément clé de la résilience opérationnelle. Des approches structurées combinant sensibilisation, architecture sécurisée, surveillance continue et planification de la reprise permettent de réduire les risques, de maintenir la continuité et de protéger la valeur des actifs critiques.

La cybersécurité comme un cycle de vie continu pour des opérations sûres et résilientes





Ne pas prendre de décision est, en soi, une décision

De récents incidents dans le secteur de l'énergie ont montré que les opérations cyber ne visent pas toujours une perturbation immédiate. Dans plusieurs cas, les systèmes ont continué à produire de l'énergie tandis que le contrôle, la visibilité ou la coordination étaient délibérément affectés.

De telles actions démontrent que l'activité cyber moderne peut façonner les conditions opérationnelles sans déclencher de conséquences immédiates. L'absence de perturbation ne doit pas être confondue avec l'absence de risque. Cela met en évidence la manière dont les systèmes interconnectés peuvent être influencés, testés ou préparés à différents scénarios au fil du temps. Dans ce contexte, la cybersécurité ne consiste pas à prédire la prochaine étape, mais à garantir que les systèmes soient conçus de manière qu'aucune étape — intentionnelle ou accidentelle — ne puisse dégénérer en un impact incontrôlé.

Ce changement nécessite une approche plus proactive et structurée, reliant la sécurité aux décisions opérationnelles et à la planification à long terme.

“La clarté des responsabilités compte davantage que la rapidité.”

“Nos systèmes n'ont pas été conçus pour la cybersécurité — nous avons besoin de clarté sur les implications avant d'agir.”

“Le risque est clair ; le défi consiste à décider quand agir sans limiter les options.”

Pourquoi les parcs éoliens sont vulnérables

Les installations éoliennes sont des infrastructures numériques : les éoliennes, les sous-stations et les systèmes de contrôle fonctionnent au sein d'un réseau numérique continu qui permet la surveillance et le contrôle à distance. La connectivité permet des gains d'efficacité — et introduit des risques cyber.

Les principaux points d'entrée cyber dans l'éolien sont :

- Réseaux SCADA.
- Accès à distance.
- Contrôleurs d'éoliennes (PLC).
- Systèmes informatiques d'entreprise (IT).
- Plateformes de supervision/cloud.
- Logiciels de la chaîne d'approvisionnement.
- Capteurs IoT et dispositifs en périphérie (edge devices).
- Interfaces de communication avec le réseau électrique.

La gestion efficace de ces risques nécessite non seulement d'identifier les points d'entrée, mais aussi de comprendre comment ils sont utilisés et exploités dans les conditions réelles d'un parc éolien. Cela implique de savoir qui se connecte, quand les accès ont lieu et comment des modifications dans un système peuvent affecter l'ensemble de l'environnement opérationnel.

Pourquoi l'expertise OEM est essentielle pour gouverner la collaboration avec des tiers en OT

La gouvernance des accès tiers dans les environnements OT exige une connaissance approfondie du fonctionnement réel d'un parc éolien, et pas seulement de son fonctionnement théorique.

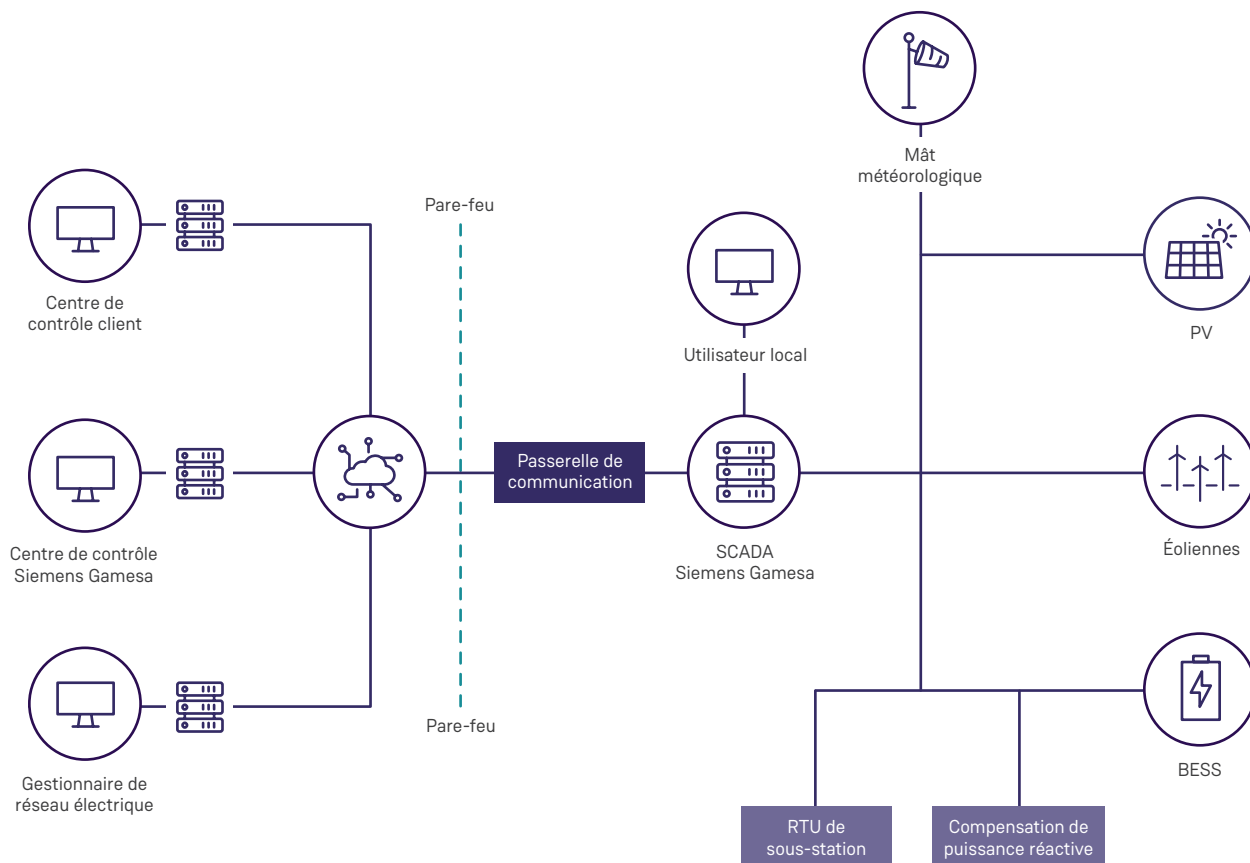
C'est là qu'un OEM apporte une valeur réelle :

- Nous comprenons comment les systèmes sont réellement accessibles et comment les composants dépendent les uns des autres.
 - Nous anticipons les risques opérationnels liés aux changements dans des environnements OT en production.
 - We structure third-party access with clear roles, controlled
- Nous anticipons les risques opérationnels liés aux changements dans des environnements OT en production.

Il ne s'agit pas d'auditer les tiers — il s'agit d'opérations pratiques et maîtrisées, fondées sur une connaissance réelle des systèmes.

Les adversaires ne s'appuient pas sur des techniques avancées ; ils exploitent les raccourcis opérationnels du quotidien





L'Approche Siemens Gamesa Cyber Maturity-by-Design

Chez Siemens Gamesa, les opérations sécurisées et les exigences réglementaires sont intégrées dès la conception, permettant une prise de décision claire et en toute confiance dans la durée. La cybersécurité est traitée comme un système intégré plutôt que comme un ensemble de contrôles isolés.

Cette approche garantit que des pratiques sûres, résilientes et permettant la reprise après sinistre s'instaurent naturellement — grâce à des contrôles intégrés, des rôles clairement définis, des procédures validées et une véritable harmonisation opérationnelle.

Cyber Maturity-by-Design est structuré autour du parcours client : chaque exploitant démarre à un niveau de maturité différent, et les quatre piliers guident l'évolution — étape par étape, au bon rythme, sans perturber les opérations.

Nos systèmes n'ont pas été conçus pour la cybersécurité — nos décisions doivent l'être

Cyber Maturity-by-Design garantit que les actifs éoliens soient :



Notre portefeuille organise les capacités nécessaires à des opérations éoliennes sûres et résilientes autour de quatre piliers, afin d'assurer une protection complète des actifs éoliens :

Awareness-by-Design

La sensibilisation intégrée à la cybersécurité réduit le risque humain en rendant les comportements sécurisés automatiques, intégrés aux opérations et alignés sur la gouvernance Siemens Gamesa ainsi que sur les normes ISO 27001.

Capacités activées :

- Évaluation de la cybersécurité.
- Gestion des actifs.
- Reporting des vulnérabilités.

Aide les opérateurs à comprendre l'éventail de risques et à prendre des décisions éclairées.

Secure-by-Design

Minimise le risque d'attaque grâce à une architecture intégrée, à la sécurité sur l'ensemble du cycle de vie et à la conformité aux normes.

Capacités activées :

- IAM (Identity Access Management).
- RIA (Remote Interactive Access).
- SRA (Secure Remote Access).
- Journalisation.
- Sécurité réseau (pare-feu, segmentation).
- Sauvegarde.

Empêche les accès non maîtrisés, limite la propagation des attaques et protège les actifs critiques.

Resilience-by-Design

Garantit la continuité des opérations pendant les incidents en minimisant l'impact et en assurant la continuité de la production.

Capacités activées :

- Sécurité réseau (surveillance et confinement).
- AEPP (Advanced Endpoint Protection).
- Gestion des vulnérabilités et des correctifs.

Détecte et contient les menaces précocement et empêche la propagation des logiciels malveillants entre les éoliennes.

Recovery-by-Design

Garantit une reprise rapide et fiable des opérations. Grâce à des mécanismes de reprise testés, des sauvegardes immuables et des plans répétés, les temps d'arrêt deviennent prévisibles, maîtrisés et sans stress — sans improvisation, sans incertitude.

Capacités activées :

- Sauvegarde et restauration.
- Reprise après sinistre.

Assure la restauration rapide des systèmes critiques et minimise l'impact opérationnel.

Certaines capacités peuvent nécessiter des mises à jour des systèmes dans le cadre d'une évolution planifiée. La disponibilité des capacités dépend de la plateforme et de la configuration existantes. Nous pouvons nous adapter à l'environnement de nos clients.

Pourquoi Siemens Gamesa

Chez Siemens Gamesa, la cybersécurité fait partie intégrante de la fiabilité et de la résilience de vos opérations éoliennes. Nous combinons une expertise OT approfondie avec une vision stratégique de la sécurité afin de protéger vos actifs tout au long de leur cycle de vie.

La fiabilité opérationnelle alliée à l'expertise cyber

Nous comprenons comment les cybermenaces affectent la performance, la disponibilité et la sécurité. Notre double expérience dans la technologie éolienne et la cybersécurité garantit une protection qui permet à vos opérations de fonctionner de manière fluide et sécurisée.

La cybersécurité est un parcours. Nous apportons de la clarté, une expertise OT et des capacités évolutives pour protéger vos actifs et vos opérations

Des opérations éoliennes sûres et résilientes



Une approche consultative, centrée sur le client

Chaque parcours client est différent. Siemens Gamesa apporte de la clarté, de la priorisation et un accompagnement adapté à votre environnement — vous aidant à identifier les risques, définir les priorités et élaborer la stratégie de cybersécurité appropriée.



Un accompagnement de votre parcours de maturité cyber

De l'évaluation initiale aux capacités avancées, Siemens Gamesa soutient chaque étape de votre parcours de maturité, en vous aidant à construire, renforcer et maintenir une posture de cybersécurité adaptée à votre organisation.



La conformité intégrée à chaque étape

Face à l'évolution des réglementations telles que NIS2, IEC 62443 ou les normes ISO, Siemens Gamesa intègre les exigences de conformité depuis la conception des systèmes jusqu'à l'exploitation à long terme — en mettant l'accent sur le secure-by-design, une gouvernance continue et une adaptabilité durable.



Un partenariat sur l'ensemble du cycle de vie

La cybersécurité est un effort continu. Siemens Gamesa fournit des conseils, du support et une surveillance tout au long de la durée de vie de vos actifs, vous aidant à rester résilient face à l'évolution des menaces, des technologies et des exigences réglementaires, tout en gardant le contrôle de chaque décision.



Espagne

P. Tecnológico de Bizkaia, edif. 222
48170 Zamudio, Biscaye

Calle Ramírez de Arellano, 37
28043 Madrid

Avda. Ciudad de la Innovación, 9-11
31621 Sarriñena, Navarre

Afrique du Sud

Maxwell Office Park
Office 1, Ground Floor, Building 3
37 Magwa Crescent
Waterfall City 2090

Chine

Siemens Center Beijing, 3rd Floor
No.7 South Wangjing Zhonghuan
Road, Chaoyang District
Pékin 100102

Grèce

75 Katechaki Avenue, 4th floor
115 25, Athens

Pays-Bas

Lange Kleiweg 40
2288 GK
Rijswijk

Allemagne

Beim Strohhaus 17-31
20097 Hambourg

500, Da Lian Road
Yangpu District
200082 Shanghai

Inde

No. 489, GNT Road
Thandalkazhani Village
Vadagarai PO, Redhills
Chennai 600052

Pologne

Aleja Armii Ludowej street 26
00-609 Varsovie

Mary-Somerville-Straße 14
28359 Bremen

Corée du Sud

8F, Gwanghwamoon D tower 17,
Jongno 3-gil Jongno-gu
Seoul

Irlande

Innovation House, DCU Alpha
Old Finglas Road 11
Glasnevin, Dublin 11

Royaume-Uni

Arena Business Centre
Watchmoor Park
Riverside Way
Camberley
GU15 3YL

Australie

Level 3, Botanicca 3
570 Swan Street
Burnley
Melbourne, 3121

Croatie

Slavonska avenija 1a
(zgrada/building C, 1st floor)
HR-10000 Zagreb

Italie

Centro Direzionale Argonauta
Via Ostiense 131/L
Corpo C1 9° piano
00154 Rome

Serbie

Tadije Sodermajera 11
(zgrada/building AFI, 8th floor)
11070 Novi Beograd
Beograd

Autriche

Siemens Energy Austria GmbH
Wind Power
Siemensstrasse 90
Vienna 1210

Danemark

Borupvej 16
7330 Brande

Via Privata Vipiteno 4
20128 Milan

Singapour

60 MacPherson Road
Singapore
348615

Brésil

Avenida Engenheiro João
Fernandes Gimenes Molina
n° 1745, Edifício 9, 1° andar
Bairro Distrito Industrial
CEP 13213-080
Jundiaí - SP

Egypte

Bureau 58 - Sector4
Business Park
90th South Road
Fifth Settlement
New Cairo - Cairo

Japon

14F Tokyo Shiodome Building
1-9-1, Higashi Shimbashi
Minato-ku, Tokyo

Suède

Evenemangsgatan 21
169 79 Solna

Canada

1577 North Service Road East
Oakville
Ontario
L6H 0H6

Etats-Unis

4400 N. Alafaya Trail
Orlando, FL 32826

Maroc

Anfa Place Blvd. de la Corniche
Centre d'Affaires "Est", RDC
20200 Casablanca

Thaïlande

Charn Issara Tower II
33rd Floor
2922/320-323
New Petchburi Road,
Bangkapi, Huaykwang,
Bangkok 10310

Finlande

Tarvonsalmenkatu 19
FI-02600 Espoo

Mexique

Paseo de la Reforma 505
Torre Mayor, 37th Floor
Col. Cuauhtémoc
Del. Cuauhtémoc
06500 Mexico

Vietnam

15th Floor, Deutsches Haus
33 Le Duan Blvd.
Sai Gon Ward
Ho Chi Minh City 71000

Chili

Edificio Territoria El Bosque
Avenida Apoquindo 2827
Piso 19 Las Condes
Santiago de Chile

France

Immeuble le Colisée
Bâtiment A - 2ème étage
10 avenue de l'Arche
92419 Courbevoie

Norvège

Norbygata 14
NO-0187 Oslo

Le présent document, son contenu, ses annexes et/ou amendements ont été rédigés par Siemens Gamesa Renewable Energy, S.A.U. à titre d'information uniquement et pourraient être modifiés sans préavis. L'information qui y figure ne contient que des descriptions générales et/ou des caractéristiques de performance qui pourraient ne pas correspondre aux caractéristiques décrites ou qui pourraient subir des modifications lors du développement futur des produits. Les caractéristiques de performance demandées ont des effets contraignants seulement si elles ont été expressément convenues dans le contrat en vigueur. Tout le contenu du document est protégé par les droits de propriété intellectuelle et industrielle qui appartiennent à Siemens Gamesa Renewable Energy, S.A.U. Le destinataire ne doit pas reproduire, ni totalement ni partiellement, aucune information. Siemens Gamesa est une marque utilisée sous licence de Siemens AG.

08/2026

comercial_consultas@siemensgamesa.com
www.siemensgamesa.com