Institut national de test pour la cybersécurité

Cybersécurité des installations photovoltaïques

Enseignements et recommandations

Version	1.0
Date	17 septembre 2026
Classification	Public

Auteurs	Tobias Castagna, Stefan Gloor, Andreas Leisibach, Dilip Many, Raphael M. Reischuk, Lukas Sohrmann, Fabio Zuber
Responsable	Tobias Castagna

Avec le soutien de suisseénergie

Table des matières

Remerciements

Un merci particulier va aux organisations et aux experts qui ont soutenu cette étude, que ce soit par la mise à disposition d'appareils de test, par un aperçu de l'utilisation de tels appareils dans différents environnements ou par une participation aux coûts. Par leur engagement, ils ont contribué de manière déterminante à la réussite de cette analyse de sécurité. En font partie:

• SuisseEnergie, Office fédéral de l'énergie OFEN
• Commission fédérale de l'électricité ElCom
• Office fédéral de la communication OFCOM
• Office fédéral de la cybersécurité OFCS
• Association des entreprises électriques suisses (AES)
• Aziende Industriali di Lugano (AIL) SA
• ch-solar AG
• Flughafen Zürich AG
• HHM Gruppe (HEFTI. HESS. MARTIGNONI.)
• Stadt Zürich Organisation und Informatik (OIZ)
• Swisscom (Suisse) SA
• Swissgrid SA
• Swissolar

• Prof. Dr. Christof Bucher, Haute école spécialisée bernoise BFH
• Prof. Roger Buser, Hochschule Luzern HSLU
• Prof. Dr. Andreas Heinzelmann, ZHAW Zürcher Hochschule für Angewandte Wissenschaften
• Ruben Santamarta, chercheur indépendant en cybersécurité
• Dr. Leonard Schliesser, Center for Security Studies CSS, ETH Zurich
• Arrigo Triulzi Lampugnani, expert indépendant en cybersécurité
• Bastian Widmer, expert indépendant en cybersécurité

Un merci tout particulier va à Robin Seidel, qui a identifié, dans le cadre de ses études à l'EPF de Zurich et en coopération avec le NTC, des vulnérabilités graves dans un appareil connecté d'une installation photovoltaïque. Ce travail préalable a conforté le NTC dans la nécessité d'agir et a donné des impulsions essentielles à la présente analyse.

1 Management Summary

L'essentiel en bref

Le photovoltaïque est d'importance systémique: fin 2025, la Suisse comptait environ 338 000 installations photovoltaïques raccordées au réseau. Leur production annuelle couvrait 13,7% de la consommation finale d'électricité. Par temps ensoleillé, à la mi-journée, les installations couvrent régulièrement plus de la moitié de la consommation instantanée.

L'étude: l'Institut national de test pour la cybersécurité NTC a testé, de sa propre initiative, sept onduleurs et quatre systèmes de gestion de l'énergie. Le NTC a été soutenu dans cette démarche par des organisations de la branche et par SuisseEnergie.

Plus de 50 constats dans onze produits: sept constats sont critiques, six élevés. Cinq produits présentaient au moins un constat critique ou élevé. Le NTC a pu prendre le contrôle complet de quatre appareils.

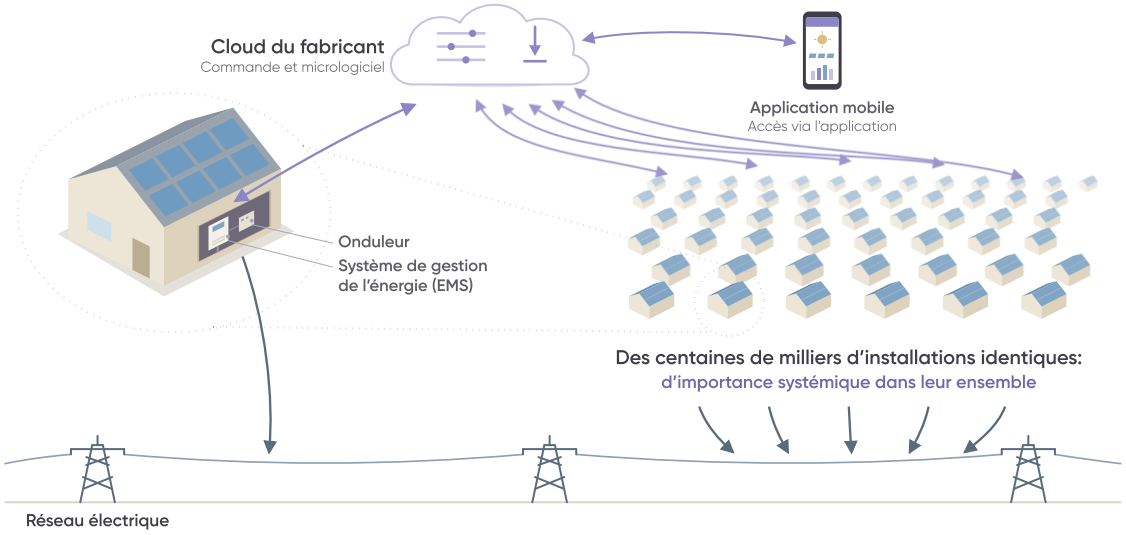
Les fabricants réagissent rapidement: le NTC a communiqué les constats aux fabricants concernés avant même la publication du présent rapport. Beaucoup ont réagi sans délai et ont déjà comblé les failles.

Ce n'est pas seulement la gravité qui décide, mais aussi la portée: une seule vulnérabilité dans un composant pertinent peut concerner des milliers d'installations raccordées. Six constats sont de cette nature. L'installation individuelle est insignifiante pour le réseau; le parc dans son ensemble est une infrastructure critique.

Risque structurel: le risque principal ne peut pas être éliminé par une meilleure sécurité des produits. Il naît du raccordement des appareils aux clouds des fabricants, par lesquels sont par exemple installées les mises à jour du micrologiciel.

Responsabilité non attribuée: les prescriptions ne vont pas assez loin pour les petites installations, et personne n'est responsable du risque né de leur somme.

Fin 2025, la Suisse comptait environ 338 000 installations photovoltaïques raccordées au réseau, pour une puissance de pointe d'environ 9,5 gigawatts (GW) (à titre de comparaison: la centrale nucléaire de Gösgen fournit environ 1 GW). Leur production annuelle de près de 8 térawattheures (TWh) couvrait 13,7% de la consommation finale d'électricité, à peu près au niveau de la centrale nucléaire de Gösgen. D'ici à 2030, la production doit plus que doubler selon les nouveaux objectifs intermédiaires du Conseil fédéral (18,7 TWh). Pour l'exploitation du réseau, ce n'est toutefois pas la somme annuelle qui compte, mais la contribution instantanée: par temps ensoleillé, à la mi-journée, le photovoltaïque couvre régulièrement plus de la moitié de la consommation, et près de 85% le 4 juillet 2026 à 14 h.



La structure de la production d'électricité s'en trouve modifiée: à côté de quelques grandes centrales réglementées apparaissent des centaines de milliers de petites installations raccordées au cloud et configurées de manière largement identique, insignifiantes individuellement, mais d'importance systémique dans leur ensemble.

Le parc suisse se compose presque exclusivement de petites installations sur les toits de bâtiments d'habitation et commerciaux, exploitées par des particuliers et de petites entreprises sans expertise dans l'exploitation et la maintenance d'infrastructures critiques. Ce qui exigeait autrefois un accès physique à une centrale est aujourd'hui possible par un accès à distance centralisé. Le risque ne réside pas dans le photovoltaïque lui-même, mais dans la manière dont sa commande est organisée.

Les installations exploitées par des particuliers n'ont jusqu'ici guère fait l'objet de tests indépendants de vulnérabilité: les incitations, les responsabilités clairement définies et une réglementation adaptée font défaut. Les prescriptions de cybersécurité de la branche de l'électricité (norme minimale TIC) s'adressent à des organisations et ne s'appliquent aux producteurs d'électricité qu'à partir de 100 mégawatts commandables par un système unique. Elles ne sont ni applicables ni destinées à l'installation d'une maison individuelle.

L'Institut national de test pour la cybersécurité NTC a donc testé, de sa propre initiative, pendant environ un an, onze produits numériques de la branche photovoltaïque répandus en Suisse: sept onduleurs et quatre systèmes de gestion de l'énergie de huit fabricants au total. L'équipe de test et une part substantielle des moyens financiers provenaient du NTC; plusieurs organisations, majoritairement du secteur de l'énergie, ont mis à disposition des appareils de test et participé aux coûts. L'étude a en outre bénéficié du soutien financier de SuisseEnergie. Ni les fabricants ni les organisations de soutien n'ont eu d'influence sur la sélection, l'étendue des tests ou les résultats. Tous les constats ont été signalés de manière confidentielle aux fabricants. Le présent rapport ne cite en principe aucun nom de produit ni aucun détail technique, mais décrit des schémas de risque typiques et les recommandations qui en découlent.

Au total, les tests ont donné plus de 50 constats, dont sept critiques et six autres élevés. Cinq des onze produits présentaient au moins un constat élevé ou critique. Sur quatre produits, le NTC a obtenu le contrôle complet de l'appareil, en partie par l'introduction de code externe, en partie par un accès de maintenance du fabricant insuffisamment protégé.

Quatre schémas sont apparus de manière récurrente:

- des défauts d'authentification et de contrôle d'accès, par exemple des mots de passe par défaut
- des accès de maintenance non sécurisés, par exemple avec des identifiants identiques pour tout le parc d'appareils
- l'absence ou la faiblesse du chiffrement des communications via les interfaces locales
- des interfaces qui ne peuvent pas être désactivées

Sur presque tous les onduleurs testés, il est possible de modifier par l'interface de commande locale, sans authentification, la puissance que l'installation injecte, jusqu'à zéro. Cette interface est active surtout là où un système de gestion de l'énergie commande l'installation. Pris en lui-même, un tel accès ne concerne qu'une seule installation. Mais si de nombreuses installations sont manipulées simultanément, cela peut mettre en danger la stabilité du réseau électrique. Le réseau doit assurer à tout moment un équilibre entre production et consommation. Une vulnérabilité ne devient donc pertinente pour le réseau non pas par sa seule gravité, mais par sa portée: six constats agissent, via une instance centrale, sur tout un parc d'appareils et donc sur de nombreuses installations à la fois.

Le niveau de sécurité des différents produits n'est pas moins bon que celui d'autres appareils connectés très répandus que le NTC a testés dans des analyses comparables. Aucun indice de portes dérobées intentionnellement intégrées ou de composants de communication cachés n'a été trouvé. La plupart des fabricants ont réagi rapidement aux vulnérabilités annoncées; pour une partie des constats, le processus de divulgation est encore en cours, notamment parce qu'un nouveau micrologiciel doit être mis à disposition dans le monde entier pour plusieurs séries de modèles. Ce qui distingue les installations solaires d'autres appareils connectés n'est pas la qualité des produits, mais leur rôle: ce qui reste le plus souvent un désagrément pour un appareil ménager pèse ici plus lourd, car les installations sont, dans leur ensemble, d'importance

systémique.

Le risque déterminant pour le réseau électrique suisse ne réside donc pas dans l'appareil individuel, mais dans la dépendance à l'égard de quelques fabricants: leur infrastructure cloud sert à commander les installations et à leur fournir des mises à jour du micrologiciel, et à côté de cela, la plupart des fournisseurs conservent un accès de maintenance privilégié à l'ensemble de leur parc d'appareils.

La concentration du marché augmente le nombre d'installations concernées: en 2025, plus de la moitié des onduleurs nouvellement installés provenait d'un seul fabricant, et environ 80% à quatre fabricants (Huawei, Fronius, Sungrow et SolarEdge). Ce risque ne se corrige pas par une meilleure sécurité des produits, mais uniquement par une réduction des dépendances: des engagements vérifiables, plusieurs fournisseurs sur le marché et une limitation technique de ce qui est possible à distance. À l'échelle internationale, le photovoltaïque distribué est traité de plus en plus comme une question d'infrastructure critique, et non plus seulement de politique climatique. L'Estonie, la Tchéquie et l'Allemagne ont publié des avertissements officiels. Taïwan fait de la preuve de cybersécurité un élément constitutif de l'homologation des produits, la Lituanie lie le raccordement au réseau à des exigences de sécurité. La Suisse a encore ce pas à franchir.

À partir des risques identifiés, le présent rapport formule des recommandations pour cinq destinataires.

Les exploitantes et exploitants de petites installations agissent le plus efficacement en choisissant un fournisseur établi auquel ils confient, outre l'installation, l'exploitation technique. Ils devraient se faire confirmer lors de la remise que des mots de passe individuels ont été définis et que l'installation n'est pas directement accessible depuis Internet, fixer par contrat qui est responsable des mises à jour et de la gestion des incidents, et renoncer à une commande à distance dont ils n'ont pas besoin.

Les exploitants d'installations plus grandes disposent de connaissances techniques et d'un pouvoir de négociation qui font défaut aux petites installations. Ils devraient inventorier leur parc d'installations, y compris les interfaces et les accès à distance, séparer le photovoltaïque, la gestion de l'énergie et l'infrastructure de recharge du reste du réseau, configurer délibérément la capacité de commande centralisée, régler par contrat les accès des fabricants et intégrer des exigences de sécurité dans leurs appels d'offres. Là où la norme minimale TIC ne s'applique pas, il est judicieux de l'appliquer volontairement.

Les entreprises d'installation décident en pratique du niveau de sécurité de l'installation individuelle, car la mise en service détermine ce qui pourra être attaqué par la suite. Elles devraient définir des identifiants individuels pour chaque installation et ne pas utiliser de mots de passe uniformes sur l'ensemble de leur clientèle, ne pas rendre l'onduleur accessible depuis Internet, désactiver les interfaces non nécessaires et séparer l'installation du reste du réseau domestique ou d'entreprise. La remise de l'installation doit inclure une documentation de la configuration et un accord clair sur qui installera à l'avenir les mises à jour. Dans l'acquisition, elles devraient privilégier des produits qui peuvent fonctionner sans cloud, offrent des interfaces locales protégées et disposent d'une période de support des mises à jour garantie.

Les fabricants devraient comprendre la sécurité comme un principe de conception: des identifiants spécifiques à l'appareil et non reconstituables, aucun secret inscrit en dur, des interfaces locales sécurisées ainsi que des mises à jour du micrologiciel signées. Les accès de maintenance doivent être limités dans le temps, journalisés et révocables par l'exploitante. Un verrouillage en usine de la commande à distance des fonctions pertinentes pour le réseau, qui ne peut être levé que sur place, est central. Il limite techniquement, et non seulement sur le plan organisationnel, la capacité d'action à grande échelle. Et l'exploitation doit rester possible même sans cloud.

Le monde politique et les autorités devraient combler la lacune concernant les petites installations. Les exigences qui portent sur le produit plutôt que sur l'exploitant sont efficaces: des exigences minimales pour la mise sur le marché d'onduleurs et de systèmes de gestion de l'énergie, des exigences de sécurité comme condition du raccordement au réseau et des contrôles récurrents qui ne se limitent pas à une homologation ponctuelle. Il est tout aussi nécessaire de désigner clairement l'entité responsable du risque qui ne naît que de la somme des petites installations. Le regroupement croissant de nombreuses petites installations auprès d'agrégateurs et de centrales électriques virtuelles est à surveiller. Pour les installations, il existe

déjà, avec le rapport de sécurité, une procédure de contrôle obligatoire qui pourrait être étendue à des aspects de cybersécurité.

Il n'existe pas de solution simple et complète; toutes les approches ont des avantages et des inconvénients, et des risques résiduels subsistent.

Le présent rapport n'est pas un argument contre le photovoltaïque, mais un argument en faveur de son développement en toute sécurité. Ce développement réduit la nécessité d'importer de l'énergie. Cette indépendance ne devrait toutefois pas être remplacée par une nouvelle dépendance, la dépendance à l'égard de quelques fabricants disposant d'un accès à distance à des milliers d'appareils pertinents pour le réseau. Le développement doit se poursuivre, avec la même exigence de contrôlabilité que celle qui va aujourd'hui déjà de soi pour d'autres infrastructures critiques.

2 Contexte et motivation

2.1 De quelques grandes centrales à de nombreuses petites

La production d'électricité de la Suisse a longtemps reposé pour l'essentiel sur un nombre restreint de grandes centrales réglementées et exploitées de manière centralisée. Il existe certes aussi de plus petites installations, comme les petites centrales hydroélectriques, mais elles ne pèsent pas outre mesure, ni par leur nombre ni par leur degré d'interconnexion. Avec le développement du photovoltaïque, un second monde est apparu à côté: des centaines de milliers de petites «centrales» décentralisées sur les toits des bâtiments d'habitation et commerciaux. Ce second monde fait apparaître de nouveaux cyberrisques, avec des effets sur l'ensemble de l'approvisionnement en électricité, dont traite le présent rapport.

2.2 Le photovoltaïque est devenu d'importance systémique

En Suisse, le photovoltaïque est passé du statut de technologie de niche à celui de pilier de l'approvisionnement en électricité. Fin 2025, on dénombrait environ 338 000 installations pour une puissance de pointe cumulée d'environ 9,5 gigawatts. Leur production annuelle de près de 8 térawattheures couvrait 13,7% de la consommation finale d'électricité[1] et correspondait ainsi à peu près à la production annuelle prévue de la centrale nucléaire de Gösgen.[2]

La contribution instantanée aux heures de pointe est plus parlante que ces valeurs annuelles. Par temps ensoleillé, à la mi-journée, le photovoltaïque couvre régulièrement plus de la moitié de la consommation instantanée, et nettement plus les jours de pointe. Le 4 juillet 2026 à 14 h par exemple, il s'agissait d'environ 6 100 mégawatts pour une charge d'environ 7 200 mégawatts, soit près de 85%[3].

Le photovoltaïque est ainsi devenu pertinent pour la sécurité de l'approvisionnement. Prise isolément, une installation reste insignifiante pour le réseau. Dans leur ensemble, les installations ont toutefois un poids significatif, et comme elles sont connectées et configurées de manière similaire, elles peuvent aussi être influencées collectivement: de manière conforme à leur destination et au service du réseau par le gestionnaire de réseau, de manière abusive par un attaquant. Ce n'est donc pas l'installation individuelle qui devient une infrastructure critique, mais le parc dans son ensemble.

Ce parc continue de croître. Le 26 novembre 2025, le Conseil fédéral a fixé pour la première fois, dans l'ordonnance sur l'énergie, des objectifs intermédiaires spécifiques par technologie: sur les 23 térawattheures que les énergies renouvelables autres que l'hydraulique doivent apporter d'ici à 2030, 18,7 TWh sont attribués au photovoltaïque. Par rapport aux quelque 8 térawattheures de 2025, cela représente plus qu'un doublement en cinq ans. L'objectif global de la loi sur l'énergie exige, pour les énergies renouvelables autres que l'hydraulique, 35 térawattheures d'ici à 2035 et 45 d'ici à 2050. Le Conseil fédéral n'a jusqu'ici fixé des objectifs intermédiaires spécifiques par technologie que pour 2030.[4] La croissance du parc accroît donc aussi la nécessité de pouvoir le piloter.

2.3 Pourquoi le sujet a jusqu'ici été peu étudié

Sur le plan international, la cybersécurité des installations photovoltaïques a récemment suscité davantage d'attention. Les appareils répandus en Suisse n'ont toutefois guère fait l'objet

[1] Office fédéral de l'énergie, «Statistique de l'énergie solaire 2025»: https://pubdb.bfe.admin.ch/fr/sammlungen/statistik-sonnenenergie
[2] Swissolar, «Baromètre du marché solaire Suisse 2025»: https://www.swissolar.ch/fr/marche-et-politique/marche-suisse/barometre-du-marche-solaire-suisse
[3] Valeurs instantanées: energy-charts.info (Fraunhofer ISE), production nette d'électricité Suisse, semaine 27/2026 (4 juillet 2026, à 14 h: charge 7 209 MW, solaire 6 121 MW): https://www.energy-charts.info/charts/power/chart.htm?c=CH&l=fr&year=2026&week=27
[4] Conseil fédéral, communiqué de presse «Le Conseil fédéral approuve l'adaptation de différentes ordonnances dans le domaine de l'énergie», 26 novembre 2025: https://www.admin.ch/fr/newnsb/dvb52hRdMmNdS3aNKL96C

jusqu'ici de tests indépendants et systématiques. Plusieurs raisons l'expliquent:

- **Peu d'incitations chez les exploitants d'installations**: les installations sont majoritairement exploitées par des particuliers et de petites entreprises. Chez les particuliers surtout, ce qui rend leur installation connectée vulnérable est rarement une préoccupation prioritaire. Si une installation tombe en panne à la suite d'une cyberattaque, ils achètent l'électricité manquante. Au regard de ces coûts d'électricité, une analyse de sécurité serait disproportionnellement coûteuse. Le risque véritable n'apparaît que lorsque de nombreuses installations sont manipulées simultanément, et il ne frappe alors pas les exploitants individuels, mais l'approvisionnement en électricité dans son ensemble.
- **Absence de compétence attribuée aux gestionnaires de réseau**: ils répondent de la stabilité du système global et en portent donc le risque. Par les conditions de raccordement, ils peuvent poser des exigences techniques, mais ils n'ont toutefois pas compétence pour la cybersécurité des petites installations privées en exploitation (cf. chapitre 7.4).
- **Acquisition coûteuse et tests risqués:** les appareils sont relativement coûteux et difficiles à acquérir pour des tests indépendants, et les tests exigent des travaux sur des appareils couplés au réseau, en partie sous haute tension, et donc des mesures de précaution particulières et des compétences spécialisées.
- **Transposabilité limitée des études internationales:** les analyses réalisées à l'étranger ne reflètent que partiellement les réalités du marché suisse. Certains produits répandus dans notre pays diffèrent de ceux étudiés à l'étranger, et certains fournisseurs importants sur le marché suisse n'apparaissent pas du tout dans les études internationales.

2.4 Pourquoi une cybermenace existe

Ce qui importe surtout pour la sécurité, c'est que les installations modernes sont la plupart du temps reliées à Internet et au cloud du fabricant. Cela permet concrètement d'influencer simultanément et de manière coordonnée un grand nombre d'installations. Le gestionnaire de réseau de distribution peut lui aussi, en partie, commander de nombreuses installations à la fois, par exemple pour réduire l'injection. Cette voie se distingue toutefois sur plusieurs points: elle ne va pas au-delà de la zone de desserte du gestionnaire concerné, elle est entre les mains d'une entreprise réglementée, et elle utilise souvent un canal de commande propre, séparé d'Internet (télécommande centralisée). Le cloud d'un fabricant peut en revanche atteindre un parc d'appareils via Internet, par-delà les zones de desserte et les frontières nationales. Ce que signifierait pour la stabilité du réseau une manipulation simultanée de nombreuses installations est traité au chapitre *6 Effets sur la stabilité du réseau*.

Cette menace rencontre des conditions-cadres défavorables. Les exploitantes et exploitants ne disposent en règle générale d'aucune expertise particulière en cybersécurité, et personne n'est tenu d'assurer la cybersécurité pour l'exploitation de leurs installations. Alors que les gestionnaires de réseau et les très grands producteurs d'électricité sont soumis à des prescriptions cyber telles que la norme minimale TIC, les petites installations, et donc pratiquement toutes les installations photovoltaïques suisses, échappent à ces règles. Pour les producteurs d'électricité, la norme ne s'applique qu'à partir de 100 MW, soit à partir de 100 000 kW. Une installation en toiture typique se situe dans une plage de quelques dizaines de kilowatts, soit plus de mille fois moins.

La société nationale du réseau de transport partage cette appréciation. Dans son white paper «Intégration du photovoltaïque compatible avec le système»[5], Swissgrid range expressément les risques de cybersécurité parmi les défis de l'exploitation du système: selon elle, les onduleurs ainsi que d'autres installations comme les bornes de recharge et les systèmes de gestion de l'énergie sont de plus en plus commandables à distance via Internet. Des prescriptions insuffisantes et une prise de conscience insuffisante du problème augmenteraient le risque que des acteurs externes déstabilisent par ce biais le système électrique.

[5] Swissgrid SA, white paper «Intégration du photovoltaïque compatible avec le système», mars 2026: https://www.swissgrid.ch/fr/home/newsroom/blog/2026/20260330-01.html

2.5 L'environnement de politique de sécurité

Cette situation technique de départ coïncide avec une situation de politique de sécurité qui se dégrade. Dans son rapport de situation «La sécurité de la Suisse 2026»[6], le Service de renseignement de la Confédération (SRC) constate une détérioration marquée et durable de l'environnement de politique de sécurité. Les infrastructures critiques y sont expressément considérées comme menacées aussi bien par des attaques physiques que par des cyberattaques. Le SRC relève en outre que les infrastructures des pays européens ne peuvent pas être considérées isolément. Selon lui, une attaque contre une infrastructure suisse visant à frapper d'autres États qui en dépendent est tout aussi concevable que, à l'inverse, des dommages collatéraux résultant d'attaques contre des infrastructures étrangères. Le SRC signale de même que l'attractivité de telles cibles croît à mesure que les États de l'OTAN et de l'UE protègent davantage leurs infrastructures critiques sans que la Suisse suive le mouvement.

La cyberattaque coordonnée de décembre 2025 contre l'approvisionnement polonais en énergie et en chaleur montre que cette appréciation n'a rien d'abstrait. Plus de 30 parcs éoliens et solaires ont notamment été touchés[7]. En juillet 2026, le Royaume-Uni et l'UE ont officiellement attribué l'attaque au service de renseignement russe FSB (Centre 16).[8] Compte tenu de l'étroite imbrication des réseaux européens et de l'appréciation du SRC, des évolutions comparables sont également pertinentes pour la Suisse.

Un avis de sécurité commun de l'Office fédéral allemand de protection de la Constitution (BfV) et de l'Office fédéral allemand de la sécurité informatique (BSI) du 3 juin 2026 montre que le photovoltaïque distribué est concrètement ciblé par des activités de reconnaissance[9]. Selon leurs informations, des cyberacteurs russes procèdent activement à la reconnaissance d'installations photovoltaïques reliées à Internet sans protection. Sont visés les systèmes de surveillance, qui permettent aussi un accès de commande aux installations. Les installations concernées sont majoritairement celles de particuliers et de coopératives sans lien avec le secteur de l'énergie. Pour une partie de ces installations, l'accès est possible sans identifiants, et les versions logicielles sont parfois fortement obsolètes. Il s'agit là de reconnaissance et non d'une attaque. L'avis montre toutefois que c'est précisément la catégorie d'installations qu'examine le présent rapport qui est systématiquement recensée par des acteurs étatiques.

2.6 Délimitation: batteries de stockage, infrastructure de recharge et autres appareils connectés

Les consommateurs et les stockages connectés tels que les batteries de stockage, les bornes de recharge pour véhicules électriques et les pompes à chaleur ne font pas l'objet de la présente analyse, mais gagnent en importance. Les batteries de stockage en particulier se répandent rapidement. Parmi les nouvelles installations photovoltaïques sur les maisons individuelles suisses, une part considérable est désormais équipée d'un stockage.[10] Du point de vue de la cybersécurité, les attaques qui utilisent le photovoltaïque en combinaison avec des batteries de stockage ou l'infrastructure de recharge sont particulièrement pertinentes, car elles permettent de manipuler aussi bien l'injection que le soutirage. Le NTC a déjà examiné l'infrastructure de recharge dans un rapport antérieur[11].

---

[6] Service de renseignement de la Confédération (SRC), «La sécurité de la Suisse 2026»: https://www.vbs.admin.ch/fr/newnsb/jyRmuld1hBVy

[7] CERT Polska, «Energy Sector Incident Report – 29 December»: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

[8] OFSI/GOV.UK, communiqué de sanctions du 13 juillet 2026: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions

[9] Bundesamt für Verfassungsschutz (BfV) et Bundesamt für Sicherheit in der Informationstechnik (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure», 3 juin 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

[10] Office fédéral de l'énergie, «Statistique de l'énergie solaire 2025»: https://pubdb.bfe.admin.ch/fr/sammlungen/statistik-sonnenenergie

[11] Institut national de test pour la cybersécurité NTC, rapport sur la cybersécurité de l'infrastructure de recharge, 2023: https://fr.ntc.swiss/news/2023-analyse-infrastructures-recharge-electromobilite

3 L'écosystème d'une installation photovoltaïque

Le présent chapitre décrit les éléments qui composent une installation photovoltaïque. Il explique comment ceux-ci communiquent entre eux et avec Internet, et qui peut les commander. L'exposé reste volontairement descriptif et montre où l'architecture offre une surface d'attaque. La question de savoir si ces surfaces se sont effectivement révélées risquées lors de l'analyse n'est pas traitée dans ce chapitre. Les composants testés et les raisons de ce choix figurent au chapitre *4 Méthodologie*. Les résultats suivent au chapitre *5 Constats et risques*.

3.1 Les composants et leur interaction

Une installation photovoltaïque typique se compose de quelques éléments de base. Selon le type de construction, ils sont plus ou moins fortement intégrés les uns aux autres. Pour l'exposé qui suit, ils sont présentés séparément par fonction. Les **modules solaires** produisent du courant continu (CC). L'**onduleur** convertit celui-ci en courant alternatif (CA) conforme au réseau et l'injecte dans le réseau. Il est ainsi le composant central de l'installation, activement commandable. Pour la surveillance à distance, l'onduleur est relié à Internet par un **module de communication** (souvent déjà intégré dans l'onduleur), le plus souvent par Wi-Fi, réseau mobile ou câble. Cette connexion n'est pas techniquement indispensable, mais elle est la règle en pratique. Sur les installations modernes, la surveillance passe le plus souvent par le portail Internet du fabricant, et lorsqu'aucun module de communication n'est installé, ou que d'autres appareils tels qu'une batterie de stockage, une borne de recharge ou une pompe à chaleur sont également pilotés, c'est souvent un **système de gestion de l'énergie** qui assure la communication vers l'extérieur. Par ce raccordement, les données d'exploitation parviennent à un **cloud du fabricant**, qui les stocke et les visualise. Selon le fabricant, il permet en outre la surveillance à distance, la commande à distance et la mise à jour du micrologiciel de l'installation. L'**application mobile ou web**, enfin, est l'interface de commande pour l'exploitante ou l'exploitant et accède elle-même au cloud. En complément, d'autres consommateurs et stockages connectés sont souvent intégrés, par exemple des **batteries de stockage**, des **bornes de recharge pour véhicules électriques ou des pompes à chaleur**. De tels composants supplémentaires élargissent encore la surface d'attaque et les effets possibles. Au point de raccordement au réseau se trouve en outre le compteur du gestionnaire de réseau de distribution. Il mesure l'énergie soutirée et l'énergie injectée et est progressivement remplacé en Suisse par un système de mesure intelligent (**smart meter**), qui rend les valeurs de mesure lisibles à distance. Le compteur n'appartient pas à l'exploitante ou à l'exploitant, mais au gestionnaire de réseau, et constitue ainsi une liaison propre vers l'extérieur, indépendante du fabricant.

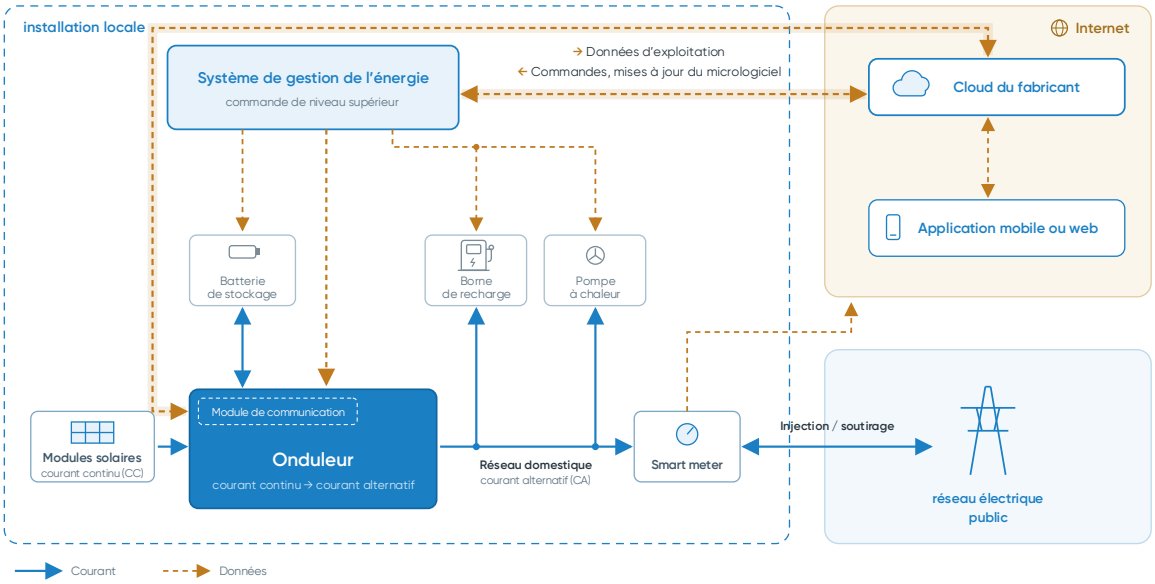


Figure 1: aperçu schématique d'une installation photovoltaïque typique

3.2 Onduleur et système de gestion de l'énergie

Pour comprendre les possibilités de commande, la distinction entre onduleur et système de gestion de l'énergie (SGE) est centrale, car les deux notions sont souvent confondues au quotidien.

L'**onduleur** convertit le courant et l'injecte dans le réseau. Grâce à ses fonctions de soutien au réseau, comme les consignes de puissance active et réactive ou les courbes caractéristiques, il est l'élément qui influence directement l'injection.

Le **système de gestion de l'énergie** est un système de commande de niveau supérieur. Il coordonne plusieurs appareils d'une installation, typiquement un onduleur, une batterie de stockage, une borne de recharge et une pompe à chaleur, et optimise leur exploitation, par exemple en fonction de l'autoconsommation.

Il en résulte une double nature qui rend le SGE particulièrement important pour la cybersécurité. Comme partie de la solution, un SGE peut réduire la dépendance à l'égard des clouds des différents fabricants: chaque appareil ne doit pas nécessairement être relié au cloud de son fabricant, et un SGE judicieusement placé entre le réseau local et l'onduleur peut limiter l'accessibilité directe des appareils individuels. Le problème s'en trouve en revanche aggravé sur un point: qui contrôle le SGE contrôle tous les appareils qui y sont raccordés et peut ainsi causer au moins autant de dommages que par un onduleur isolé, potentiellement davantage, parce que le SGE commande aussi d'autres composants comme la batterie de stockage et la borne de recharge. Les fournisseurs de SGE multimarques agrègent en outre ce contrôle sur différentes marques d'appareils. Le SGE est ainsi, par essence, un composant local, mais en même temps un point de concentration dont la compromission a une portée plus grande que celle d'un onduleur isolé.

3.3 Voies de communication et vulnérabilités connues

Deux questions importent pour la sécurité: quels composants communiquent entre eux et dans quelle mesure ces liaisons sont protégées. Le module de communication transmet les données d'exploitation au cloud du fabricant et en reçoit des commandes. L'application accède elle aussi typiquement au cloud, et non directement à l'installation. Si le module de communication est intégré dans l'onduleur, cette liaison se déroule à l'intérieur de l'appareil. Il en va autrement dès qu'un appareil externe doit s'adresser directement à l'onduleur, par exemple un système de gestion de l'énergie. La liaison passe alors localement par le réseau du bâtiment ou le réseau domestique.

Pour cette liaison locale, des protocoles industriels sont répandus, au premier rang desquels Modbus: autrefois par une liaison série filaire (RS485), de plus en plus par le réseau (Modbus TCP). En parallèle, des protocoles propres aux fabricants sont utilisés. Modbus a été conçu pour des installations cloisonnées et n'offre de lui-même ni chiffrement ni authentification. Certains fabricants ajoutent des mécanismes d'autorisation propriétaires. Une extension de sécurité fondée sur TLS, ajoutée en 2018, n'est guère répandue en pratique. C'est pourquoi cette interface est importante pour les constats présentés plus loin.

Selon cette architecture, l'onduleur n'est pas directement accessible depuis Internet. La voie venant de l'extérieur passe au contraire par le cloud du fabricant. Le cloud du fabricant peut à son tour, de par sa conception, surveiller, commander et mettre à jour un très grand nombre d'installations à la fois.

Ce tableau concorde avec la recherche existante. Une analyse[12] de 93 vulnérabilités divulguées depuis 2012 avec un numéro CVE chez 34 fabricants attribue la plus grande part au niveau de la surveillance et du cloud, environ 38% au monitoring solaire et environ 25% au cloud, tandis que l'onduleur avec module de communication était concerné dans près de 30% des cas. Environ 80% de tous les cas sont considérés comme élevés ou critiques. Ces chiffres sont à lire avec prudence, car ils comptent des occurrences recensées et non un risque, et le niveau connecté est

[12] dos Santos, La Spina, Dashevskyi, «A Closer Look at the Gaps in the Grid», Black Hat Asia 2025: https://i.blackhat.com/Asia-25/Asia-25-dosSantos-A-Closer-Look-at-the-Gaps-in-the-Grid.pdf

incomparablement plus facile à tester à distance. Ces vulnérabilités ne restent toutefois pas théoriques: six des vulnérabilités cataloguées sont régulièrement exploitées par des botnets depuis 2022. Ce qui est finalement déterminant, c'est moins le nombre de vulnérabilités que le fait qu'un seul cloud puisse atteindre simultanément un très grand nombre d'installations.

3.4 Commande centralisée et commande locale

Les éléments de base peuvent être classés selon le nombre d'installations qu'un composant compromis peut influencer. Une instance centrale comme le cloud du fabricant agit simultanément sur de nombreuses installations. Qui la contrôle peut envoyer des commandes à tous les appareils raccordés. Une instance locale comme l'onduleur lui-même, l'application mobile ou un appareil de commande local n'influence en revanche que sa propre installation. Cette distinction sépare les attaques à effet d'échelle, qui touchent à distance de nombreuses installations, des attaques sans effet d'échelle, qui restent limitées à l'installation individuelle. C'est pourquoi de petites installations isolées sont insignifiantes en elles-mêmes, mais deviennent pertinentes dans la masse connectée. Pour une manipulation ayant un effet sur le réseau, le niveau central constitue la cible la plus intéressante. Cette capacité de commande centralisée peut toutefois aussi être limitée délibérément par des moyens techniques. Le présent rapport recommande donc de concevoir les appareils de telle sorte que le cloud puisse encore surveiller l'installation et lui fournir des mises à jour signées, mais ne puisse plus la commander (cf. chapitre *8.4.2*).

À côté du cloud du fabricant apparaît de plus en plus un deuxième niveau de commande centralisée: les agrégateurs et les centrales électriques virtuelles. Un fournisseur y regroupe de nombreuses installations distribuées par des interfaces Internet et commercialise leur puissance agrégée, par exemple sur le marché de l'énergie de réglage. Le projet pilote «PV4Balancing»[13] de la société nationale du réseau de transport Swissgrid en est un exemple: des installations photovoltaïques agrégées y réduisent sur demande leur injection en tant que réserve tertiaire négative. Un deuxième exemple est encore plus proche de la masse des petites installations: Helion a reçu de Swissgrid l'autorisation de regrouper, via sa propre plateforme, de petites installations photovoltaïques privées, des accumulateurs domestiques et des bornes de recharge, et d'offrir la puissance ainsi regroupée sur le marché de l'énergie de réglage[14]. Ce sont ainsi précisément les installations qui, individuellement, ne sont soumises à aucune exigence de cybersécurité qui se retrouvent sous une commande à distance centralisée. L'agrégateur lui-même est en revanche assujetti dès qu'il peut accéder, par un système unique, à au moins 100 MW (cf. chapitre *7.4).* Le «Flexpool»[15] de CKW réunit par exemple déjà plus de 1 000 MW provenant d'environ 1 700 installations de clients en un seul point de commande, même s'il est technologiquement mixte et ne relève pas uniquement du photovoltaïque. Cette évolution est à double tranchant: utilisées au service du réseau, des installations commandables et regroupées sont un instrument de stabilisation. En même temps, l'agrégateur constitue un point de commande central supplémentaire qui, en cas de compromission, ouvre une commande à distance déjà coordonnée sur de nombreuses installations. Ce regroupement n'est pas un effet secondaire, mais fait partie de l'architecture cible. Swissgrid retient que la participation d'unités décentralisées aux marchés de l'énergie de réglage devrait se faire par des agrégateurs avec le moins d'obstacles possible, et cite une plateforme de flexibilité centrale dotée d'un mécanisme de coordination comme la variante la plus appropriée. Cette approche est testée dans un autre projet pilote, la «coordination TSO-DSO».[16] Le nombre d'installations accessibles par un point de commande unique devrait continuer de croître. Il est d'autant plus important de clarifier les exigences de sécurité applicables à ce niveau tant qu'il est encore en cours de mise en place. Le NTC n'a pas testé ces plateformes; cette mise en perspective concerne la structure, non la sécurité de fournisseurs individuels.

[13] Swissgrid, projet pilote «PV4Balancing»: https://www.swissgrid.ch/fr/home/newsroom/blog/2025/20250225-01.html
[14] Helion Energy AG, centrale électrique virtuelle pour la clientèle privée sur la base de la plateforme «Helion ONE»: https://www.gebaeudetechnik.ch/de/news/virtuelles-kraftwerk-fuer-die-schweiz--252
[15] CKW (groupe Axpo), «Flexpool»: https://www.ckw.ch/ueber-ckw/medienstelle/medienmitteilungen/2025/1000-megawatt-virtuelles-grosskraftwerk-von-ckw-erreicht-meilenstein
[16] Swissgrid SA, white paper «Intégration du photovoltaïque compatible avec le système», mars 2026: https://www.swissgrid.ch/fr/home/newsroom/blog/2026/20260330-01.html

3.5 Types d'installations et exploitants

La connexion au réseau informatique et le niveau de protection dépendent fortement du type d'installation. En s'appuyant sur les catégories d'encouragement de la Confédération, les installations jusqu'à 100 kW sont considérées comme de **petites installations**: elles comprennent les maisons individuelles, les immeubles d'habitation et les petits bâtiments commerciaux. Les petites installations se trouvent le plus souvent dans le réseau ordinaire du bâtiment ou le réseau domestique et sont exploitées par des particuliers ou de petites entreprises qui, en règle générale, ne disposent pas d'expertise particulière en cybersécurité. Les **grandes installations** de plus de 100 kW sont plus souvent suivies par des professionnels et segmentées derrière un pare-feu. Les plus grandes installations sont raccordées à une sous-station propre et au gestionnaire de réseau de distribution et renoncent plus souvent à un raccordement au cloud du fabricant. À l'inverse, le raccordement au cloud est certes la règle pour les petites installations, mais il n'y est pas non plus impératif.

2025	Nombre de système	Puissance en MW	Ø Puissance en kW
jusque 4 kW	1'132	3.0	2.7
de 4 kW à 10 kW	9'073	68.9	7.6
de 10 kW à 20 kW	14'864	211.9	14.3
de 20 kW à 30 kW	4'831	117.8	24.4
de 30 kW à 50 kW	3'134	119.8	38.2
de 50 kW à 100 kW	1'977	138.9	70.3
de 100 kW à 1000 kW	2'175	536.2	246.6
plus de 1000 kW	72	136.4	1'882.5
Total install. racc. au réseau	**37'257**	**1'332.9**	**35.8**

Figure 2: installations raccordées au réseau par taille. Source: Statistique de l'énergie solaire 2025[17], OFEN

La répartition par taille met clairement en évidence le déséquilibre. Sur les 37 257 installations raccordées au réseau nouvellement installées en 2025, 35 011, soit 94%, atteignaient au plus 100 kW. Elles représentaient environ la moitié de la puissance nouvellement installée. L'installation moyenne mesure environ 25 kW, la médiane environ 11 kW. Dans le même temps, environ 40% de la production photovoltaïque suisse proviennent d'installations de moins de 30 kW. Le parc auquel ne s'applique aucune prescription de cybersécurité en exploitation représente ainsi une part considérable de la production.

3.6 Concentration du marché

Pour la sécurité, il n'importe pas seulement de savoir combien d'installations sont installées, mais de combien de fabricants différents elles proviennent: le micrologiciel, les accès de maintenance et la chaîne de mise à jour sont déterminés par le fabricant, raison pour laquelle un seul constat peut valoir pour l'ensemble de son parc d'appareils, y compris pour des installations sans raccordement au cloud. En Suisse, la répartition du marché a évolué à plusieurs reprises. Le PV-Barometer 2026[18] analyse à cette fin les conceptions de projets: en 2017, Fronius détenait 45,7% de part de marché; en 2020, le marché se répartissait entre trois fournisseurs de taille comparable (FIMER 23,5%, Fronius 22,9, SolarEdge 22,8); en 2025, Huawei représentait 52,3%, Fronius 13,3%, Sungrow 9,2% et SolarEdge 8,2%. La part du plus grand fournisseur est ainsi aujourd'hui plus élevée que jamais durant la période d'observation. Le nombre de fournisseurs n'a pas diminué pour autant; c'est la répartition qui a changé.

[17] Office fédéral de l'énergie, «Statistique de l'énergie solaire 2025»: https://pubdb.bfe.admin.ch/fr/sammlungen/statistik-sonnenenergie
[18] Haute école spécialisée bernoise & Eturnity SA, «PV-Barometer 2026»: https://www.pv-barometer.ch/

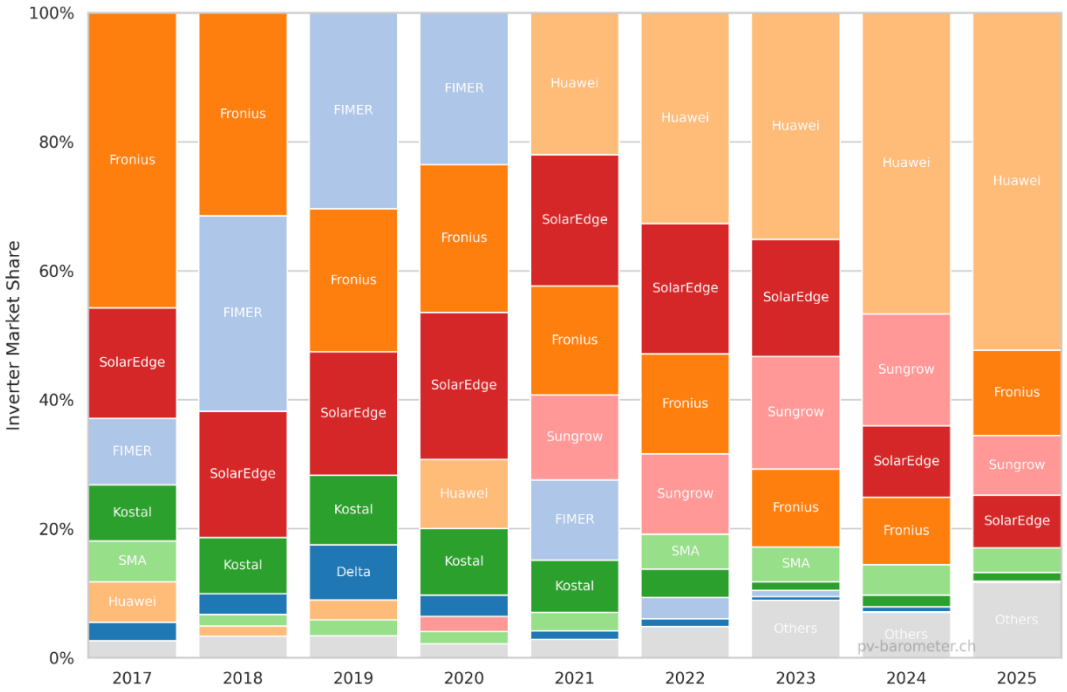


Figure 3: parts de marché des fabricants d'onduleurs en Suisse. Source: PV-Barometer 2026

4 Méthodologie

Le NTC a soumis des onduleurs et des systèmes de gestion de l'énergie à une analyse de sécurité technique complète. L'analyse était axée sur trois principes:

- **Proximité du marché:** une sélection des appareils fondée sur leur diffusion sur le marché suisse.
- **Indépendance:** aucune implication des fabricants dans la sélection, la réalisation et le financement; contacts uniquement dans le cadre du signalement des vulnérabilités.
- **Effet d'échelle:** concentration sur les vulnérabilités permettant de manipuler simultanément de nombreuses installations.

Sur une période d'environ un an, le NTC a consacré au total quelque 1 300 heures de travail à cette étude. Elle a été soutenue par de nombreuses organisations du secteur de l'énergie, qui ont mis à disposition des appareils de test et participé aux coûts. Les fabricants des produits testés n'y ont pas pris part. Les sections suivantes décrivent l'objet de l'étude et sa délimitation, la sélection et l'acquisition des appareils, le dispositif de test, la priorité analytique ainsi que la gestion des vulnérabilités identifiées.

4.1 Objet de l'étude et délimitation

L'analyse s'est délibérément concentrée sur les onduleurs et les systèmes de gestion de l'énergie ainsi que sur les installations situées dans des bâtiments d'habitation et de petits bâtiments commerciaux. Ces deux choix découlent de l'architecture décrite au chapitre *3 L'écosystème d'une installation photovoltaïque*: les onduleurs et les systèmes de gestion de l'énergie sont les composants centraux d'une installation photovoltaïque, raccordés au réseau et au cloud, et peuvent commander activement l'injection. De telles petites installations ne sont quant à elles soumises à aucune prescription de cybersécurité en exploitation. Du côté des produits, les exigences de cybersécurité de la directive européenne sur les équipements radioélectriques s'appliquent depuis août 2025 aux appareils nouvellement mis sur le marché, pour autant qu'ils disposent d'une interface radio (cf. chapitre *7.3.2*). Celles-ci fixent un niveau de base, mais ne disent rien de la configuration, de l'exploitation et de la maintenance de l'installation installée et reposent sur l'autodéclaration du fabricant. Les installations sont le plus souvent exploitées par des particuliers ou de petites entreprises sans expertise particulière en cybersécurité, et n'ont jusqu'ici guère fait l'objet de tests indépendants.

Les modules solaires n'ont délibérément pas été examinés. Certains modules contiennent certes de l'électronique active comme des optimiseurs de module. Mais ceux-ci, si tant est qu'ils soient connectés, ne sont reliés qu'à l'onduleur et se situent ainsi en dehors du schéma d'attaque à effet d'échelle. Des composants comme les systèmes de mesure intelligents, les batteries de stockage et les bornes de recharge pour l'électromobilité ne faisaient pas non plus partie de l'étude. Ces composants aussi sont pertinents pour la sécurité et gagnent en importance: les batteries de stockage, par exemple, sont raccordées au réseau et au cloud de manière analogue aux onduleurs, et une charge ou une décharge coordonnée de nombreux stockages aurait un effet comparable sur le réseau.

Les très petits appareils solaires enfichables («kits solaires de balcon») se situaient en outre en dehors du périmètre de l'étude. Ils sont nettement moins répandus sur le marché suisse qu'en Allemagne et font déjà l'objet d'études indépendantes. L'existence de vulnérabilités sérieuses dans cette catégorie est illustrée, par exemple, par les vulnérabilités radio divulguées par le Chaos Computer Club (CCC)[19] concernant les micro-onduleurs Hoymiles (2026) (cf. chapitre *5.3.4*).

Le cadre juridique a lui aussi déterminé la profondeur d'analyse. Le NTC a acquis les appareils eux-mêmes et a pu les examiner sans restriction. Les clouds des fabricants sont en revanche des systèmes tiers exploités en production: y accéder sans le consentement de l'exploitant peut être

[19] Chaos Computer Club (B. Heinz «Hunz»), «Analyse der Funk- und Firmware-Schwachstellen von Hoymiles-Wechselrichtern», 2026: https://www.ccc.de/updates/2026/blinkenlights-hoymiles

punissable au sens de l'art. 143bis CP. Un avis de droit établi en 2023 sur mandat du NTC[20] délimite les actes de test admissibles sans un tel consentement.

Un consentement n'aurait pu être obtenu que par l'intermédiaire des fabricants. Cela aurait signifié leur implication dans l'étude et aurait été contraire au principe d'indépendance. Le NTC s'est donc délibérément limité au cadre admissible sans consentement et a renoncé à un test approfondi du niveau cloud.

Le présent rapport évalue la faisabilité technique, non l'intention d'acteurs potentiels ni le déroulement de la gestion d'une crise.

4.2 Sélection des appareils

Il n'existe pas de statistique complète des onduleurs installés dans notre pays. Pour le nombre d'installations et la répartition des puissances, des données officielles sont disponibles (statistiques de Pronovo[21], Statistique de l'énergie solaire[22] de l'OFEN). Pour les parts de marché des fabricants, il n'existe en revanche que le relevé du PV-Barometer, placé sous la responsabilité d'un acteur du marché, mais qui indique les parts chaque année depuis 2017 et rend ainsi visible l'évolution dans le temps. On ne peut pas en déduire des chiffres exacts, mais bien des ordres de grandeur, et ceux-ci sont sans équivoque. En 2025, un peu plus de la moitié des onduleurs nouvellement installés provenait d'un seul fabricant, environ deux tiers à deux fabricants et environ 80% à quatre fabricants. Sept onduleurs de six fabricants ont donc été examinés, dont les principaux fournisseurs du marché.

Pour les systèmes de gestion de l'énergie, les données sont encore plus limitées. Il n'existe pas de statistique comparable. Les entretiens avec des spécialistes de la branche ont ici été déterminants. Quatre systèmes ont été testés.

La sélection couvre ainsi les deux horizons temporels. Pour le passé, l'analyse sur plusieurs années est utile: comme la plus grande partie du parc suisse n'a été construite que ces dernières années, les parts de marché de ces années reflètent approximativement le parc installé. Pour l'avenir, ce qui est installé aujourd'hui détermine le risque sur plus d'une décennie.

4.3 Acquisition

Les appareils ont été acquis par l'intermédiaire d'organisations partenaires et par la même voie qu'utiliserait une clientèle ordinaire. Cette manière de procéder garantit que les appareils ont été testés dans leur état réel à la livraison et avec des configurations réelles, et non des échantillons de test spécialement préparés. Les contacts avec les fabricants ont eu lieu exclusivement dans le cadre du signalement des vulnérabilités.

L'analyse a été menée à l'initiative du NTC. La conception, la réalisation et l'évaluation relevaient entièrement du NTC et ont eu lieu dans son propre laboratoire. Elle a été financée principalement par des fonds du NTC, complétés par plusieurs organisations partenaires du secteur de l'énergie qui ont participé aux coûts et fourni des appareils de test. Les fabricants n'y ont pas pris part et les organisations partenaires n'ont eu aucune influence sur l'étendue des tests ni sur les résultats.

4.4 Dispositif de test

L'exploitation des onduleurs nécessite une alimentation en courant continu à l'entrée. Comme l'exploitation de véritables modules solaires n'est pas praticable en laboratoire, les modules ont été remplacés par une source de courant continu commandable. Les appareils ont ainsi pu être

[20] Walder Wyss SA, avis de droit «Responsabilité pénale de l'Ethical Hacking»: https://www.walderwyss.com/fr/news/2023-06-26_rechtsgutachten-zur-strafbarkeit-von-fuer-das-nationale-testinstitut-fuer-cybersicherheit-ntc
[21] Pronovo SA, statistiques: https://pronovo.ch/fr/services/rapports-et-publications/
[22] Office fédéral de l'énergie, «Statistique de l'énergie solaire 2025»: https://pubdb.bfe.admin.ch/fr/sammlungen/statistik-sonnenenergie

testés dans des conditions reproductibles. L'accent a porté sur l'analyse du micrologiciel, des interfaces, du raccordement au cloud et de la configuration. Une réserve de principe subsiste: un appareil pourrait modifier son comportement dès qu'il détecte qu'il est testé. Un tel mode spécifique au banc d'essai ne serait pas nécessairement décelable avec une approche en laboratoire. Le NTC est conscient de cette possibilité et y a paré dans la mesure du possible: les appareils ont été acquis par les canaux de distribution ordinaires et exploités dans leur état à la livraison, et le dispositif de test a été conçu de manière à se distinguer aussi peu que possible d'une installation réelle.

4.5 Priorité aux vulnérabilités à effet d'échelle

L'analyse s'est concentrée sur les vulnérabilités permettant de manipuler simultanément un grand nombre d'installations. Les vulnérabilités qui ne concernent que l'installation individuelle, par exemple celles qui supposent un accès physique à l'appareil, n'étaient pas prioritaires. Cette distinction entre vulnérabilités à effet d'échelle et vulnérabilités sans effet d'échelle traverse l'ensemble du rapport et détermine la pondération des différents constats.

4.6 Processus de signalement des vulnérabilités

Toutes les vulnérabilités identifiées ont été signalées de manière confidentielle aux fabricants concernés dans le cadre d'un processus de divulgation coordonnée (responsible disclosure), afin de permettre leur correction avant la publication. Cette manière de procéder correspond à la Responsible Disclosure Policy[23] du NTC et à la pratique courante de la branche. Le présent rapport public renonce donc délibérément aux détails techniques et à la mention des produits concernés et présente à la place les schémas de risque sous-jacents.

[23] Vulnerability Disclosure Policy du NTC: https://www.ntc.swiss/hubfs/ntc-vulnerability-disclosure-policy.pdf

5 Constats et risques

5.1 Vue d'ensemble

Le NTC a examiné onze produits: sept onduleurs de six fabricants et quatre systèmes de gestion de l'énergie. Deux des systèmes de gestion de l'énergie proviennent de fabricants qui produisent aussi l'un des onduleurs testés, de sorte que les onze produits se répartissent sur huit fabricants. Au total, plus de 50 vulnérabilités ont été identifiées, dont sept classées «critiques» et six «élevées». Cinq des onze produits présentaient au moins un constat élevé ou critique.

Sur quatre produits, le NTC a obtenu le contrôle complet de l'appareil, soit le niveau de privilèges le plus élevé (accès root). Sur un produit, trois vulnérabilités y ont mené, qui permettent l'exécution de code arbitraire sur l'appareil (Remote Code Execution) et sont toutes classées comme critiques. Sur trois produits, un accès de maintenance du fabricant insuffisamment protégé a suffi. Ce niveau de privilèges est important parce qu'il permet non seulement de commander l'installation, mais de modifier le micrologiciel et donc le comportement de l'appareil dans son ensemble.

Six des plus de 50 constats agissent, via une instance centrale, sur de nombreuses installations à la fois et ont donc un effet d'échelle. Les autres restent limités à l'installation individuelle. Ces six constats constituent la partie des résultats déterminante pour la stabilité du réseau, car une vulnérabilité ne devient pas pertinente pour le réseau par sa gravité technique, mais par sa capacité à toucher tout un parc d'appareils. Le BSI cite lui aussi expressément dans son avis[24] de juin 2026 l'«utilisation des effets d'échelle» comme la voie qui mène de l'installation individuelle à la stabilité du réseau. Deux des six constats sont classés «critique», un «élevé» et trois «moyen». Ce classement évalue l'effet sur le produit testé et non les conséquences pour le réseau électrique. Un constat classé «moyen» dans un cloud qui commande un parc d'appareils peut peser plus lourd du côté du réseau qu'un constat critique sur l'appareil individuel. Cinq des six constats proviennent du niveau ayant le plus grand effet de levier, le cloud du fabricant, et plus précisément d'interfaces accessibles depuis l'extérieur. Un test approfondi du cloud lui-même n'était pas possible pour des raisons juridiques (cf. chapitre *4.1*). Une analyse menée uniquement depuis l'extérieur a toutefois suffi pour trouver des vulnérabilités d'une portée s'étendant à tout le réseau.

Pour une partie des constats, dont plusieurs des constats critiques, le processus de divulgation coordonnée n'est pas encore achevé au moment de la publication. Cela s'explique par la nature des corrections à apporter et non par un défaut de coopération: plusieurs séries de modèles à l'échelle mondiale sont parfois concernées, qui nécessitent un nouveau micrologiciel.

Le niveau de sécurité des différents produits n'est généralement pas moins bon que celui d'autres appareils très répandus de l'«Internet of Things» (IoT), et il est même meilleur sur certains aspects. Cette mise en perspective s'appuie sur l'expérience de test du NTC avec des catégories d'appareils comparables, notamment sur les analyses de périphériques[25] et de produits relevant du champ d'application de la directive RED[26]. Il faut toutefois prendre au sérieux les schémas récurrents et surtout les risques structurels, qui dominent le tableau d'ensemble et sont au centre de ce chapitre. C'est précisément là que réside le cœur du sujet: ce qui reste un désagrément pour des appareils ménagers connectés concerne ici une catégorie d'appareils qui, dans son ensemble, est d'importance systémique.

Les autorités de sécurité allemandes confirment que ces faiblesses n'existent pas seulement en laboratoire: elles observent des installations photovoltaïques pour lesquelles un accès est en partie possible sans identifiants et dont les versions logicielles sont fortement obsolètes (cf. chapitre *2.5*).

[24] Bundesamt für Verfassungsschutz (BfV) et Bundesamt für Sicherheit in der Informationstechnik (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure», 3 juin 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html
[25] NTC, rapport de synthèse sur la cybersécurité des périphériques: https://fr.ntc.swiss/news/2026-rapport-peripheriques
[26] NTC, rapport sur la cybersécurité des appareils connectés au regard de la directive RED: https://fr.ntc.swiss/news/2025-rapport-red

5.2 Deux perspectives sur la menace

Les constats doivent être lus à la lumière de deux perspectives de menace fondamentalement différentes:

- **L'exposition aux attaques de tiers**: des vulnérabilités techniques qu'un attaquant externe exploite. Ce type de vulnérabilité se rencontre chez tous les fabricants et peut être réduite par une meilleure qualité des produits et des tests indépendants.
- **Le fabricant ou sa chaîne d'approvisionnement comme attaquant:** il ne s'agit pas ici de vulnérabilités techniques, mais de dépendances. Les moyens légitimes de la maintenance à distance et de la distribution du micrologiciel peuvent être détournés par le fabricant lui-même, par un attaquant qui compromet le fabricant, par des collaborateurs malveillants ou en vertu d'une injonction étatique adressée au fabricant. Ce risque est propre à chaque fabricant et ne peut pas être corrigé par des mesures techniques de sécurité. Il ne peut être réduit qu'en diminuant la dépendance elle-même: par des engagements vérifiables plutôt que par la simple confiance, par la diversification et par une limitation technique de ce qui est possible à distance (cf. chapitre *7.6*).

Ces deux perspectives se retrouvent dans les constats qui suivent. Cette distinction n'a rien d'inhabituel. Le BSI allemand mentionne expressément, dans sa prise de position[27] sur la cybersécurité dans le secteur de l'énergie, la «manipulation de l'infrastructure énergétique par les fabricants ou des tiers» parmi les nouveaux vecteurs d'attaque, en citant les onduleurs comme exemple.

5.3 Résultats de l'analyse technique

5.3.1 Clouds des fabricants

Pour les attaques à effet d'échelle, le niveau du cloud est le plus lourd de conséquences. Un cloud gère tout un parc d'appareils, raison pour laquelle une seule vulnérabilité y concerne potentiellement un grand nombre d'installations, contrairement à une faille sur un appareil isolé.

C'est toutefois précisément ce niveau qui n'a pu être testé que de manière restreinte. Tester le cloud d'un fabricant implique d'accéder à un système tiers exploité en production; sans le consentement de l'exploitant, de tels tests ne sont admissibles que sous certaines conditions au sens de l'art. 143bis CP[28]. Obtenir un tel consentement aurait signifié associer les fabricants à l'étude, ce qui aurait contredit le principe d'indépendance. Les tests se sont donc limités au cadre admissible sans consentement. Le résultat n'en est que plus remarquable: même dans ce cadre étroit, des vulnérabilités ont été trouvées dans plusieurs clouds de fabricants, notamment des vulnérabilités des catégories injection SQL et cross-site scripting. Les fabricants les ont corrigées après le signalement.

Un problème structurel apparaît en même temps: le niveau ayant le plus grand effet de levier est précisément celui que des organismes de test indépendants ne peuvent pas examiner entièrement sans le concours du fabricant.

Un constat issu de ces tests est instructif à plus d'un titre. Une vulnérabilité classée comme critique concernait le système de gestion de l'énergie du fabricant suisse Solar Manager. Elle aurait permis à un attaquant d'accéder à distance à des systèmes individuels, non pas toutefois à un seul, mais successivement à d'autres systèmes. Le fabricant a réagi de manière exemplaire et a comblé la faille en quelques heures. Il a en outre donné au NTC son consentement pour tester également son cloud. La barrière juridique décrite plus haut, qui rend normalement difficile un test du niveau cloud, a ainsi disparu. Le cas montre que cette barrière peut se lever lorsqu'un fabricant voit dans la transparence une opportunité. Contrairement au reste du rapport, nous

[27] Bundesamt für Sicherheit in der Informationstechnik (BSI), «Positionspapier: Cybersicherheit im Energiesektor Deutschlands»: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Positionspapier_Cybersicherheit_Energiesektor.html

[28] Walder Wyss SA, avis de droit «Responsabilité pénale de l'Ethical Hacking»: https://www.walderwyss.com/fr/news/2023-06-26_rechtsgutachten-zur-strafbarkeit-von-fuer-das-nationale-testinstitut-fuer-cybersicherheit-ntc

nommons ici le fabricant, avec son accord et comme exemple positif de la manière de traiter ce signalement de vulnérabilité.

Le cas est instructif pour une deuxième raison encore. Solar Manager est surtout répandu dans la région DACH, avec, selon les estimations, environ 50 000 installations. Les produits présentant une telle diffusion régionale n'apparaissent en règle générale pas dans les études internationales, qui proviennent le plus souvent des États-Unis ou d'entreprises de sécurité actives à l'échelle mondiale. Ils passent entre les mailles du filet, bien qu'ils commandent des dizaines de milliers d'installations dans notre pays. Cette lacune ne peut être comblée que par des tests qui s'appuient sur la réalité du marché suisse.

Un cas documenté à l'échelle internationale montre l'ampleur que peut atteindre l'effet de levier d'un seul cloud et la difficulté que peut représenter la correction[29]. Le Dutch Institute for Vulnerability Disclosure (DIVD), qui recherche et signale des vulnérabilités de manière analogue au NTC, est tombé, sur la plateforme de monitoring Solarman, sur des identifiants d'un compte d'administration qui se trouvaient en clair dans un dépôt logiciel public (GitHub) et n'étaient pas protégés par un deuxième niveau de sécurité (authentification multifacteur). Par ce seul compte, près d'un million d'installations dans le monde, totalisant plus de 10 GW de puissance, pouvaient être consultées et commandées, jusqu'à la lecture et l'écrasement du micrologiciel. La manière dont le cas a été traité est révélatrice: l'exploitant n'a pas réagi pendant des mois, après une première correction, le mot de passe exposé a même été rétabli à la valeur divulguée, et une solution n'a été trouvée que par des canaux diplomatiques et l'implication du CERT chinois. Le cas illustre ainsi deux schémas à la fois: la portée énorme d'un cloud central et la collaboration parfois difficile, en pratique, avec les fabricants lors de la correction. Aux Pays-Bas, il a ensuite donné lieu à des questions parlementaires et à une attention accrue des autorités pour la cybersécurité des onduleurs. Qu'il ne se soit pas agi d'un cas isolé, une divulgation ultérieure et nettement plus vaste le montre[30]: en 2024, l'entreprise de sécurité Bitdefender a trouvé, dans ces mêmes plateformes Solarman et Deye, de nouvelles vulnérabilités qui, selon des articles de presse, auraient théoriquement concerné un parc encore plus grand (environ 195 GW de puissance répartis sur plus de deux millions d'installations).

5.3.2 Interfaces locales et accès des fabricants

Les autres constats se répartissent en catégories récurrentes. Les plus fréquents, et sur de nombreux appareils testés, étaient des défauts d'authentification et de contrôle d'accès (par exemple une expiration de session manquante ainsi que des mots de passe par défaut absents ou inchangés), auxquels s'ajoutait l'absence ou la faiblesse du chiffrement des interfaces locales. D'autres constats concernaient des interfaces impossibles à désactiver (par exemple un hotspot Wi-Fi qu'on ne peut pas éteindre) ainsi que des accès de maintenance à distance des fabricants non sécurisés (SSH, en partie avec des identifiants identiques pour tout le parc).

Des études indépendantes confirment qu'il ne s'agit pas de cas isolés. Dans l'étude SUN:DOWN[31], Forescout a documenté des faiblesses comparables chez plusieurs leaders du marché (notamment des interfaces cloud non sécurisées, des identifiants inscrits en dur dans l'appareil et non modifiables ainsi que des mises à jour du micrologiciel sans signature cryptographique). Le chercheur Ruben Santamarta, spécialisé dans la cybersécurité du secteur de l'énergie, décrit[32] des accès de maintenance à distance non sécurisés chez des fabricants européens.

Un constat montre particulièrement bien à quel point de tels accès de maintenance sont parfois peu protégés. Sur un appareil, il était possible, par le point d'accès Wi-Fi de l'appareil lui-même, de réinitialiser et de redéfinir le mot de passe du compte installateur sans aucune authentification. Les droits administratifs ainsi obtenus permettaient ensuite d'activer l'accès à

[29] Dutch Institute for Vulnerability Disclosure (DIVD), cas «Solarman» (DIVD-2022-00009): https://csirt.divd.nl/cases/DIVD-2022-00009/
[30] Bitdefender, étude sur des vulnérabilités dans les plateformes Solarman et Deye, août 2024: https://blogapp.bitdefender.com/labs/content/files/2024/08/Bitdefender-PReport-solarman-creat7907.pdf
[31] Forescout (dos Santos et al.), «SUN:DOWN»: https://www.forescout.com/research-labs/sun-down-a-dark-side-to-solar-energy-grids/
[32] Santamarta, «Cyber-Physical Attacks on Solar Inverters», mai 2026: https://www.reversemode.com/2026/05/a-practical-analysis-of-cyber-physical.html

distance (SSH) et l'accès root. Celui-ci est protégé, dans l'état à la livraison, par un mot de passe par défaut qui doit être changé lors de la première connexion. En exploitation normale, l'accès reste toutefois inutilisé, et le mot de passe par défaut reste donc en vigueur. La première personne qui se connecte définit elle-même le nouveau mot de passe. Pour la compromission complète, un accès au Wi-Fi de l'appareil suffisait.

L'enchaînement est révélateur: trois mécanismes de protection sont présents: une authentification au compte, un accès à distance désactivable et un changement de mot de passe lors de la première connexion. Aucun ne joue son rôle, parce que le premier peut être contourné sans authentification et que le troisième n'agit que si quelqu'un se connecte, ce que l'on ne peut pas présumer.

D'autres vulnérabilités ne sont apparues qu'à l'analyse du micrologiciel des appareils. Sur un produit, des services ont été trouvés qui s'exécutent avec les droits les plus élevés et traitent des entrées avant même qu'une connexion ait eu lieu. Dans un cas, un service de débogage était encore actif dans le micrologiciel livré, qui copie sans vérification un paramètre d'une requête réseau dans une zone mémoire de taille fixe (buffer overflow). Comme ce service s'exécute avec les droits les plus élevés, un tel débordement permet d'introduire et d'exécuter son propre code. Sans identifiants et avec un simple accès au réseau local, le contrôle complet de l'appareil était ainsi atteignable (accès root). Il est remarquable que ce service ne soit pas nécessaire en exploitation et qu'il ait néanmoins été accessible dans le micrologiciel livré. C'est précisément ce que vise le principe formulé par les lignes directrices citées au chapitre *8.4.2 Verrouillage en usine de la commande des fonctions pertinentes pour le réseau*: ce qui n'est pas nécessaire dans chaque mode d'utilisation devrait être désactivé en usine.

L'interface de commande locale est particulièrement lourde de conséquences. Sur presque tous les onduleurs testés, elle permet non seulement de lire des valeurs de mesure, mais aussi de modifier les réglages de l'appareil pertinents pour le réseau, et cela souvent sans authentification. Techniquement, cela se fait par le protocole industriel Modbus. Que le fabricant utilise pour cela les modèles de registres normalisés SunSpec ou un schéma propre n'y change rien: SunSpec[33] ne décrit que la signification des registres et n'est pas une couche de sécurité. Cette interface est désactivée en usine chez plusieurs fabricants. Pour l'exploitation avec un système de gestion de l'énergie, elle doit toutefois être activée. Lorsqu'elle est active, l'accès se fait sans aucune authentification, de sorte que tout appareil du même réseau peut envoyer des commandes. Entre le système de gestion de l'énergie et l'onduleur, il n'existe ainsi très souvent aucune protection.

Tous les constats décrits dans cette section ont en commun de supposer un accès au réseau local. Ils permettent le contrôle complet d'un appareil isolé, non d'un grand nombre d'appareils.

5.3.3 De l'attaque locale à l'attaque à effet d'échelle

Prises en elles-mêmes, les vulnérabilités locales ne concernent que l'installation individuelle et n'ont pas d'effet d'échelle. Une considération relativise toutefois ce constat rassurant: un attaquant qui se trouve déjà dans le réseau local peut commander des onduleurs par le protocole Modbus TCP non sécurisé. L'effet peut même être obtenu, de par la conception, sans vulnérabilité. Un attaquant accède au réseau local par exemple par des appareils IoT infectés. Que des appareils domestiques soient compromis à grande échelle, tant les botnets classiques composés d'ordinateurs et d'appareils IoT infectés (par exemple du type Mirai) que la progression rapide des Residential Proxy Networks, où des connexions domestiques détournées sont louées à des tiers comme nœuds d'accès, le montrent.[34] Le SRC décrit lui aussi des réseaux d'anonymisation composés d'appareils domestiques mal protégés et exposés à Internet, comme des routeurs, en partie sur une infrastructure louée en Suisse.[35] Si de nombreux réseaux domestiques sont compromis de cette manière, un vecteur local devient un vecteur à large

[33] SunSpec Alliance, spécification «Modbus»: https://sunspec.org/modbus/
[34] BSI, rapport sur l'abus de residential proxies, «Steckbriefe aktueller Botnetze: Mirai», 2026: https://www.bsi.bund.de/dok/12820010
[35] Service de renseignement de la Confédération (SRC), «La sécurité de la Suisse 2026»: https://www.vbs.admin.ch/fr/newnsb/jyRmuld1hBVy

portée.

5.3.4 Ce qui n'a pas été examiné: l'endommagement durable des appareils

La possibilité d'endommager durablement des appareils en les faisant fonctionner dans certains états n'a pas fait l'objet de la présente étude. Le cas Hoymiles montre qu'il ne s'agit pas là d'un danger purement hypothétique. Des chercheurs du Chaos Computer Club ont démontré en 2026 que des micro-onduleurs peuvent être rendus définitivement inutilisables par le protocole radio non sécurisé, en y introduisant un micrologiciel manipulé.[36] Sur quatre appareils, le NTC a obtenu le contrôle complet de l'appareil (accès root, le niveau de privilèges le plus élevé), mais n'a pas testé un endommagement durable. D'autres mécanismes de protection peuvent en outre intervenir, par exemple au niveau de l'électronique. Une telle attaque aurait, contrairement à une perturbation passagère du réseau, des conséquences à long terme.

5.3.5 Ce qui n'a pas été trouvé

Ce qui n'a pas été observé est tout aussi important que les vulnérabilités identifiées. Aucun indice n'a été trouvé de portes dérobées intentionnellement intégrées ou de composants de communication cachés et non documentés, tels qu'ils sont discutés dans les médias internationaux.[37] Un microphone a certes d'abord été découvert dans un appareil, ce qui a donné lieu à des clarifications. L'analyse a toutefois révélé une fonction de commande documentée (interaction par tapotements) et aucun indice d'une fonction cachée. Le cas n'est pas réglé pour autant: le composant peut capter davantage que ne l'exige la commande et pourrait, après une mise à jour du micrologiciel, être détourné. Comme la même fonction serait aussi possible sans microphone, ce choix doit être considéré comme une vulnérabilité, indépendamment de toute intention malveillante. C'est précisément là le schéma du rapport: les risques constatés sont de nature structurelle et n'exigent pas de supposer une intention malveillante pour être sérieux.

5.4 Risques structurels

Le message central de ce rapport ne réside pas dans les constats individuels, mais dans cinq risques structurels qui existent indépendamment de la qualité des différents produits.

5.4.1 Dépendance au cloud du fabricant

La commandabilité centrale décrite au chapitre «L'écosystème d'une installation photovoltaïque» est voulue sur le plan fonctionnel, mais déplace le contrôle sur un grand nombre d'installations vers un point unique. Il en résulte un risque en cas de dysfonctionnement ou si le fabricant est compromis, et, dans un cas extrême, la possibilité d'une utilisation comme moyen de pression géopolitique. La dépendance est renforcée par le fait que de nombreux appareils sont reliés en permanence au cloud, une situation en partie encouragée par des incitations telles que des garanties prolongées. Le canal de mise à jour du micrologiciel relève du même niveau: il est nécessaire, mais agit lui aussi simultanément sur l'ensemble du parc, et ce qui est distribué par ce canal modifie l'appareil en profondeur.

L'attaque contre le réseau satellitaire KA-SAT de février 2022 a montré que ce canal a effectivement été exploité. Les attaquants ont accédé au serveur par lequel les mises à jour logicielles sont distribuées aux modems et ont diffusé par ce biais un logiciel malveillant qui a écrasé la mémoire des appareils. La surveillance à distance de 5 800 éoliennes du fabricant Enercon, totalisant 11 gigawatts, a notamment été touchée. Les installations ont continué

[36] Chaos Computer Club (B. Heinz «Hunz»), «Analyse der Funk- und Firmware-Schwachstellen von Hoymiles-Wechselrichtern», 2026: https://www.ccc.de/updates/2026/blinkenlights-hoymiles
[37] Reuters, articles sur des modules de communication non documentés, mai 2025: https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/

d'injecter, mais ne pouvaient plus être surveillées ni réinitialisées à distance. L'attaque visait l'Ukraine, les installations allemandes ont constitué un dommage collatéral, soit exactement le scénario que le SRC tient également pour possible en ce qui concerne la Suisse (cf. chapitre 2.5).[38]

5.4.2 Accès de maintenance à distance privilégié

Indépendamment du cloud, la plupart des fabricants conservent un accès privilégié à leur parc d'appareils, par exemple par des comptes de maintenance ou des accès à distance. Ce n'est pas une erreur isolée, mais un principe de conception: un seul mécanisme d'accès compromis ou reconstituable concerne potentiellement l'ensemble du parc, et un tel accès ne peut pas être corrigé comme une vulnérabilité ordinaire. Sont également concernées les grandes installations qui ne sont pas raccordées à un cloud de fabricant, mais disposent d'interfaces de commande et de maintenance propres, accessibles à distance. Le cas des onduleurs Deye a montré en novembre 2024 à quel point cette possibilité est réelle: dans le cadre d'un litige de distribution, le fabricant a désactivé de manière ciblée, dans plusieurs pays, de nombreux appareils de sa marque distribués sans autorisation, et cela sans aucune vulnérabilité.[39]

Le même schéma va au-delà du fabricant: les entreprises d'installation, les prestataires de services et les agrégateurs disposent eux aussi souvent d'un accès à distance à toutes les installations dont ils s'occupent, sans qu'aucune prescription de cybersécurité ne leur soit applicable. Une attaque ciblée contre le prestataire de maintenance de Brême Deutsche Windtechnik, qui s'occupe de plus de 7 600 éoliennes, a montré en avril 2022 l'ampleur du phénomène: l'entreprise a alors coupé toutes les liaisons de télésurveillance, de sorte qu'aucune surveillance à distance n'a plus été possible pendant un à deux jours. Les installations elles-mêmes n'étaient pas touchées.[40] Ce n'est ni un fabricant ni un exploitant qui a été attaqué, mais le prestataire situé entre les deux.

5.4.3 Protocoles de commande locaux non sécurisés comme caractéristique de conception

La commande locale de nombreux onduleurs repose sur des protocoles industriels répandus qui ne prévoient pas d'authentification. Ce n'est pas un défaut de certains appareils, mais la norme de fait de toute une catégorie d'appareils. Le risque est aggravé par le déplacement de cette commande, qui passe de liaisons à accès physiquement restreint (RS485) à des interfaces en réseau (Ethernet, Wi-Fi), car tout appareil du même réseau devient ainsi un émetteur possible de commandes.

5.4.4 La concentration du marché comme risque de concentration

La concentration décrite au chapitre «L'écosystème d'une installation photovoltaïque» agit, sur le plan de la sécurité, comme un «Single Point of Failure»: plus la part d'un fabricant est grande, plus un constat unique peut toucher d'appareils. Une appréciation de l'entreprise de cybersécurité néerlandaise Secura montre à quel point ce risque est concret: aux Pays-Bas, deux fabricants (Huawei et Sungrow) détiennent chacun à lui seul une part de marché si grande qu'une attaque contre les systèmes d'un seul d'entre eux suffirait pour atteindre l'ordre de grandeur nécessaire à un effet sur le réseau. À l'échelle européenne, plusieurs fabricants dépasseraient ce seuil selon Secura.[41]

[38] SentinelOne: «AcidRain – A Modem Wiper Rains Down on Europe», 31 mars 2022: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
[39] Articles sur des onduleurs Deye désactivables à distance, 2024: https://www.heise.de/news/Photovoltaik-Deaktivierte-Deye-und-Sol-Ark-Wechselrichter-in-den-USA-10183706.html
[40] heise online, «Cyber-Angriff: Fernüberwachung von Windkraftanlagen lahmgelegt», 27 avril 2022: https://www.heise.de/news/Cyber-Angriff-legte-offenbar-Windturbinen-lahm-7066606.html
[41] Secura, «Cybersecurity threats and measures for the solar power sector», 2024: https://www.energy-innovation.nl/documents/1299/2024-Secura_Report-Cybersecurity_threats_and_measures_for_the_solar_power_sector.pdf

5.4.5 Localisation et origine: une sécurité apparente

Différents fabricants font valoir que leur cloud est exploité dans des centres de calcul européens et administré par des organisations européennes. Le lieu d'hébergement seul dit toutefois peu de chose du contrôle effectif sur l'appareil, notamment parce que le micrologiciel et les logiciels proviennent du fabricant et ne sont pas développés sur le lieu d'hébergement. Les tests du NTC ont certes confirmé que le trafic de données observé allait vers des points de terminaison de l'UE. On ne peut pas en déduire un contrôle exclusivement européen ni une conservation des données exclusivement en Europe. L'origine de l'appareil ne résout pas davantage le problème: les appareils de fournisseurs européens contiennent eux aussi souvent des puces ou des composants logiciels provenant d'États tiers, ou y sont fabriqués.

6 Effets sur la stabilité du réseau

6.1 Principe de base: l'équilibre entre production et consommation

Un réseau à courant alternatif doit être exploité en permanence près de sa fréquence nominale (50 Hz en Europe). Cela suppose un équilibre en temps réel entre production et consommation. Si la fréquence s'écarte, des réserves échelonnées interviennent dans le réseau interconnecté européen: une réserve primaire qui se déclenche en quelques secondes (environ 3 000 MW), ainsi qu'une réserve secondaire et une réserve tertiaire aux temps de mobilisation plus longs.[42] Un saut de puissance soudain dépassant l'incident de référence de 3 000 MW ne peut plus être absorbé par la seule réserve primaire. À 49 Hz, un délestage est déclenché conformément à la réglementation.[43]

Un facteur structurel aggravant est le recul de l'inertie du réseau. Les centrales classiques stabilisent la fréquence par les masses tournantes de leurs générateurs, alors que la production à base d'onduleurs ne fournit pas cette inertie d'elle-même.[44] Les onduleurs modernes sont censés compenser cela de plus en plus par des fonctions de formation de réseau («grid-forming»). Cet aspect est repris plus loin, au sujet des facteurs atténuants.

6.2 Faits avérés: le réseau peut basculer même sans cyberattaque

Le blackout ibérique du 28 avril 2025 a montré à quel point un système peut être fragile lorsque la production à base d'onduleurs est élevée, et cela sans participation malveillante. Une part très élevée de l'électricité provenait par moments de sources renouvelables. Une chaîne de problèmes de tension et de puissance réactive, une grandeur qui contribue au soutien du réseau et à la détermination de sa tension et qui est expliquée plus en détail plus loin, sous le type B, a conduit à une montée rapide de la tension, à des déconnexions en cascade de la production et finalement à l'effondrement complet du système en Espagne et au Portugal. Pour garder le sens des proportions, l'attribution des causes par ENTSO-E, l'association des gestionnaires de réseau de transport européens, est importante: ce n'est pas un «trop-plein» de production renouvelable qui a été déterminant, mais des lacunes dans le réglage de la tension et de la puissance réactive.[45]

Que de nombreuses installations configurées de la même manière réagissent simultanément n'est pas une expérience de pensée. En Allemagne, une directive de 2005 prescrivait que les installations photovoltaïques se déconnectent immédiatement du réseau à une fréquence de réseau de 50,2 Hz. Avec l'essor du photovoltaïque, cela est devenu un risque systémique: si cette fréquence avait été atteinte, des installations totalisant plusieurs gigawatts de puissance se seraient déconnectées d'un seul coup. L'ordonnance allemande sur la stabilité du système, de 2012, a donc obligé les gestionnaires de réseau à mettre à niveau environ 300 000 installations existantes comportant environ un million d'onduleurs, afin que la déconnexion se fasse de manière échelonnée et non simultanée.[46]

6.3 Trois types d'attaque à partir d'un onduleur compromis

L'idée répandue selon laquelle une attaque consisterait en une «mise en marche et un arrêt» massifs est réductrice. Le chercheur en sécurité Ruben Santamarta distingue trois types

[42] Goerke et al., Karlsruher Institut für Technologie, «Who Controls Your Power Grid? On the Impact of Misdirected Distributed Energy Resources on Grid Stability», 2024: https://publikationen.bibliothek.kit.edu/1000173186
[43] Règlement (UE) 2017/2196 de la Commission du 24 novembre 2017 établissant un code de réseau sur l'état d'urgence et la reconstitution du réseau électrique, article 15 (délestage automatique en sous-fréquence) et annexe: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32017R2196
[44] ENTSO-E: «Frequency stability in long-term scenarios», étude sur le recul de l'inertie du système dans la zone synchrone d'Europe continentale, décembre 2021: https://www.entsoe.eu/news/2021/12/06/entso-e-assesses-the-impact-of-reduction-of-inertia-on-frequency-stability-in-long-term-scenarios/
[45] ENTSO-E, «Expert Panel Final Report on 28 April 2025 Blackout in Spain and Portugal»: https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/
[46] BDEW, problème des 50,2 hertz: https://www.bdew.de/energie/systemstabilitaetsverordnung/502-hertz-problem/

d'attaques cyber-physiques de complexité croissante.[47]

6.3.1 Type A: puissance active et fréquence (connexion et déconnexion)

En déconnectant ou en connectant de manière concertée de nombreuses installations, l'équilibre entre production et consommation est perturbé et la fréquence s'écarte de sa valeur nominale. Cela peut être obtenu par des ordres de déconnexion directs, par la manipulation de la fonction de protection qui déconnecte automatiquement une installation du réseau en cas de défaillance du réseau (anti-islanding), ou par des consignes modifiées quant à la tension à laquelle une installation doit rester connectée au réseau ou s'en déconnecter (les courbes de tenue HVRT et LVRT, «High/Low Voltage Ride-Through»). Une attaque est particulièrement efficace lorsqu'elle répète la manipulation au rythme de la régulation du réseau et amplifie ainsi l'oscillation, comme lorsqu'on pousse une balançoire au bon rythme.

Un phénomène issu de l'exploitation du marché montre que la simultanéité a un effet sur le réseau même sans attaque. Lorsque de nombreuses installations adaptent brusquement leur injection au changement d'intervalle de marché, des écarts de fréquence apparaissent à chaque changement d'heure ou de quart d'heure, connus sous le nom de «deterministic frequency deviations». Swissgrid entend donc prescrire que les installations photovoltaïques effectuent elles aussi de telles modifications planifiées en suivant une rampe. Un attaquant qui connecte ou déconnecte simultanément de nombreuses installations exploite le même effet, mais intentionnellement et sans rampe.[48]

6.3.2 Type B: puissance réactive et tension

C'est, selon l'appréciation de Santamarta, le moyen le plus efficace de provoquer des pannes locales. Les onduleurs soutiennent le réseau non seulement avec de la puissance active, mais aussi avec de la puissance réactive, qui contribue à déterminer la tension dans le réseau. La manière dont un onduleur doit réagir est fixée par des courbes caractéristiques, par exemple la courbe Volt-Var: si la tension monte, l'onduleur absorbe de la puissance réactive et abaisse à nouveau la tension. Cela stabilise le réseau. Une attaque inverse cette réaction. Une courbe caractéristique manipulée contraint l'onduleur à injecter en plus de la puissance réactive alors que la tension est déjà élevée, et à faire ainsi monter la tension davantage. Quelques installations suffisent déjà pour que la tension locale dépasse les limites admissibles; les dispositifs de protection d'installations et de sous-stations voisines peuvent se déclencher et amorcer une cascade. Quant à la plausibilité: par une logique de commande modifiée, par exemple après une compromission du micrologiciel, une telle inversion est plausible. L'attaque n'a besoin ni de code malveillant complexe ni d'une grande échelle. Les simulations de réseau que DNV a réalisées sur mandat de SolarPower Europe avec les modèles de réseau d'ENTSO-E aboutissent à la même conclusion:[49] si de grandes capacités sont commutées simultanément entre puissance réactive inductive et capacitive, des sauts de tension rapides apparaissent, qui peuvent déclencher les dispositifs de protection d'installations de production et de sous-stations voisines et provoquer une cascade. L'étude retient en même temps qu'il reste incertain à quelle vitesse et dans quelle mesure les mécanismes existants de maintien de la tension pourraient compenser cet effet.

6.3.3 Type C: instabilité induite par les convertisseurs (oscillations)

L'excitation ciblée d'oscillations propres au réseau, jusqu'à des oscillations forcées, est le vecteur le plus complexe. Il est considéré, y compris selon l'appréciation de Santamarta lui-même, comme actuellement irréaliste, en particulier sous la forme d'une attaque coordonnée utilisant une multitude de petits onduleurs domestiques hétérogènes. En tant que phénomène, il est

[47] Santamarta, «Cyber-Physical Attacks on Solar Inverters», mai 2026: https://www.reversemode.com/2026/05/a-practical-analysis-of-cyber-physical.html
[48] Swissgrid SA, white paper «Intégration du photovoltaïque compatible avec le système», mars 2026: https://www.swissgrid.ch/fr/home/newsroom/blog/2026/20260330-01.html
[49] SolarPower Europe / DNV: «Solutions for PV Cyber Risks to Grid Stability», 2025: https://www.solarpowereurope.org/insights/thematic-reports/solutions-for-pv-cyber-risks-to-grid-stability

néanmoins réel. Lors du blackout ibérique, une oscillation forcée provenant d'une seule grande centrale photovoltaïque (selon l'analyse de Santamarta, l'installation Núñez de Balboa), et non d'installations décentralisées de petite taille, a excité une oscillation suprarégionale.[50]

6.3.4 Mise en perspective: le vecteur le plus dangereux n'est pas le plus élaboré

Ce qui surprend ici: le vecteur le plus dangereux n'est pas le plus élaboré. Face à de simples pertes de production, le réseau est comparativement robuste. L'attaque par la tension au moyen de la puissance réactive ne nécessite en revanche qu'une ampleur limitée et une faible complexité, ce qui rend la menace plus réelle, comme le montre le blackout ibérique précisément à ce niveau (cf. chapitre *6.2*).

6.4 Le scénario cyber: manipulation coordonnée de la charge et de la production

L'idée que des appareils compromis et reliés à Internet puissent être regroupés en un ensemble ayant un effet sur le réseau est établie dans la recherche depuis environ une décennie (sous les termes «load-altering» et MaDIoT, «Manipulation of Demand via IoT»). Les travaux vont des premiers modèles de Dabrowski et al.[51] (2017) et Soltan et al.[52] (2018) jusqu'à Goerke et al.[53] (2024), qui quantifient en détail combien d'installations de chaque type seraient nécessaires pour un effet sur le réseau interconnecté européen. La première formulation spécifiquement photovoltaïque de cette idée de base provient du «scénario Horus»[54] de Willem Westerhof, publié en août 2017 et fondé sur un signalement au fabricant datant de décembre 2016.

Les onduleurs se prêtent particulièrement bien à de telles attaques, car, en tant que systèmes temps réel, ils suivent précisément la fréquence du réseau et peuvent de ce fait mener une attaque avec une grande précision.

Au-delà de la seule déstabilisation du réseau, il faut mentionner un deuxième type de dommage. Des attaquants disposant d'un accès étendu peuvent mettre durablement hors service des appareils au moyen d'un micrologiciel malveillant, de sorte qu'ils doivent être remplacés ou reprogrammés sur place. Une extorsion est également concevable («ransomware sur les onduleurs»). De tels effets destructifs auraient des conséquences nettement plus durables qu'une perturbation passagère du réseau.

6.5 Ordre de grandeur (calcul approximatif à titre illustratif)

À titre de mise en perspective, et expressément non comme prévision autonome de blackout, l'ordre de grandeur peut être déduit de la littérature. Selon Dabrowski et al., dans des conditions favorables à un attaquant, le contrôle d'environ 4 500 MW suffit pour faire descendre la fréquence du réseau interconnecté européen sous le seuil de délestage de 49 Hz, soit une fois et demie la puissance de l'incident de référence. Cette valeur vaut pour une attaque qui module la puissance au rythme du réglage du réseau et amplifie ainsi l'écart; un saut de puissance unique devrait, dans les mêmes conditions de réseau, atteindre environ 6 000 MW. Le seuil désigne un déséquilibre de puissance qui peut être atteint aussi bien du côté de la consommation que du côté de la production: Dabrowski le déduit du côté de la charge, Goerke et al. ainsi que dos Santos et al. le transposent au photovoltaïque. Pour le photovoltaïque, cela signifie concrètement une journée ensoleillée à faible charge, par exemple un week-end d'été ou un jour

[50] ENTSO-E, «Expert Panel Final Report on 28 April 2025 Blackout in Spain and Portugal»: https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/
[51] Dabrowski, Ullrich, Weippl, «Grid Shock: Coordinated Load-Changing Attacks on Power Grids», 2017: https://dl.acm.org/doi/10.1145/3134600.3134639
[52] Soltan, Mittal, Poor, «BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid», 2018: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan
[53] Goerke et al., Karlsruher Institut für Technologie, «Who Controls Your Power Grid? On the Impact of Misdirected Distributed Energy Resources on Grid Stability», 2024: https://publikationen.bibliothek.kit.edu/1000173186
[54] Westerhof, «Horus Scenario», 2017: https://horusscenario.com/

férié.

Pour situer: 4 500 MW correspondent à un peu moins de la moitié des 9,5 GW installés en Suisse. Le seuil est donc européen et non suisse. À l'échelle européenne, en revanche, une faible proportion suffit: rapportés au parc installé dans l'UE fin 2025, d'environ 406 GW, 4 500 MW représentent un peu plus d'un pour cent, et même la variante conservatrice de 6 000 MW reste en dessous de deux pour cent; cette part diminue à mesure que le parc continue de croître.[55] Une simulation indépendante aboutit à un ordre de grandeur similaire: pour le réseau européen, DNV cite une compromission ciblée de 3 GW comme seuil à partir duquel des effets considérables sont possibles.[56]

Pour la Suisse, il n'en découle aucun motif de se rassurer, mais une autre question: dans quelle mesure le parc suisse est regroupé sur des points de commande uniques. Comme un seul fabricant détient un peu plus de la moitié du marché (cf. chapitre *3.6*), un seul cloud de fabricant atteint déjà une part considérable et croissante du parc suisse. Un regroupement analogue résulte des agrégateurs et des centrales électriques virtuelles (cf. chapitre *3.4*). Pour une attaque coordonnée à l'échelle européenne, ce n'est pas la somme nationale qui est déterminante, mais le nombre de plateformes par lesquelles elle est accessible.

Un calcul indépendant et robuste pour le réseau suisse se situe en dehors du périmètre de l'étude. L'affirmation centrale reste solide: une part de moins de deux pour cent du parc européen d'onduleurs suffit déjà, selon ces calculs, pour déclencher des effets significatifs sur le réseau, la valeur concrète dépendant fortement de la répartition des appareils et de l'état du réseau. Selon Santamarta, le vecteur de la puissance réactive (type B) nécessite nettement moins de puissance contrôlée, mais agit localement et non de manière suprarégionale.

6.6 Précédent réel: Pologne, 29 décembre 2025

Une cyberattaque coordonnée a touché plus de 30 parcs éoliens et solaires ainsi qu'une centrale de cogénération et une entreprise industrielle. Dans les installations renouvelables, les communications avec les gestionnaires de réseau de distribution ont été interrompues. La production d'électricité elle-même n'a pas été affectée, et le gestionnaire de réseau de transport n'a à aucun moment considéré la stabilité du système polonais comme menacée. La production a certes continué, mais elle était découplée des exigences du réseau. Le gestionnaire de réseau de transport polonais a retenu que des irrégularités avaient été observées et corrigées dans l'exploitation de petits producteurs d'électricité, mais que le système avait pu être équilibré avec les moyens disponibles. Le logiciel malveillant utilisé était destructif (wiper). Le rapport de l'organisme compétent compare les attaques à un incendie criminel.

L'importance de l'incident ne réside pas dans un blackout évité de justesse, mais dans le fait qu'un acteur compétent a obtenu de manière avérée l'accès au niveau de commande (Operational Technology, OT) de nombreux parcs renouvelables et a montré une intention destructrice. Le scénario perd ainsi son caractère purement théorique. Le 13 juillet 2026, le Royaume-Uni et l'UE ont officiellement attribué l'attaque au service de renseignement russe FSB (Centre 16) et ont adopté un train de sanctions commun. Selon l'appréciation britannique, l'attaque aurait pu, en hiver, priver d'électricité environ 500 000 personnes.[57] La documentation technique est fournie par CERT Polska.[58]

6.7 Appréciation de spécialistes indépendants

Le danger est pris au sérieux également en dehors des organismes étatiques. Le DIVD néerlandais (cf. chapitre *5*) examine dans le cadre de son propre programme les onduleurs, les

[55] SolarPower Europe, «EU Solar Market Outlook 2025-2030», décembre 2025: https://www.solarpowereurope.org/insights/outlooks/eu-solar-market-outlook-2025-2030
[56] SolarPower Europe / DNV: «Solutions for PV Cyber Risks to Grid Stability», 2025: https://www.solarpowereurope.org/insights/thematic-reports/solutions-for-pv-cyber-risks-to-grid-stability
[57] OFSI/GOV.UK, communiqué de sanctions du 13 juillet 2026: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions
[58] CERT Polska, «Energy Sector Incident Report – 29 December»: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

bornes de recharge, les systèmes de mesure intelligents et, de plus en plus, les systèmes de gestion de l'énergie. En juillet 2026, à la suite de l'attaque en Pologne, des spécialistes ont averti publiquement que, dans le scénario le plus grave, une attaque réussie pourrait entraîner des pannes d'électricité étendues et persistantes pendant plusieurs jours.[59]

6.8 Facteurs atténuants

Le réseau n'est pas sans défense. Des réserves échelonnées, des systèmes de protection et l'inertie encore présente absorbent de nombreuses perturbations, et une manipulation ne déclenche pas nécessairement une cascade. L'hétérogénéité du parc, avec ses nombreux fabricants, versions de micrologiciel et configurations, rend en outre difficile un exploit unique valable pour plusieurs fabricants. À l'intérieur d'un cloud de fabricant dominant, la concentration reste toutefois réelle, et en Suisse elle est marquée (cf. chapitre *3).*

En même temps, l'inertie du réseau diminue avec le recul des centrales classiques. Les onduleurs formant le réseau sont censés compenser cela. Mais si ce sont précisément ces onduleurs qui constituent la cible de l'attaque, la composante de stabilisation disparaît en même temps que la production. Dans l'ensemble, le niveau de protection de base devrait s'élever grâce aux mises à jour régulières fournies par les fabricants ainsi qu'à la réglementation européenne des produits, actuelle et à venir (RED, CRA). Les risques structurels et géopolitiques ne sont toutefois pas écartés pour autant.

[59] Dutch Institute for Vulnerability Disclosure (DIVD), avertissement public sur la vulnérabilité du réseau électrique (Chris van 't Hof), juillet 2026: https://www.nu.nl/klimaat/6403086/stroomnet-kwetsbaar-voor-cyberaanval-geen-kwestie-van-of-maar-wanneer.html

7 Comparaison internationale et réglementation

La cybersécurité des installations photovoltaïques s'est inscrite, ces deux dernières années environ, à l'ordre du jour réglementaire international. Le présent chapitre donne un aperçu des mesures d'autres États et de l'UE et y situe la Suisse. Les appréciations présentées émanent des autorités et des gouvernements concernés. Elles sont exposées ici, non évaluées.

7.1 Un schéma commun

Il est frappant que les initiatives de différents pays visent les deux mêmes points: la possibilité de commande à distance par les clouds des fabricants et la forte concentration du marché sur quelques fabricants, majoritairement chinois. Neuf des dix plus grands fabricants d'onduleurs au monde étaient chinois en 2024; Huawei et Sungrow représentaient à eux seuls environ 55% des livraisons mondiales.[60] Cette situation est classée comme un risque stratégique par plusieurs autorités nationales de sécurité.

La position opposée fait aussi partie de la mise en perspective. En mai 2026, le ministère chinois du commerce a déclaré que le classement de la Chine parmi les États à haut risque était intervenu sans preuves concrètes et l'a qualifié de stigmatisation des produits chinois.[61] La chambre de commerce chinoise auprès de l'UE a pour sa part rejeté le reproche selon lequel la Chine pourrait utiliser l'énergie comme moyen de pression et a souligné la contribution des entreprises chinoises à la transition énergétique européenne.[62]

7.2 Vue d'ensemble des instruments utilisés

Les initiatives peuvent être classées selon leur degré d'intervention, de la simple information au refus du raccordement au réseau.

- **Avertir:** l'Estonie et la Tchéquie misent sur des avertissements officiels. Le service de renseignement extérieur estonien a mis en garde[63] expressément en février 2024 contre les onduleurs chinois et a estimé que, plus l'Estonie misait sur l'énergie solaire, plus l'effet d'une manipulation éventuelle serait grand. Le chef du service de renseignement a parlé d'un risque de chantage.[64] Le 3 septembre 2025, l'autorité tchèque de cybersécurité NÚKIB a mis en garde contre le transfert de données vers la Chine et l'administration à distance depuis la Chine dans les infrastructures critiques, et a cité les onduleurs photovoltaïques comme un exemple parmi plusieurs. Il s'agit d'un avertissement, non d'une interdiction: les entités réglementées doivent en tenir compte dans leur analyse de risques.[65] En juin 2026, l'Allemagne a mis en garde, dans un avis commun de l'Office fédéral allemand de protection de la Constitution et du BSI, contre la reconnaissance d'installations photovoltaïques reliées à Internet sans protection par des acteurs russes.[66]
- **Recommander:** l'Australie a abordé le sujet tôt. En août 2023, le Cyber Security Cooperative Research Centre a publié le rapport «Power Out? Solar Inverters and the Silent Cyber Threat» et a recommandé trois mesures: des évaluations des cyberrisques pour tous les

[60] EUISS, Caspar Hobhouse, «The dragon in the grid: Limiting China's influence in Europe's energy system», janvier 2026: https://www.iss.europa.eu/publications/briefs/dragon-grid-limiting-chinas-influence-europes-energy-system
[61] Ministry of Commerce, China, «Remarks on the EU's Prohibition of Funding for Projects Using Chinese Inverters», mai 2026: https://english.mofcom.gov.cn/News/SpokesmansRemarks/art/2026/art_29f372ba6bfc4cde81fd567ea440cc60.html
[62] Euronews, «Bruxelles va interdire les onduleurs chinois dans ses infrastructures énergétiques», 5 mai 2026: https://fr.euronews.com/my-europe/2026/05/05/bruxelles-va-interdire-les-onduleurs-chinois-dans-ses-infrastructures-energetiques
[63] Estonian Foreign Intelligence Service (Välisluureamet): «International Security and Estonia 2024», février 2024: https://raport.valisluureamet.ee/2024/en/6-china/6-3-the-advance-of-chinese-technology/
[64] Reuters, articles sur des modules de communication non documentés, mai 2025: https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/
[65] Autorité tchèque de cybersécurité NÚKIB, septembre 2025: https://nukib.gov.cz/en/infoservis-en/news/2295-nukib-warns-against-the-transfer-of-the-data-to-and-remote-administration-from-people-s-republic-of-china/
[66] Bundesamt für Verfassungsschutz (BfV) et Bundesamt für Sicherheit in der Informationstechnik (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure», 3 juin 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

onduleurs vendus, des notations de cybersécurité obligatoires ainsi que le rappel ou la mise en conformité des appareils présentant des vulnérabilités graves.[67] Indépendamment de cela, une exigence générale s'applique en Australie depuis le 4 mars 2026 aux produits de consommation connectés: le Cyber Security Act 2024 australien et les Security Standards for Smart Devices Rules qui s'y rattachent exigent notamment des mots de passe uniques, un point de contact pour les vulnérabilités et l'indication de la durée de support.[68]

- **Tester et divulguer:** les Pays-Bas sont passés de la recherche à la surveillance réglementaire. Entre 2021 et 2023, l'inspection néerlandaise des infrastructures numériques (RDI) a testé neuf onduleurs du commerce de huit marques au regard de la norme ETSI EN 303 645, une norme de base européenne qui ne pose que des exigences minimales aux produits de consommation connectés et qui doit expressément protéger uniquement contre des attaques élémentaires exploitant des faiblesses fondamentales de conception, par exemple contre des mots de passe par défaut identiques pour tous les appareils d'un même fabricant. Aucun appareil ne remplissait toutes les exigences. L'autorité a averti que des appareils pouvaient être désactivés à distance ou détournés pour des attaques.[69] Indépendamment de cela, les divulgations décrites au chapitre «Constats et risques» ont suscité des questions parlementaires aux Pays-Bas.
- **Émettre un avis sur un projet législatif national:** l'Allemagne montre particulièrement bien le conflit d'objectifs entre commande au service du réseau et cybersécurité (cf. chapitre *7.3.1*).
- **Conditionner les aides financières:** l'Union européenne exclut des aides financières de l'UE les onduleurs de fournisseurs à haut risque et relève parallèlement, par la RED et le CRA, le niveau de protection de base des produits connectés (cf. chapitre *7.3.2*).
- **Conditionner l'accès au marché à un test:** Taïwan fait de la preuve de cybersécurité un élément constitutif de l'homologation de type (cf. chapitre *7.3.3*).
- **Conditionner le raccordement au réseau au respect d'exigences de sécurité:** la Lituanie interdit aux fabricants originaires d'États considérés comme une menace l'accès à distance aux installations de plus de 100 kW et autorise les gestionnaires de réseau à déconnecter les installations non conformes (cf. chapitre *7.3.4*).
- **Autorégulation:** en 2025, l'association professionnelle européenne SolarPower Europe a présenté une analyse, élaborée par la société d'essais DNV, sur les cyberrisques du photovoltaïque pour la stabilité du réseau. Elle contient une évaluation des risques, des simulations de réseau et un catalogue d'exigences minimales pour les fabricants, les exploitants et le monde politique. La branche a ainsi elle-même pris le sujet en main.[70]

7.3 Quatre approches en détail

Les quatre approches mentionnées en dernier sont présentées ci-après plus en détail, parce qu'elles sont directement pertinentes pour le débat suisse.

7.3.1 Allemagne: le conflit d'objectifs entre commande du réseau et cybersécurité

L'Allemagne montre particulièrement bien le conflit d'objectifs entre commande au service du réseau et cybersécurité. Selon l'art. 14a de la loi allemande sur l'industrie énergétique (EnWG), les gestionnaires de réseau peuvent, depuis le 1er janvier 2024, réduire temporairement à une puissance minimale de 4,2 kW le soutirage d'installations de consommation commandables telles que les pompes à chaleur, les bornes de recharge murales et les batteries de stockage en cas de

[67] Cyber Security Cooperative Research Centre (CSCRC), Rachael Falk / Anne-Louise Brown, «Power Out? Solar Inverters and the Silent Cyber Threat», 2023: https://cybersecuritycrc.org.au/power-out-solar-inverters-and-silent-cyber-threat/
[68] The Department of Home Affairs, Australia, Cyber Security (Security Standards for Smart Device) Rules 2025: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/security-standards-for-smart-devices
[69] Rijksinspectie Digitale Infrastructuur (RDI), «Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen», mai 2023: https://www.rdi.nl/documenten/rapporten/2023/05/30/onderzoek-storingsproblematiek-en-cyberveiligheid-omvormers-voor-zonnepanelen
[70] SolarPower Europe, «Solutions for PV Cyber Risks to Grid Stability», 2025: https://www.solarpowereurope.org/insights/thematic-reports/solutions-for-pv-cyber-risks-to-grid-stability

menace de surcharge locale du réseau. En contrepartie, le tarif d'utilisation du réseau est réduit.[71]

Lorsque la loi allemande sur les pics solaires (Solarspitzengesetz) a également prévu l'écrêtage des installations photovoltaïques par les onduleurs existants, l'Office fédéral allemand de la sécurité informatique (BSI) a exprimé de sérieuses réserves. Il a indiqué considérer d'un œil très critique la réalisation d'une commande à distance des onduleurs au service du réseau par l'intermédiaire des fabricants. Le fait que des fabricants aient, peut-être par un cloud exploité à l'étranger, un accès direct à un nombre aussi élevé d'appareils dans le réseau interconnecté européen présenterait un risque considérable. Outre le fabricant lui-même, des failles de sécurité pourraient aussi ouvrir un accès non autorisé à des tiers. Comme alternative, le BSI a proposé d'exploiter de telles installations aussi localement que possible et de réaliser la commande au service du réseau par des systèmes de mesure intelligents plutôt que par les clouds des fabricants.[72] Des commentaires spécialisés ont objecté que des onduleurs commandables à distance peuvent de toute façon être désactivés par le backend de leur fabricant et que l'accès redouté par le BSI existe donc déjà depuis longtemps, même sans la loi, compte tenu de la domination du marché par les fabricants chinois.[73]

Il est en outre remarquable, pour la Suisse, que l'Allemagne connaisse la même lacune réglementaire. L'ordonnance allemande sur les infrastructures critiques (BSI-KritisV)[74] ne s'applique qu'à partir de 104 MW de puissance d'installation; les installations photovoltaïques plus petites ne sont pas soumises aux prescriptions relatives aux infrastructures critiques.

7.3.2 Union européenne

L'étape la plus nette à ce jour est l'«Economic Security Doctrine» publiée le 3 décembre 2025, qui désigne expressément la dépendance à l'égard des onduleurs solaires comme une dépendance à haut risque et la justifie par la concentration des fournisseurs, les risques de cybermanipulation et l'accès à des données d'exploitation pertinentes pour le réseau. Elle cite comme instruments, entre autres, des évaluations coordonnées du cyberrisque et la certification au titre du Cyber Resilience Act. L'association de fabricants ESMC demande en outre que les États membres puissent exclure du raccordement au réseau le matériel à haut risque.[75]

Au printemps 2026 a suivi une mesure concrète: la Commission restreint les aides financières de l'UE, notamment celles de la Banque européenne d'investissement, pour les projets solaires, éoliens et de stockage qui utilisent des onduleurs de fournisseurs à haut risque de Chine, de Russie, d'Iran ou de Corée du Nord. Les fournisseurs de pays partenaires dignes de confiance restent éligibles.[76] Il importe de préciser qu'il s'agit d'une restriction de financement, et non d'une interdiction de mise sur le marché. Une étape plus poussée en direction de restrictions durables du marché est prévue avec la révision proposée du Cybersecurity Act (CSA2). Une lacune structurelle subsiste: la directive NIS2, fondamentale pour beaucoup de ces mesures, s'applique principalement aux entreprises de taille moyenne ou supérieure et ne couvre en règle générale pas les installations de production plus petites, comme le photovoltaïque privé en toiture.

Indépendamment de cela, l'UE relève le niveau de protection de base des produits connectés. Les exigences de cybersécurité de la directive sur les équipements radioélectriques (RED) s'appliquent depuis le 1er août 2025 et exigent, pour les équipements radio pouvant se connecter à Internet, la protection du réseau, la protection des données personnelles ainsi que la prévention de la fraude. À partir du 11 décembre 2027, le Cyber Resilience Act prend leur place; les

[71] Bundesnetzagentur, «Integration von steuerbaren Verbrauchseinrichtungen (§14a EnWG)»: https://www.bundesnetzagentur.de/DE/Vportal/Energie/SteuerbareVBE/artikel.html
[72] pv magazine Deutschland, Petra Hannen, «Solarspitzen-Gesetz: BSI warnt vor Zugriff chinesischer Hersteller auf deutsche Photovoltaikanlagen», janvier 2025: https://www.pv-magazine.de/2025/01/20/solarspitzen-gesetz-bsi-warnt-vor-zugriff-chinesischer-hersteller-auf-deutsche-photovoltaik-anlagen/
[73] zfk, Julian Korb, «Wirbel um Überwachung in chinesischen Wechselrichtern»: https://www.zfk.de/energie/strom/wirbel-um-ueberwachung-in-chinesischen-wechselrichtern
[74] BSI-KritisV, annexe 1, partie 3 no 1.1.1: https://www.gesetze-im-internet.de/bsi-kritisv/anhang_1.html
[75] pv magazine: «EU security doctrine highlights high-risk dependency on Chinese solar inverters», 16 décembre 2025: https://www.pv-magazine.com/2025/12/16/eu-security-doctrine-highlights-high-risk-dependency-on-chinese-solar-inverters/
[76] pv magazine, «EU moves to restrict funding for projects using inverters from high-risk suppliers», 23 avril 2026: https://www.pv-magazine.com/2026/04/23/eu-moves-to-restrict-funding-for-projects-using-inverters-from-high-risk-suppliers/

obligations de signaler les vulnérabilités activement exploitées et les incidents graves s'appliquent déjà à partir du 11 septembre 2026. Le CRA est technologiquement neutre et orienté cycle de vie et exige notamment des mécanismes de mise à jour sécurisés et un traitement structuré des vulnérabilités sur toute la durée de vie du produit. Comme ces règles conditionnent l'accès au marché et que les produits concernés sont largement les mêmes qu'en Suisse, elles devraient relever le niveau de sécurité aussi dans notre pays.

7.3.3 Taïwan: un test axé sur le produit avec une profondeur d'analyse considérable

Taïwan dispose de l'un des rares régimes de test axés sur le produit pour les onduleurs solaires, et du plus détaillé qui soit documenté publiquement. En octobre 2025, l'autorité taïwanaise de normalisation et de contrôle BSMI a publié une spécification technique de test et a rendu contraignantes les preuves de cybersécurité par une révision de l'homologation de type de mai 2026. Pour les onduleurs solaires, ainsi que pour l'infrastructure de recharge, les convertisseurs de puissance et les accumulateurs au lithium stationnaires, ces preuves deviennent un élément obligatoire de l'homologation de type à partir du 1er janvier 2028, et la voie simplifiée de la déclaration de conformité disparaît alors.[77]

Deux unités sont testées séparément, l'onduleur lui-même et l'unité de surveillance. Pour l'unité de surveillance, quatre dimensions de sécurité s'appliquent, à savoir la sécurité physique, la sécurité du système, la sécurité de la communication et la sécurité de l'authentification; pour l'onduleur, il y en a trois, fondées sur des normes internationales comme IEC 62443-4-2. La profondeur d'analyse est considérable. La remise du code source est exigée pour une analyse statique, les vulnérabilités présentant un score de gravité (CVSS) de 7 ou plus conduisant à la non-conformité en l'absence de mesure compensatoire justifiée. S'y ajoute un contrôle d'intégrité de la mise à jour du micrologiciel, lors duquel l'onduleur doit rejeter un micrologiciel intentionnellement manipulé ou revenir à un état sûr. Pour l'unité de surveillance, une analyse du trafic sur au moins 24 heures est en outre prévue, au cours de laquelle les adresses de destination effectives sont comparées aux serveurs déclarés par le fabricant.

Deux limites sont instructives sur le plan analytique. Premièrement, il s'agit d'un essai de type au moment de la certification: la spécification exige certes que l'appareil détecte un micrologiciel manipulé, mais ne prescrit pour cela aucun procédé cryptographique déterminé, et elle ne prévoit pas de nouveau contrôle spécifique lors de modifications ultérieures du micrologiciel. Deuxièmement, elle exclut expressément de l'étendue des tests la sécurité de l'information du système de gestion, c'est-à-dire du niveau cloud; seule est incluse la vérification de sa capacité à gérer des comptes d'utilisateur et à mettre à jour le micrologiciel à distance. Ce régime de test laisse ainsi de côté le niveau qui, selon les constats de la présente analyse, a le plus grand effet de levier. L'enseignement pour la Suisse et l'UE est donc double: un régime de test axé sur le produit est possible et judicieux, mais il reste incomplet tant qu'il n'intègre ni composante de cycle de vie ni niveau de commande central.

7.3.4 Lituanie: la sécurité comme condition du raccordement au réseau

La Lituanie est allée le plus loin. Avec l'article 73^3 adopté le 12 novembre 2024, l'accès à distance aux systèmes de commande d'installations solaires, éoliennes et de stockage de plus de 100 kW est interdit aux fabricants originaires d'États considérés comme une menace selon la stratégie nationale de sécurité, dont la Chine fait partie; concrètement, il s'agit de la modification à distance des paramètres de puissance ainsi que de la mise en marche et de l'arrêt. Sont notamment exigés une authentification multifacteur, une communication sécurisée, des contrôles de la chaîne d'approvisionnement ainsi qu'un audit. Pour les nouvelles installations, la réglementation s'applique depuis le 1er mai 2025; les installations existantes devaient se mettre en conformité jusqu'au 1er juin 2026. La conformité est une condition du raccordement au réseau et, depuis l'expiration du délai transitoire, les gestionnaires de réseau peuvent aussi déconnecter

[77] Taïwan, Bureau of Standards, Metrology and Inspection (BSMI): révision des règles d'homologation de type de mai 2026: https://www.bsmi.gov.tw/wSite/public/Attachment/f1761016956224.pdf; résumé: https://www.gmalabs.com/post/taiwan-bsmi-type-approval-update-new-cybersecurity-files

du réseau les installations non conformes.[78] L'association européenne des fabricants solaires a soutenu la réglementation.[79]

Ce que la loi n'exige pas est remarquable. Les appareils chinois ne sont pas interdits, et les installations existantes ne doivent pas être remplacées. Leurs exploitants doivent toutefois mettre en œuvre des mesures de protection supplémentaires.

L'expérience lituanienne montre en même temps où se situe la charge de travail. Pour les nouvelles installations, la conformité s'obtient à un coût comparativement faible, parce qu'elle peut être prise en compte dès le départ lors de l'acquisition et du raccordement. La mise à niveau du parc est coûteuse et chronophage, et des engorgements sont apparus dans sa mise en œuvre. Pour la Suisse, il en découle qu'une telle approche déploie ses effets surtout par les nouvelles installations et que le parc reste pendant des années le flanc le plus exposé.

7.4 Réglementation en Suisse

En Suisse, la norme minimale TIC est contraignante pour la branche de l'électricité depuis le 1er juillet 2024. L'ordonnance révisée sur l'approvisionnement en électricité (OApEl, annexe 1a) prescrit des niveaux de protection et des degrés de maturité, dont la Commission fédérale de l'électricité (ElCom) peut contrôler le respect. Le classement se fonde sur la capacité: le niveau de protection A s'applique par exemple aux gestionnaires de réseau à partir de 450 GWh par an, le niveau de protection B aux gestionnaires de réseau à partir de 112 GWh par an ainsi qu'aux producteurs d'électricité, aux exploitants de stockage et aux prestataires de services, pour autant qu'ils exploitent des installations d'une puissance totale d'au moins 100 MW et puissent les commander par un système unique.[80] S'y ajoute, depuis le 1er avril 2025, une obligation d'annoncer: les cyberattaques contre des infrastructures critiques doivent être annoncées dans les 24 heures à l'Office fédéral de la cybersécurité (OFCS).

La lacune déterminante concerne les petites installations et donc pratiquement toutes les installations photovoltaïques suisses. Les producteurs d'électricité ne sont soumis à la norme qu'à partir de 100 MW de puissance totale commandable par un système unique. Le parc de petites installations, réparti sur des centaines de milliers d'exploitants, n'est couvert par aucune entité assujettie unique. La réglementation européenne des produits, actuelle et à venir, devrait relever le niveau des appareils. Elle ne traite toutefois pas les questions structurelles et géopolitiques, à savoir la concentration du marché et la commandabilité à distance.

Un document de la société nationale du réseau de transport montre que cette lacune est reconnue. Dans le white paper «Intégration du photovoltaïque compatible avec le système»[81] de mars 2026, Swissgrid retient que l'approvisionnement énergétique suisse est déjà aujourd'hui réparti sur des centaines de milliers d'installations décentralisées. Cela exige, pour ces installations et leur commande également, un niveau de protection défini contre les cyberattaques. Swissgrid demande des exigences minimales contraignantes pour les installations photovoltaïques, qui devraient en outre être effectivement mises en œuvre et contrôlées y compris sur les installations existantes. La recommandation s'adresse au législateur et à l'Inspection fédérale des installations à courant fort (ESTI). La nécessité d'agir décrite dans le présent rapport est ainsi partagée par l'entité qui répond de la stabilité du système global.

Il faut avoir à l'esprit ce que la norme minimale TIC apporte et ce qu'elle n'apporte pas. Elle s'adresse à des organisations et exige d'elles qu'elles identifient les risques, mettent en œuvre des mesures de protection, détectent les incidents et y réagissent. Elle n'est pas applicable de manière judicieuse à une installation privée exploitée par une personne ne disposant pas d'une structure informatique. La lacune concernant les petites installations ne peut donc pas être comblée en abaissant le seuil de puissance. D'autres instruments sont efficaces ici: des exigences

[78] pv magazine, «Lithuania's grid operators can now disconnect solar plants without cybersecurity measures», juin 2026: https://www.pv-magazine.com/2026/06/05/lithuanias-grid-operators-can-now-disconnect-solar-plants-without-cybersecurity-measures/
[79] pv magazine, «Lithuania bans remote Chinese access to solar, wind, storage devices», 18 novembre 2024: https://www.pv-magazine.com/2024/11/18/lithuania-bans-remote-chinese-access-to-solar-wind-storage-devices/
[80] Office fédéral de la cybersécurité (OFCS), «Norme minimale pour les TIC»: https://www.bacs.admin.ch/fr/norme-minimale-tic
[81] Swissgrid SA, white paper «Intégration du photovoltaïque compatible avec le système», mars 2026: https://www.swissgrid.ch/fr/home/newsroom/blog/2026/20260330-01.html

relatives au produit, des conditions pour le raccordement au réseau ou l'assujettissement de l'entité qui concentre l'accès à de nombreuses installations.

7.5 Mise en perspective pour la Suisse

La tendance internationale est sans équivoque: plusieurs États traitent le photovoltaïque distribué de plus en plus comme une question d'infrastructure critique et non plus seulement de politique climatique. Les instruments utilisés vont d'avertissements (Tchéquie, Estonie, Allemagne) et de prises de position d'autorités sur des projets de loi (Allemagne) à des critères d'encouragement et d'acquisition (UE) et à des conditions contraignantes de raccordement au réseau (Lituanie), en passant par des contrôles du marché par les autorités de surveillance (Pays-Bas) et des régimes de test axés sur le produit (Taïwan).

S'y ajoute, sur le plan de l'application, un autre instrument. Avec l'attribution de l'attaque contre le réseau électrique polonais au service de renseignement russe FSB et le train de sanctions commun du 13 juillet 2026 (cf. chapitre *6.6*), l'UE et le Royaume-Uni montrent qu'une telle attribution et des sanctions sont utilisées en complément de la protection technique et réglementaire.[82]

La réglementation suisse couvre les gestionnaires de réseau, les grands producteurs d'électricité et exploitants de stockage ainsi que les prestataires de services disposant d'une capacité de commande d'une portée correspondante. Des prescriptions contraignantes de cybersécurité pour l'exploitation de chaque petite installation font défaut. La recommandation de branche RR/IPE-NR7 contient certes, depuis 2025, un chapitre sur l'accès à distance et les mises à jour du micrologiciel, mais s'y limite à la protection par mot de passe et aux mises à jour. La question de savoir lesquelles de ces approches entrent en ligne de compte pour la Suisse est reprise au chapitre *8 Recommandations*.

7.6 Perspectives réglementaires

Le niveau de protection de base des produits connectés augmente, mais les questions structurelles restent toutefois inchangées.

Du côté des produits, les exigences de cybersécurité de la directive sur les équipements radioélectriques RED s'appliquent depuis août 2025; en Suisse, elles sont mises en œuvre par l'ordonnance sur les installations de télécommunication, et l'autorité de surveillance du marché est l'Office fédéral de la communication OFCOM. La conformité à ces exigences peut être vérifiée à l'aide de la série de normes EN 18031, qui concrétise le contrôle d'accès, les mécanismes de mise à jour sécurisés et le traitement des identifiants. À partir de décembre 2027, le Cyber Resilience Act remplace les exigences de la RED et les étend à tous les produits comportant des éléments numériques, donc aussi aux appareils sans interface radio. Parallèlement, des régimes de test spécifiques à cette catégorie d'appareils apparaissent: l'homologation de type taïwanaise, UL 2941 et la certification de la SunSpec Alliance (cf. chapitres *7.3.3* et *8.3*).

Ce que ces réglementations apportent, c'est un niveau de base plus élevé; elles rendent plus difficile l'accès non autorisé par des tiers. Elles ne traitent toutefois ni la concentration du marché ni la possibilité de commande à distance par le fabricant lui-même. Les fabricants ainsi que les exploitantes et exploitants ne devraient donc pas attendre l'entrée en vigueur d'obligations futures pour mettre en œuvre les recommandations du chapitre suivant, mais agir dès aujourd'hui.

[82] OFSI/GOV.UK, communiqué de sanctions du 13 juillet 2026: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions

8 Recommandations

Les recommandations qui suivent découlent du constat central de ce rapport: le risque déterminant est de nature structurelle, donc une question de dépendance au cloud, de concentration du marché et de protocoles de commande non protégés de par leur conception, et moins une question d'appareils individuels défectueux. Elles sont structurées par destinataires et volontairement maintenues à un niveau général. Le présent rapport ne se prononce pas contre le photovoltaïque. Les recommandations doivent permettre la poursuite de son développement en toute sécurité. Il faut relever d'emblée que la solution unique, simple et complète n'existe pas: toutes les approches ont des inconvénients, et des risques résiduels subsistent.

8.1 Pour les exploitants de petites installations

L'installation initiale ne suffit pas à elle seule: les installations doivent être correctement configurées et régulièrement mises à jour, et la responsabilité doit être clairement attribuée en cas d'incident. Qui ne peut pas assumer ces tâches lui-même devrait les confier par contrat, à l'entreprise d'installation ou à un tiers. Une offre d'exploitation ne constitue pas à elle seule une preuve de compétence. Un fournisseur se révèle approprié s'il aborde de lui-même les points suivants et les garantit par écrit.

Points concrets pour l'installation individuelle:

- Changer immédiatement les mots de passe par défaut et activer les mises à jour automatiques du micrologiciel, ou installer les mises à jour sans tarder.
- Ne rendre aucun composant de l'installation accessible depuis Internet, en particulier ne pas configurer de redirection de port.
- Décider consciemment si l'installation doit être reliée en permanence au cloud du fabricant. Cette liaison n'est techniquement pas impérative, mais elle est en pratique le réglage par défaut et elle est rarement remise en question. Sur de nombreux appareils, la production peut aussi être lue localement sans cloud. Une telle exploitation sans raccordement au cloud réduit la surface d'attaque, mais au prix d'une perte de confort, par exemple le suivi pratique via l'application. Il faut en outre mettre en balance que, sans raccordement, les mises à jour automatiques du micrologiciel ne sont plus reçues et que des vulnérabilités connues peuvent de ce fait subsister. Là où l'appareil le permet, un verrouillage de la commande est donc souvent le meilleur compromis: il continue d'autoriser les mises à jour, mais pas la commande à distance active (cf. chapitre *8.4.2*). Les accès à distance non nécessaires devraient être désactivés.
- Choisir un système de gestion de l'énergie selon des caractéristiques vérifiables plutôt que selon l'étendue des fonctions: possibilité de commande locale sans liaison permanente au cloud, une période garantie de mises à jour et de support et, là où c'est possible, un test indépendant. Un SGE concentre en un point le contrôle de tous les appareils raccordés, de sorte qu'une seule vulnérabilité concerne l'ensemble de l'installation.
- Se faire confirmer, lors de la remise, que des mots de passe individuels ont été définis et que l'installation n'est pas accessible depuis Internet.
- Fixer par contrat qui veille à ce que les mises à jour du micrologiciel soient installées et qui est responsable en cas d'incident.

8.2 Pour les exploitants d'installations plus grandes

Pour les gestionnaires de réseau et les exploitants de grandes installations commerciales et industrielles, les principes éprouvés des environnements OT et IoT s'appliquent:

- **Inventorier le parc d'installations:** recenser et tenir à jour les onduleurs, les systèmes de gestion de l'énergie et leurs interfaces, y compris l'ensemble des accès à distance (fabricant, installateur, prestataire de services, agrégateur). Ce qui n'est pas connu ne peut pas être sécurisé.
- **Pas accessible depuis Internet:** les onduleurs et les systèmes de gestion de l'énergie, avec leurs interfaces d'administration, n'ont pas leur place sur Internet. Si un accès à distance est

nécessaire, il devrait passer par des canaux sécurisés, par exemple par un réseau privé virtuel (VPN).

- **Segmentation du réseau:** séparer individuellement le photovoltaïque, la gestion de l'énergie et l'infrastructure de recharge du reste du réseau, parce qu'un accès combiné à l'injection et à la consommation est particulièrement efficace (cf. chapitre *2.6*).
- **Séparation de la commande locale du réseau côté Internet:** si Modbus TCP est utilisé, l'onduleur se trouve souvent dans le même segment de réseau qu'un système de gestion de l'énergie relié à Internet. Un pare-feu réseau ordinaire ne protège ici que contre les accès venant de l'extérieur, mais pas contre un attaquant déjà présent dans le réseau local, par exemple via un appareil IoT compromis (cf. chapitre *5.3.3).* Un système de gestion de l'énergie doté de deux ports réseau physiquement séparés est donc plus robuste, l'un pour la partie locale (onduleur, sans Internet) et l'autre pour le réseau côté Internet. Un changement de support délibéré (par exemple RS485 au lieu d'Ethernet de bout en bout) réduit le risque qu'un appareil devienne accidentellement accessible depuis Internet.
- **Traiter le système de gestion de l'énergie comme un point de concentration**: il contrôle tous les appareils raccordés et sa compromission a donc une portée plus grande que celle d'un onduleur isolé.
- **Encadrer contractuellement les accès des fabricants:** régler par écrit l'étendue, le but et la durée d'un accès à distance privilégié et prévoir un droit de révocation (cf. chapitre *5.4.2*).
- **Configurer délibérément la capacité de commande centralisée:** là où l'installation n'a pas besoin d'une commande à distance du côté du fabricant, celle-ci devrait être restreinte et la commande des fonctions pertinentes pour le réseau réservée à l'entité réglementée (cf. chapitres *3.4* et *8.4.2*).
- **Surveillance et journalisation**: surveiller en continu les onduleurs, les systèmes de gestion de l'énergie et leurs accès à distance et centraliser et analyser les journaux générés par les appareils.
- **Exploiter un processus de mise à jour:** vérifier, selon un processus défini, pour son propre parc, si de nouvelles versions du micrologiciel, notamment des mises à jour de sécurité, sont disponibles, et l'installer sans tarder après évaluation des risques.
- **Prendre des dispositions pour le cas d'incident:** déterminer à l'avance qui est responsable en cas d'incident de sécurité, avec les contacts du fabricant ou de l'agrégateur et des autorités de cybersécurité. Les installations devraient en outre pouvoir se séparer de manière ordonnée du canal de commande touché, sans se déconnecter simultanément et de façon incontrôlée (cf. chapitre *8.4.2*).
- **Sécurité dans l'acquisition:** intégrer des exigences de sécurité dans les appels d'offres et faire de la cybersécurité un critère d'acquisition.
- **Appliquer volontairement la norme minimale TIC:** l'appliquer aussi à des systèmes qui ne relèvent pas de son champ d'application obligatoire (cf. chapitre *7.4).*

8.3 Pour les entreprises d'installation

Les entreprises d'installation décident en pratique du niveau de sécurité de l'installation individuelle. La mise en service détermine ce qui pourra être attaqué par la suite: qui définit les identifiants, configure les interfaces et raccorde l'installation au réseau détermine si un mot de passe par défaut reste en vigueur, si l'onduleur est accessible depuis Internet et si l'interface de commande locale reste ouverte sans protection. Ces décisions ne sont en règle générale pas prises par l'exploitante, mais par l'entreprise d'installation. Le BSI juge probable que l'installation et la configuration soient souvent effectuées par des entreprises spécialisées dans le solaire qui disposent de peu d'expertise en sécurité informatique.[83] Il est d'autant plus important que quelques principes soient respectés lors de la mise en service:

- Définir des identifiants individuels pour chaque installation et ne pas utiliser de mots de passe uniformes sur l'ensemble de la clientèle. Un code installateur valable pour tout le parc transfère au niveau de l'entreprise d'installation le même risque que celui décrit dans ce rapport chez les fabricants (cf. chapitre *5.4.2*).

[83] Bundesamt für Verfassungsschutz (BfV) et Bundesamt für Sicherheit in der Informationstechnik (BSI): «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure», 3 juin 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

- Ne rendre aucun composant de l'installation accessible depuis Internet, en particulier ne pas configurer de redirection de port.
- Désactiver les interfaces non nécessaires, par exemple un hotspot Wi-Fi inutilisé ou une interface de commande locale ouverte (cf. chapitre *5.3.2*).
- Séparer l'installation du reste du réseau domestique ou d'entreprise, de sorte qu'un appareil compromis dans le même réseau ne puisse pas accéder facilement à l'onduleur (cf. chapitre *5.3.3*).
- La remise de l'installation doit inclure une documentation de la configuration choisie et un accord clair sur la question de savoir qui veillera à l'avenir à ce que les mises à jour du micrologiciel soient installées et qui est responsable en cas d'incident.
- Dans l'acquisition, privilégier des produits qui fonctionnent aussi sans cloud, offrent des interfaces locales protégées et pour lesquels une période de support des mises à jour est garantie.

Pour que ces points soient respectés en pratique, l'entreprise d'installation doit disposer des compétences correspondantes. Les bases de la cybersécurité devraient donc faire partie intégrante de la formation initiale et continue.

8.4 Pour les fabricants

8.4.1 Exigences de base

La responsabilité du niveau de sécurité de base incombe aux fabricants. Les points centraux sont:

- **Sécurité comme principe de conception:** intégrer la sécurité dès le début et ne pas l'ajouter après coup («Security by Design»).
- **Mises à jour sécurisées du micrologiciel:** signées cryptographiquement, avec une protection contre le retour à des versions antérieures vulnérables.
- **Sécuriser les accès de maintenance et de service:** les données de connexion doivent être spécifiques à l'appareil et non reconstituables, afin qu'un seul mécanisme d'accès compromis ne concerne pas tout le parc. Un accès à distance privilégié devrait en outre être limité dans le temps et révocable par l'entité responsable.
- **Journalisation des événements pertinents pour la sécurité:** les connexions, les modifications de paramètres pertinents pour le réseau, les changements de micrologiciel et les accès par des comptes de maintenance doivent être journalisés dans l'appareil et pouvoir être lus.
- **Interfaces cloud sécurisées:** authentification et autorisation systématiques dans toutes les API.
- **Traitement des vulnérabilités signalées:** un processus de divulgation responsable structuré, avec un point de contact joignable et une correction dans un délai approprié.
- **État sûr à la fin du support:** lorsque le support du fabricant prend fin, par exemple par cessation d'activité, retrait du marché, sanctions ou litige de distribution, l'appareil doit rester fonctionnel localement et ne doit pas pouvoir être désactivé ou bloqué à distance.
- **Sauvegarde et restauration:** la configuration et les réglages pertinents pour le réseau doivent pouvoir être sauvegardés et restaurés, et le fabricant devrait mettre à disposition une version de référence vérifiée du micrologiciel de telle sorte qu'une installation puisse être remise en service même sans son concours.
- **Limiter la portée de son propre accès à distance:** même un accès légitime ne doit pas pouvoir commander ou mettre à jour simultanément l'ensemble du parc d'appareils. Cela doit être assuré techniquement par des réseaux, des serveurs de commande et des applications cloud séparés (cf. chapitre *8.5.2*).
- **Offrir une interface locale sécurisée:** il manque pour la commande locale un standard sécurisé répandu, et une obligation de chiffrement compromettrait l'interopérabilité avec les systèmes de gestion de l'énergie courants. Les fabricants devraient donc offrir en plus une variante authentifiée et chiffrée, comme certains le font déjà (cf. chapitre *3.3*), et désactiver l'interface en usine tant qu'elle n'est pas nécessaire.

Une partie de ces exigences n'est pas une recommandation, mais du droit des produits: pour les appareils dotés d'une interface radio, les exigences de cybersécurité de la directive sur les

équipements radioélectriques RED s'appliquent depuis août 2025; elles seront remplacées pour ces produits par le CRA à partir de décembre 2027, lequel vaudra alors pour tous les produits comportant des éléments numériques (cf. chapitre *7.3.2*). Les constats de la présente analyse montrent que ces exigences ne sont pas systématiquement remplies en pratique. Il est donc recommandé aux fabricants de ne pas viser le minimum nécessaire à la déclaration de conformité, mais de mettre en œuvre les principes sous-jacents à ces exigences: configuration sécurisée par défaut et sécurité comme principe de conception.

8.4.2 Verrouillage en usine de la commande des fonctions pertinentes pour le réseau

Au-delà de l'hygiène de base, il est recommandé de limiter du côté de l'appareil ce qui peut être modifié à distance. Le principe n'est pas nouveau: les lignes directrices du National Institute of Standards and Technology américain (NIST) pour les onduleurs (NIST IR 8498)[84] recommandent de désactiver en usine les capacités qui ne sont pas nécessaires dans chaque mode d'utilisation et de ne les activer que de manière délibérée.

Une telle limitation n'est efficace qu'en un point capable de distinguer le contenu des commandes et qui ne peut pas être contourné. Un pare-feu réseau ordinaire ne remplit pas la première condition, parce que les données d'exploitation et les commandes passent par la même liaison vers le même point de terminaison. Elle peut être mise en œuvre dans l'onduleur lui-même ou dans un système de gestion de l'énergie placé en amont (cf. chapitre *8.2*), ce dernier toutefois seulement si l'onduleur n'a pas de voie propre ouverte vers le cloud du fabricant et refuse les accès en écriture locaux non authentifiés. La recommandation distingue trois classes de capacités, pour chacune desquelles un régime différent s'applique: l'accès à distance dans l'état à la livraison, les paramètres pertinents pour le réseau et les valeurs de consigne d'injection.

État à la livraison: sont admis à distance exclusivement la lecture des données d'exploitation et les mises à jour du micrologiciel signées cryptographiquement. L'installation doit continuer de fonctionner entièrement sans ce canal, avec un comportement inchangé à l'égard du réseau.

La recommandation de branche suisse RR/IPE-NR7[85] préconise au contraire de désactiver là où c'est possible la fonction de mise à jour du micrologiciel à distance et de n'effectuer les mises à jour que sur place. Le raisonnement est compréhensible, car le canal de mise à jour est effectivement l'accès à distance le plus puissant. Avec un parc de centaines de milliers de petites installations, cette approche conduit toutefois, du point de vue du NTC, à un risque plus grand encore: sans canal de mise à jour fonctionnel, des vulnérabilités connues restent ouvertes pendant des années. Le BSI allemand recommande instamment de vérifier régulièrement si de nouvelles versions logicielles sont disponibles et d'installer le plus rapidement possible, après pesée des risques, au moins celles qui corrigent des failles de sécurité.[86] Le présent rapport suit cette ligne, mais la lie à des exigences portant sur la chaîne de mise à jour elle-même: signature cryptographique, protection contre l'installation de versions antérieures et une version identifiable dont les modifications du comportement à l'égard du réseau sont documentées.

Paramètres pertinents pour le réseau: les paramètres pertinents pour le réseau sont définis lors de la mise en service et sont verrouillés ensuite. Sont visées les valeurs qui déterminent le comportement de l'installation à l'égard du réseau: p. ex. le paramètre pays dans son ensemble, les réglages de protection pour la tension et la fréquence, les conditions de connexion et de reconnexion, le comportement en puissance réactive et en puissance active en fonction de la tension et de la fréquence ainsi que le comportement en cas de défaut du réseau. L'annexe E de la recommandation de branche RR/IPE-NR7 en définit l'étendue. Ils constituent en même temps un vecteur d'attaque particulièrement efficace (cf. chapitre *6.3*, type B). Swissgrid exige la même protection sans référence à une attaque: le comportement des installations lors d'une

[84] National Institute of Standards and Technology NIST: Cybersecurity for Smart Inverters – Guidelines for Residential and Light Commercial Solar Energy Systems, NIST IR 8498, décembre 2024: https://doi.org/10.6028/NIST.IR.8498
[85] AES: recommandation de branche «Raccordement au réseau pour les installations productrices d'énergie sur le réseau basse tension RR/IPE-NR7 – CH 2025»: https://www.strom.ch/fr/document/raccordement-au-reseau-pour-les-installations-productrices-denergie-sur-le-reseau-basse-tension
[86] Bundesamt für Verfassungsschutz (BfV) et Bundesamt für Sicherheit in der Informationstechnik (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure», 3 juin 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

déconnexion du réseau et leurs conditions de reconnexion devraient être définis directement dans l'installation, afin de réduire une grande composante d'incertitude dans la phase délicate de la reconstitution du réseau. Ces valeurs sont donc à protéger non seulement parce qu'elles peuvent être manipulées, mais aussi parce que l'exploitation du réseau s'appuie sur elles.

La protection particulière de ces valeurs est également recommandée à l'échelle internationale:

- Les recommandations du NIST pour les onduleurs préconisent des interfaces désactivées en usine, des logiciels provenant uniquement de sources vérifiées et une séparation des fonctions de régulation et des interfaces de communication. Un mot de passe seul n'y est plus considéré comme approprié pour des accès ayant un effet sur des infrastructures critiques.
- L'étude de Secura recommande de rendre les paramètres critiques non modifiables et de n'autoriser la configuration à distance qu'avec un accord local.[87]

Pour la Suisse, il n'existe pas de prescription uniforme à ce sujet. Il serait déterminant qu'un tel verrouillage ne repose pas uniquement sur une authentification. Un mécanisme d'autorisation disponible de manière centralisée peut être utilisé simultanément sur de nombreuses installations, et c'est précisément cette simultanéité qui produit l'effet que le présent rapport décrit comme d'importance systémique. Il est donc logique de lier la levée du verrouillage à une autorisation locale sur l'appareil, par exemple au moyen d'une action physique sur place, de sorte qu'elle ne puisse pas être déclenchée simultanément sur de nombreuses installations par un accès disponible de manière centralisée. Le verrouillage vaut pour tous les chemins d'écriture vers ces valeurs, soit l'interface de commande, les interfaces de communication locales, le raccordement au cloud et l'accès de maintenance. Le plombage des compteurs et des dispositifs de protection poursuit le même principe depuis longtemps. Il s'agit là de la protection contre une modification non autorisée et non de l'immuabilité en tant que telle. Si les conditions de raccordement changent, une adaptation du parc existant doit rester possible.

Valeurs de consigne d'injection: verrouillées, mais activables sur place dès que l'installation participe à un service de réseau. Une simple limitation de la plage de consigne ne suffit pas, parce que l'écrêtage à zéro est précisément le service de réseau prévu et correspond en même temps au schéma d'attaque de type A. Deux conditions s'y ajoutent:

- Si la capacité est activée, elle ne devrait pas passer par le cloud du fabricant, mais par le gestionnaire de réseau ou par l'agrégateur lié par contrat (cf. chapitre *8.5.1*).
- Si la liaison de commande tombe en panne ou reste absente, l'appareil revient après un temps de maintien à un état défini lors de la mise en service. Le temps de maintien empêche qu'une perturbation de la communication déclenche simultanément un saut de puissance sur de nombreuses installations.
  La même exigence est également posée sans scénario d'attaque. Swissgrid recommande de construire les nouvelles installations «fail-safe»: elles devraient pouvoir continuer à être exploitées en sécurité même sans commande externe et sans communication fonctionnelle, ce pour quoi les gestionnaires de réseau devraient élaborer des prescriptions pour un état défini à l'avance. L'élément déclencheur y est l'interruption ordinaire de la communication, donc le même cas que celui traité par le temps de maintien décrit ci-dessus. La recommandation ne présuppose donc pas l'hypothèse d'un attaquant.[88]

L'état sécurisé devient ainsi la configuration par défaut, et toute commandabilité à distance supplémentaire devient une décision délibérée, visible et prise sur place. Ce mécanisme ne protège toutefois pas l'appareil contre un micrologiciel manipulé, car du code présent sur l'appareil peut contourner tout verrouillage côté appareil. Contre le fabricant lui-même et contre une chaîne de mise à jour compromise, seuls agissent dès lors l'intégrité de cette chaîne, un contrôle ultérieur lors de modifications importantes du micrologiciel (cf. chapitre *8.5.3*), la diversification et la possibilité d'un test indépendant.

[87] Secura, «Cybersecurity threats and measures for the solar power sector», 2024: https://www.energy-innovation.nl/documents/1299/2024-Secura_Report-Cybersecurity_threats_and_measures_for_the_solar_power_sector.pdf
[88] Swissgrid SA, white paper «Intégration du photovoltaïque compatible avec le système», mars 2026: https://www.swissgrid.ch/fr/home/newsroom/blog/2026/20260330-01.html

Pour finir, sur le rapport entre cette recommandation et l'orientation de la politique énergétique: la branche évolue vers davantage de possibilités de commande. Dans son white paper sur l'intégration du photovoltaïque, Swissgrid retient que la flexibilité ne sera à l'avenir plus une option pour les installations photovoltaïques, mais une condition. Le verrouillage de la commande en usine proposé ici n'est pas en contradiction avec cela. Il n'exige pas de renoncer à la flexibilité, mais seulement que son activation ait lieu sur place et que la commande pertinente pour le réseau passe ensuite par l'entité réglementée.

8.5 Pour les responsables politiques et les autorités de régulation

8.5.1 Compétence

Combler la lacune de responsabilité pour les petites installations: des prescriptions existent, mais elles ne vont pas assez loin. Les exigences de cybersécurité de la directive sur les équipements radioélectriques ne couvrent que les appareils dotés d'une interface radio et reposent sur la déclaration du fabricant, et la recommandation de branche sur le raccordement au réseau se limite à la protection par mot de passe et aux mises à jour. Les instruments efficaces sont ceux qui ne s'attachent pas à l'exploitant individuel. Des interventions réglementaires sont ici vraisemblablement nécessaires, parce que cette protection ne se met pas en place d'elle-même. Parmi les approches possibles figurent des modèles déjà utilisés par d'autres États: des conditions de raccordement au réseau portant sur la commandabilité des installations (comme en Lituanie) ou des critères d'acquisition et d'encouragement (comme au niveau de l'UE). Aucune de ces voies n'est parfaite (cf. chapitre *7*). Cette nécessité d'agir ne découle pas seulement des constats techniques. Le SRC signale expressément que la Suisse devient une cible plus attractive lorsque les États voisins protègent davantage leur infrastructure critique et que la Suisse ne suit pas le mouvement (cf. chapitre *2.5*).

Assurer la maîtrise de la commande des fonctions pertinentes pour le réseau: le but n'est pas d'interdire le cloud, mais de répondre clairement à la question de savoir qui a le droit de donner à une installation des commandes pertinentes pour le réseau. Cette compétence devrait revenir à une entité qui est elle-même réglementée et qui répond de la stabilité du réseau: au gestionnaire de réseau de distribution ou à un agrégateur lié par contrat, soumis à la norme minimale TIC. L'association européenne de la branche recommande le même modèle, en distinguant entre fonctions critiques et non critiques: le démarrage, l'arrêt et la modification de la puissance active et réactive uniquement par l'entité réglementée, la surveillance et les mises à jour logicielles aussi par d'autres canaux, pour autant que ceux-ci puissent être interrompus en cas de soupçon.[89] Pour la Suisse, ce principe est déjà esquissé: le gestionnaire de réseau de distribution ne peut utiliser la flexibilité d'une installation qu'au service du réseau.[90] Swissgrid signale en même temps les lacunes pratiques:[91] font défaut une communication standardisée entre l'installation ou le système de gestion de l'énergie et le gestionnaire de réseau de distribution, une cascade de commandes standardisée entre les gestionnaires de réseau ainsi que la mise en œuvre technique de la règle légale selon laquelle la flexibilité garantie au service du réseau prime sur tous les autres signaux de commande. Pour réglementer de manière contraignante la maîtrise de la commande, il faut donc aussi créer l'interface nécessaire. Sans elle, la voie passant par le cloud du fabricant reste la seule qui fonctionne en pratique. Il reste à clarifier si un raccordement permanent à un cloud de fabricant est vraiment nécessaire du côté du réseau et, dans l'affirmative, quelles exigences cette infrastructure doit remplir. Le seul lieu d'hébergement n'y suffit pas (cf. chapitre *5.4.5*). Du côté de l'appareil, la prescription selon laquelle les onduleurs doivent avoir un verrouillage de la commande des fonctions pertinentes pour le réseau actif en usine serait réalisable (cf. chapitre *8.4.2*). Cette orientation coïncide avec la position du BSI allemand (cf. chapitre *7.3.1*).

Attribuer clairement la responsabilité du risque cumulé: personne n'est responsable de la petite

[89] SolarPower Europe / DNV: «Solutions for PV Cyber Risks to Grid Stability», 2025: https://www.solarpowereurope.org/insights/thematic-reports/solutions-for-pv-cyber-risks-to-grid-stability
[90] Art. 17c LApEl (RS 734.7) et art. 19a OApEl (RS 734.71). Pour la mise en perspective: AES, «Potentiel et limites de la nouvelle réglementation en matière de flexibilité», décembre 2025: https://www.strom.ch/fr/perspective/potentiel-et-limites-de-la-nouvelle-reglementation-en-matiere-de-flexibilite
[91] Swissgrid SA, white paper «Intégration du photovoltaïque compatible avec le système», mars 2026: https://www.swissgrid.ch/fr/home/newsroom/blog/2026/20260330-01.html

installation individuelle, et pour le risque qui ne naît que de la somme de nombreuses installations, aucune entité n'est clairement désignée. Il reste à clarifier quelle entité observe ce risque agrégé, coordonne en cas d'incident et surveille l'efficacité des mesures portant sur le produit et sur le raccordement.

Prendre des dispositions pour le cas d'incident: à côté de la prévention, il faut la capacité de détecter un abus en cours et d'y mettre fin de manière ordonnée. Il n'existe pas d'interrupteur d'arrêt d'urgence central, et une déconnexion massive défensive mettrait elle-même en danger la stabilité du réseau. Un canal de commande compromis ne peut être coupé sans danger que si les installations retombent alors dans un état sûr et conforme au réseau (cf. chapitre *8.4.2*) et qu'une entité désignée tienne à jour le tableau de situation et coordonne les acteurs concernés. Cette capacité sert avant tout à parer à une compromission persistante et à la gestion après un incident, non à empêcher la première attaque, qui se déroule en quelques secondes.

8.5.2 Portée d'un accès unique

Limiter la portée d'un accès unique: ce qui rend une vulnérabilité pertinente pour le réseau, ce n'est pas sa gravité, mais sa portée. Il en découle une mesure qui agit indépendamment des parts de marché et de la qualité des produits: aucun point unique ne doit pouvoir modifier simultanément tout un parc d'appareils. Dans la production classique, cette limite allait de soi, parce qu'une centrale dépasse rarement environ 1,5 gigawatt et que son système de conduite n'atteint que cette seule centrale. Avec les clouds des fabricants et les agrégateurs, elle disparaît. L'association européenne de la branche propose donc de la prescrire expressément et de l'étayer techniquement:[92]

- une limite supérieure pour la puissance de production qui peut être commandée par un seul système de commande: qui en exploite davantage doit utiliser pour cela des systèmes séparés sans causes de défaillance communes
- une segmentation de l'accès à distance propre au fabricant, de sorte que l'ensemble du parc ne puisse pas être commandé d'un seul coup
- des dispositions techniques contre la mise à jour simultanée de tous les appareils, afin qu'il reste du temps pour intervenir si une mise à jour est défectueuse ou manipulée
- des temporisations aléatoires propres à chaque appareil pour des commandes sélectionnées. Les commandes concernées et la durée de la temporisation sont à définir dans des normes et en concertation avec l'exploitation du réseau

Ces mesures n'exigent aucun renoncement à la commande à distance ni aucune modification des parts de marché. Elles limitent seulement l'effet qu'une seule commande peut produire. Trois réserves s'y ajoutent: le seuil reste à définir et devrait faire l'objet d'une décision spécifique. La mise en œuvre relève de l'architecture du fabricant et n'est guère vérifiable de l'extérieur; sans obligation de preuve, elle reste donc une autodéclaration. Et elle limite la portée, non la dépendance elle-même: un accès à distance segmenté procure du temps pour intervenir en cas d'incident, mais laisse le fabricant conserver le contrôle sur chaque segment.

Encourager à temps la diversification: le marché des onduleurs se consolide fortement. Pour la cybersécurité, cela est directement pertinent, car la diversité des fabricants constitue elle-même un facteur de protection: des fabricants, des plateformes et des versions de micrologiciel différents rendent plus difficile d'atteindre de nombreuses installations avec une seule attaque. À l'inverse, chaque consolidation supplémentaire du marché crée un «Single Point of Failure» plus grand. L'objectif devrait donc être de disposer durablement de fabricants dans plusieurs régions du monde, et non de privilégier une origine déterminée. Les instruments sont par exemple des critères d'acquisition qui récompensent les stratégies multifournisseurs. Le point touche au droit des marchés publics et au droit commercial et n'est que partiellement réalisable de manière unilatérale. La fenêtre temporelle pourrait se rétrécir, parce que plusieurs fournisseurs disposent certes encore de capacités, mais perdent des parts de marché. L'évolution reste incertaine. La diversification abaisse le risque d'un exploit unique commun à plusieurs fabricants, mais ne résout pas le problème structurel central: avec un seuil de moins de deux pour cent du parc européen (cf. chapitre *6.5)*, pratiquement chaque fabricant pertinent sur le marché reste à lui seul

[92] SolarPower Europe / DNV: «Solutions for PV Cyber Risks to Grid Stability», 2025: https://www.solarpowereurope.org/insights/thematic-reports/solutions-for-pv-cyber-risks-to-grid-stability

d'importance systémique. Selon Secura, aux Pays-Bas, l'attaque contre un seul fabricant suffit; deux entrent en ligne de compte au vu de leur part de marché (cf. chapitre *5.4*). La diversification est donc un complément judicieux, mais pas un substitut aux autres mesures mentionnées ici.

8.5.3 Contrôle et mise à niveau du parc installé

Test de produit avec composante de cycle de vie: un régime de test de cybersécurité axé sur le produit pour les onduleurs et les systèmes de gestion de l'énergie est possible et judicieux. Avec l'analyse du code source, l'analyse du trafic et le contrôle d'intégrité du micrologiciel, Taïwan montre jusqu'où un tel test peut aller. Il est toutefois déterminant qu'un tel régime ne s'arrête pas à un essai de type ponctuel: une procédure de mise à jour imposée et sécurisée par cryptographie et un contrôle ultérieur lors de modifications importantes du micrologiciel sont nécessaires. Il faut tenir compte de la limite de tout test de produit: il traite l'exposition aux attaques de tiers, mais ne supprime pas la dépendance à l'égard du fabricant lui-même. Contre le scénario de l'acteur interne ou étatique qui contrôle la chaîne de mise à jour légitime, seuls agissent la diversification et une limitation technique de ce que le cloud peut commander à distance (cf. chapitre *5.2*).

Tout cela n'exige pas nécessairement de nouvelle base légale. Pour les onduleurs dotés d'une interface radio, la conformité aux exigences de cybersécurité de la directive sur les équipements radioélectriques et à la norme correspondante EN 18031 pourrait déjà être contrôlée aujourd'hui dans le cadre de la surveillance du marché (cf. chapitre 7.4 Réglementation en Suisse). Des régimes de test axés sur le produit pour cette catégorie d'appareils apparaissent en outre à l'échelle internationale: à côté de l'homologation de type taïwanaise, il existe avec UL 2941[93] et la certification de la SunSpec Alliance des programmes[94] auxquels une exigence suisse ou européenne pourrait se rattacher.

Utiliser le contrôle de l'installation existant pour la cybersécurité: les installations photovoltaïques sont soumises à contrôle selon l'ordonnance sur les installations à basse tension. Un organe de contrôle indépendant contrôle l'installation après sa réalisation, le rapport de sécurité est transmis au gestionnaire de réseau, et le contrôle se répète périodiquement. Il existe ainsi une procédure obligatoire qui couvre l'installation dans son état installé et dont le résultat est transmis à une entité réglementée. Elle intervient là où les exigences relatives au produit et les prescriptions adressées à l'exploitante individuelle ne suffisent pas. Il est recommandé de compléter le procès-verbal de contrôle correspondant par quelques points vérifiables sans ambiguïté: p. ex. des mots de passe par défaut changés, aucune accessibilité depuis Internet, des interfaces non nécessaires désactivées et l'état du verrouillage de la commande (cf. chapitre *8.4.2*). Swissgrid propose la même voie pour les réglages d'exploitation et exige séparément, pour la cybersécurité, des exigences minimales qui doivent aussi être contrôlées, sans nommer de procédure à cet effet.[95] Une adaptation des prescriptions est nécessaire pour cela, mais elle s'inscrit dans une procédure rodée plutôt que dans un régime nouveau, et seul reste vérifiable ce qui peut être constaté sans marge d'interprétation.

Ne pas oublier le parc: toutes les mesures qui précèdent produisent avant tout leurs effets sur les nouvelles installations. Seul le contrôle périodique des installations couvre aussi le parc existant, mais lentement. Le parc d'installations existant reste pendant des années le flanc le plus exposé (cf. chapitre *7.3.4*). Une unité de communication placée en amont, qui coopère avec les onduleurs existants et attribue la commande au gestionnaire de réseau, serait réalisable. Elle transpose ainsi au parc ce que propose le chapitre *8.5.1 Compétence*.

Toutes ces recommandations s'inscrivent dans une même logique: le photovoltaïque doit

[93] UL Solutions: UL 2941, Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources, 2023; programme de certification depuis février 2026: https://www.ul.com/services/cybersecurity-distributed-energy-and-inverter-based-resources
[94] SunSpec Alliance: DER Device Cybersecurity Certification: https://sunspec.org/certifications/
[95] Swissgrid SA, white paper «Intégration du photovoltaïque compatible avec le système», mars 2026: https://www.swissgrid.ch/fr/home/newsroom/blog/2026/20260330-01.html

continuer de croître, mais le contrôle de centaines de milliers d'appareils pertinents pour le réseau ne doit pas se trouver entre les mains de quelques entités dont les interventions sont techniquement illimitées et non vérifiables de l'extérieur. La fenêtre temporelle pour cela est ouverte. Elle se referme avec chaque installation construite aujourd'hui et encore raccordée au réseau dans vingt ans.