Istituto nazionale di test per la cibersicurezza

Cibersicurezza degli impianti fotovoltaici

Risultati e raccomandazioni

Versione	1.0
Data	17 settembre 2026
Classificazione	Pubblico
Autori	Tobias Castagna, Stefan Gloor, Andreas Leisibach, Dilip Many, Raphael M. Reischuk, Lukas Sohrmann, Fabio Zuber
Responsabile	Tobias Castagna

Con il sostegno di svizzeraenergia

Indice

Ringraziamenti

Un ringraziamento particolare va alle organizzazioni e agli esperti che hanno sostenuto questo studio, sia mettendo a disposizione dispositivi di test, sia offrendo uno sguardo sull'impiego di tali dispositivi in ambienti diversi, sia partecipando ai costi. Con il loro impegno hanno contribuito in misura determinante alla riuscita di questa analisi di sicurezza. Tra queste figurano:

• SvizzeraEnergia, Ufficio federale dell'energia UFE
• Commissione federale dell'energia elettrica ElCom
• Ufficio federale della cibersicurezza UFCS
• Ufficio federale delle comunicazioni UFCOM
• Associazione delle aziende elettriche svizzere (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 (Svizzera) SA
• Swissgrid SA
• Swissolar

• Prof. Dr. Christof Bucher, Berner Fachhochschule BFH
• Prof. Roger Buser, Hochschule Luzern HSLU
• Prof. Dr. Andreas Heinzelmann, ZHAW Zürcher Hochschule für Angewandte Wissenschaften
• Ruben Santamarta, ricercatore indipendente in cibersicurezza
• Dr. Leonard Schliesser, Center for Security Studies CSS, ETH Zurigo
• Arrigo Triulzi Lampugnani, esperto indipendente in cibersicurezza
• Bastian Widmer, esperto indipendente in cibersicurezza

Un ringraziamento speciale va a Robin Seidel, che nell'ambito dei suoi studi al Politecnico federale di Zurigo e in collaborazione con l'NTC ha individuato gravi vulnerabilità in un dispositivo connesso di un impianto fotovoltaico. Questo lavoro preliminare ha rafforzato l'NTC nella convinzione della necessità di intervento e ha dato impulsi essenziali alla presente analisi.

1 Management Summary

L'essenziale in breve

Il fotovoltaico è rilevante per il sistema: alla fine del 2025 in Svizzera erano installati circa 338'000 impianti fotovoltaici allacciati alla rete. La loro produzione annua ha coperto il 13,7 per cento del consumo finale di elettricità. Nelle ore di mezzogiorno con cielo sereno gli impianti coprono regolarmente oltre la metà del consumo istantaneo.

L'indagine: l'Istituto nazionale di test per la cibersicurezza NTC ha verificato di propria iniziativa sette inverter e quattro sistemi di gestione dell'energia. L'NTC è stato in ciò sostenuto da organizzazioni di settore e da SvizzeraEnergia.

Oltre 50 rilievi in undici prodotti: sette rilievi sono critici, sei elevati. Cinque prodotti presentavano almeno un rilievo critico o elevato. Di quattro dispositivi è stato possibile ottenere il controllo completo.

I produttori reagiscono rapidamente: l'NTC ha comunicato i rilievi ai produttori interessati già prima della pubblicazione del presente rapporto. Molti hanno reagito immediatamente e hanno già chiuso le falle.

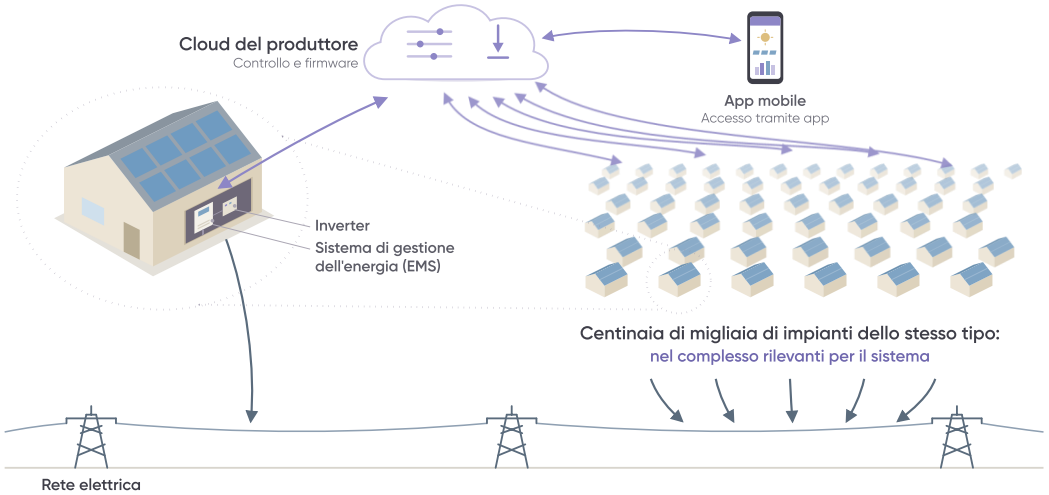
Non decide soltanto la gravità, bensì la portata: una singola vulnerabilità in un componente rilevante può riguardare migliaia di impianti collegati. Sei rilievi sono di questo tipo. Il singolo impianto è irrilevante per la rete, il parco impianti nel suo insieme è infrastruttura critica.

Rischio strutturale: il rischio maggiore non si lascia eliminare con una migliore sicurezza dei prodotti. Esso nasce dal collegamento dei dispositivi ai cloud dei produttori, attraverso i quali vengono ad esempio installati gli aggiornamenti del firmware.

Competenza mancante: le prescrizioni sono insufficienti per gli impianti di piccole dimensioni e, per il rischio che nasce dalla loro somma, nessuno è responsabile.

Alla fine del 2025 in Svizzera erano installati circa 338'000 impianti fotovoltaici allacciati alla rete con circa 9,5 gigawatt (GW) di potenza di picco (per confronto: la centrale nucleare di Gösgen eroga circa 1 GW). La loro produzione annua di poco meno di 8 terawattora (TWh) ha coperto il 13,7 per cento del consumo finale di elettricità, all'incirca al livello della centrale nucleare di Gösgen. Entro il 2030 la produzione dovrebbe più che raddoppiare secondo i nuovi obiettivi intermedi del Consiglio federale (18,7 TWh). Per l'esercizio della rete non conta però la somma annua, bensì il contributo istantaneo: nelle ore di mezzogiorno con cielo sereno il fotovoltaico copre regolarmente oltre la metà del consumo, il 4 luglio 2026 alle ore 14 quasi l'85 per cento.

Con ciò cambia la struttura della produzione di energia elettrica: accanto a poche grandi centrali regolamentate si affiancano centinaia di migliaia di impianti piccoli, collegati al cloud e configurati in larga misura allo stesso modo, singolarmente irrilevanti, nel complesso rilevanti per il sistema.



Il parco impianti svizzero è composto quasi esclusivamente da piccoli impianti su tetti di edifici abitativi e commerciali, gestiti da privati e da piccole imprese senza competenze nell'esercizio e nella manutenzione di infrastrutture critiche. Ciò che un tempo richiedeva l'accesso fisico a una centrale è oggi possibile attraverso un accesso remoto centrale. Il rischio non risiede nel fotovoltaico stesso, bensì nel modo in cui il suo controllo è organizzato.

Gli impianti gestiti da privati finora non sono quasi mai stati verificati in modo indipendente riguardo alle vulnerabilità: mancano incentivi, competenze chiare e una regolamentazione adeguata. Le prescrizioni di cibersicurezza del settore elettrico (standard minimo TIC) si rivolgono a organizzazioni e si applicano ai produttori di energia elettrica solo a partire da 100 megawatt controllabili tramite un unico sistema. All'impianto di una casa unifamiliare non sono né applicabili né destinate.

L'Istituto nazionale di test per la cibersicurezza NTC ha perciò verificato di propria iniziativa, nell'arco di circa un anno, undici prodotti digitali del settore fotovoltaico diffusi in Svizzera: sette inverter e quattro sistemi di gestione dell'energia di otto produttori complessivamente. Il team di test e una parte sostanziale dei mezzi finanziari provenivano dall'NTC; diverse organizzazioni, in prevalenza del settore energetico, hanno messo a disposizione dispositivi di test e hanno partecipato ai costi. L'indagine è stata inoltre sostenuta finanziariamente da SvizzeraEnergia. Né i produttori né le organizzazioni di sostegno hanno influito sulla selezione, sulla portata della verifica o sui risultati. Tutti i rilievi sono stati segnalati ai produttori in via confidenziale. Il presente rapporto non indica per principio né nomi di prodotti né dettagli tecnici, bensì descrive schemi di rischio tipici e le raccomandazioni che ne derivano.

Complessivamente le verifiche hanno portato alla luce oltre 50 rilievi, sette dei quali critici e altri sei elevati. Cinque degli undici prodotti presentavano almeno un rilievo elevato o critico. In quattro prodotti l'NTC ha ottenuto il controllo completo del dispositivo, in parte introducendo codice di programma estraneo, in parte attraverso un accesso di manutenzione del produttore protetto in modo insufficiente.

Sono emersi quattro schemi ricorrenti:

- carenze nell'autenticazione e nel controllo degli accessi, ad esempio password predefinite
- accessi di manutenzione non sicuri, ad esempio con credenziali identiche per l'intero parco di dispositivi
- cifratura assente o debole della comunicazione tramite interfacce locali
- interfacce che non si lasciano disattivare

In quasi tutti gli inverter verificati è possibile modificare, attraverso l'interfaccia di comando locale e senza alcuna autenticazione, quanta potenza l'impianto immette in rete, fino a zero. Questa interfaccia è attiva soprattutto dove un sistema di gestione dell'energia controlla l'impianto. Preso di per sé, un simile accesso riguarda un solo impianto. Se però molti impianti vengono manipolati simultaneamente, ciò può mettere in pericolo la stabilità della rete elettrica. La rete deve garantire in ogni momento un equilibrio tra produzione e consumo. Una vulnerabilità diventa perciò rilevante per la rete non per la sua sola gravità, bensì per la sua portata: sei rilievi agiscono attraverso un'istanza centrale su un intero parco di dispositivi e quindi su molti impianti contemporaneamente.

Il livello di sicurezza dei singoli prodotti non è peggiore di quello di altri dispositivi connessi molto diffusi che l'NTC ha verificato in analisi comparabili. Non sono emersi indizi di backdoor inserite intenzionalmente o di componenti di comunicazione nascosti. La maggior parte dei produttori ha reagito rapidamente alle vulnerabilità segnalate; per una parte dei rilievi il processo di divulgazione è ancora in corso, tra l'altro perché per più serie di modelli in tutto il mondo deve essere messo a disposizione un nuovo firmware. Ciò che distingue gli impianti solari da altri dispositivi connessi non è la qualità dei prodotti, bensì il loro ruolo: ciò che in un elettrodomestico resta per lo più un fastidio pesa qui di più, perché gli impianti sono nel complesso rilevanti per il sistema.

Il rischio determinante per la rete elettrica svizzera non risiede dunque nel singolo dispositivo, bensì nella dipendenza da pochi produttori: attraverso la loro infrastruttura cloud gli impianti vengono controllati e ricevono gli aggiornamenti del firmware e, accanto a ciò, la maggior parte dei fornitori mantiene un accesso di manutenzione privilegiato all'intero proprio parco di dispositivi.

La concentrazione del mercato accresce il numero degli impianti interessati: nel 2025 oltre la metà degli inverter installati ex novo è ricaduta su un unico produttore, circa l'80 per cento su quattro (Huawei, Fronius, Sungrow e SolarEdge). Questo rischio non viene eliminato da una migliore sicurezza dei prodotti, bensì soltanto da una riduzione delle dipendenze: garanzie verificabili, più fornitori sul mercato e una limitazione tecnica di ciò che è in generale possibile fare da remoto. A livello internazionale il fotovoltaico distribuito viene trattato sempre più come una questione di infrastruttura critica e non più soltanto di politica climatica. Estonia, Repubblica Ceca e Germania hanno pubblicato avvertimenti delle autorità. Taiwan rende la prova della cibersicurezza parte integrante dell'omologazione dei prodotti, la Lituania vincola l'allacciamento alla rete a requisiti di sicurezza. La Svizzera ha ancora davanti a sé questo passo.

Il rapporto formula raccomandazioni per cinque destinatari.

I gestori di impianti di piccole dimensioni decidono nel modo più efficace con la scelta di un fornitore affermato, al quale affidano, oltre all'installazione, anche l'esercizio tecnico. Alla consegna dovrebbero farsi confermare che sono state impostate password individuali e che l'impianto non è direttamente raggiungibile da Internet, fissare contrattualmente chi è competente per gli aggiornamenti e per il caso di incidente, e rinunciare a un controllo a distanza non necessario.

I gestori di impianti più grandi dispongono di conoscenze specialistiche e di potere negoziale che agli impianti di piccole dimensioni mancano. Dovrebbero inventariare il proprio parco impianti, comprese le interfacce e gli accessi remoti, separare il fotovoltaico, la gestione dell'energia e l'infrastruttura di ricarica dal resto della rete, configurare consapevolmente la controllabilità centrale, disciplinare contrattualmente gli accessi dei produttori e inserire requisiti di sicurezza nei loro bandi di concorso. Dove lo standard minimo TIC non si applica, l'applicazione volontaria è opportuna.

Le aziende installatrici decidono nella pratica il livello di sicurezza del singolo impianto, perché alla messa in servizio nasce ciò che in seguito è attaccabile. Dovrebbero impostare per ogni impianto credenziali individuali e non utilizzare password uniformi per il proprio portafoglio clienti, non rendere l'inverter raggiungibile da Internet, disattivare le interfacce non necessarie e separare l'impianto dal resto della rete domestica o aziendale. La consegna comprende una documentazione della configurazione e un accordo chiaro su chi installerà in futuro gli aggiornamenti. Negli acquisti dovrebbero preferire prodotti che possano funzionare senza cloud, offrano interfacce locali protette e abbiano un periodo di aggiornamento assicurato.

I produttori dovrebbero intendere la sicurezza come principio costruttivo: credenziali specifiche del dispositivo e non ricostruibili, nessun segreto codificato in modo fisso, interfacce locali protette nonché aggiornamenti del firmware firmati. Gli accessi di manutenzione devono essere limitati nel tempo, registrati e revocabili da parte del gestore. Centrale è un blocco preimpostato in fabbrica del controllo a distanza rilevante per la rete elettrica, che possa essere revocato soltanto in loco. Esso limita il livello scalabile per via tecnica e non soltanto organizzativa. E l'esercizio deve restare possibile anche senza cloud.

La politica e le autorità dovrebbero colmare la lacuna per gli impianti di piccole dimensioni. Efficaci sono i requisiti che fanno leva sul prodotto e non sul gestore: requisiti minimi per l'immissione in commercio di inverter e sistemi di gestione dell'energia, requisiti di sicurezza come condizione per l'allacciamento alla rete e una verifica ricorrente che non si esaurisca in un'omologazione una tantum. Altrettanto necessaria è una competenza designata per il rischio che nasce solo dalla somma degli impianti di piccole dimensioni. Il crescente raggruppamento di molti impianti di piccole dimensioni presso aggregatori e centrali elettriche virtuali va al riguardo tenuto d'occhio. Per gli impianti esiste già, con il rapporto di sicurezza, una procedura di controllo obbligatoria che si potrebbe estendere a punti di cibersicurezza.

Una soluzione semplice e completa non esiste; tutti gli approcci hanno vantaggi e svantaggi, e permangono rischi residui.

Il presente rapporto non è un argomento contro il fotovoltaico, bensì uno a favore del suo sviluppo sicuro. Lo sviluppo riduce la necessità di importazioni di energia. Questa indipendenza non dovrebbe però essere sostituita da una nuova dipendenza, dalla dipendenza da pochi produttori con accesso remoto a migliaia di dispositivi rilevanti per la rete elettrica. Lo sviluppo deve poter proseguire, con la stessa esigenza di controllabilità che per altre infrastrutture critiche è oggi già scontata.

2 Situazione di partenza e motivazione

2.1 Da poche grandi centrali a molte centrali piccole

La produzione di energia elettrica in Svizzera si è a lungo basata prevalentemente su un numero contenuto di grandi centrali, gestite centralmente e regolamentate. Esistono sì anche impianti più piccoli, come le piccole centrali idroelettriche, che tuttavia non incidono in misura eccessiva né per numero né per grado di interconnessione. Con lo sviluppo del fotovoltaico è nato accanto a queste un secondo mondo: centinaia di migliaia di piccole «centrali» decentralizzate sui tetti di edifici abitativi e commerciali. Con questo secondo mondo emergono nuovi ciberrischi con ripercussioni sull'intero approvvigionamento elettrico, di cui tratta il presente rapporto.

2.2 Il fotovoltaico è diventato rilevante per il sistema

In Svizzera il fotovoltaico si è trasformato da tecnologia di nicchia in un pilastro portante dell'approvvigionamento elettrico. Alla fine del 2025 erano installati circa 338'000 impianti con una potenza di picco cumulata di circa 9,5 gigawatt. La loro produzione annua di poco meno di 8 terawattora ha coperto il 13,7 per cento del consumo finale di elettricità[1] e corrispondeva così all'incirca alla produzione annua prevista della centrale nucleare di Gösgen.[2]

Più significativo di questi valori annui è il contributo istantaneo nelle ore di punta. Nelle ore di mezzogiorno con cielo sereno il fotovoltaico copre regolarmente oltre la metà del consumo istantaneo, nei giorni di punta nettamente di più. Il 4 luglio 2026 alle ore 14:00, ad esempio, si trattava di circa 6'100 megawatt a fronte di un carico di circa 7'200 megawatt, quindi quasi l'85 per cento[3].

Il fotovoltaico è così diventato rilevante per la sicurezza dell'approvvigionamento. Preso singolarmente, un impianto resta irrilevante per la rete. Nella massa, però, incide, e poiché questi impianti sono interconnessi e configurati in modo simile, possono anche essere influenzati collettivamente: in modo conforme alla destinazione e a supporto della rete da parte del gestore di rete, in modo abusivo da parte di un aggressore. A diventare infrastruttura critica non è quindi il singolo impianto, bensì il parco impianti nel suo insieme.

Questo parco impianti continua a crescere. Il 26 novembre 2025 il Consiglio federale ha fissato per la prima volta nell'ordinanza sull'energia obiettivi intermedi specifici per tecnologia: dei 23 terawattora che le energie rinnovabili senza forza idrica devono apportare entro il 2030, 18,7 spettano al fotovoltaico. Rispetto ai poco meno di 8 terawattora del 2025 si tratta di più di un raddoppio nell'arco di cinque anni. L'obiettivo generale della legge sull'energia richiede per le energie rinnovabili senza forza idrica 35 terawattora entro il 2035 e 45 entro il 2050. Finora il Consiglio federale ha fissato obiettivi intermedi specifici per tecnologia soltanto per il 2030.[4] Con il parco impianti cresce quindi anche l'esigenza di renderlo controllabile.

2.3 Perché finora il tema è stato poco approfondito

A livello internazionale la cibersicurezza degli impianti fotovoltaici ha guadagnato attenzione negli ultimi tempi. I dispositivi diffusi in Svizzera non sono però finora quasi mai stati sottoposti a verifiche indipendenti e sistematiche. Le ragioni sono diverse:

---

[1] Ufficio federale dell'energia UFE, «Statistik Sonnenenergie 2025», https://pubdb.bfe.admin.ch/it/sammlungen/statistik-sonnenenergie

[2] Swissolar, «Solarmonitor Schweiz 2025», https://www.swissolar.ch/it/mercato-e-politica/mercato-svizzera/solarmonitor-svizzera

[3] Valori istantanei: energy-charts.info (Fraunhofer ISE), produzione netta di elettricità in Svizzera, settimana 27/2026 (4 luglio 2026, ore 14:00: carico 7'209 MW, solare 6'121 MW): https://www.energy-charts.info/charts/power/chart.htm?c=CH&l=de&year=2026&week=27

[4] Consiglio federale, comunicato stampa «Bundesrat genehmigt Anpassungen von Verordnungen im Energiebereich» (Il Consiglio federale approva adeguamenti di ordinanze nel settore dell'energia), 26 novembre 2025: https://www.admin.ch/it/newsb/dvb52hRdMmNdS3aNKL96C

- **Scarsi incentivi per i gestori degli impianti**: gli impianti sono gestiti prevalentemente da privati e da piccole imprese. Proprio per i privati è poco probabile che sia in primo piano che cosa renda attaccabile il loro impianto connesso. Se un impianto si ferma a causa di un ciberattacco, essi acquistano l'elettricità mancante. Rapportata a questi costi dell'elettricità, una verifica di sicurezza sarebbe sproporzionatamente costosa. Il rischio vero e proprio nasce solo quando molti impianti vengono manipolati simultaneamente, e allora non colpisce i singoli gestori, bensì l'approvvigionamento elettrico nel suo complesso.
- **Nessuna competenza in capo ai gestori di rete**: essi rispondono della stabilità del sistema complessivo e ne portano quindi il rischio. Attraverso le condizioni di allacciamento possono porre requisiti tecnici, ma per la cibersicurezza degli impianti privati di piccole dimensioni in esercizio manca loro la competenza (cfr. capitolo 7.4).
- **Approvvigionamento oneroso e verifica rischiosa:** i dispositivi sono relativamente cari e onerosi da procurarsi per verifiche indipendenti, e i test richiedono interventi su apparecchi collegati alla rete, in parte sotto tensioni elevate, e quindi particolari misure precauzionali e competenze specialistiche.
- **Trasferibilità limitata degli studi internazionali:** le analisi esistenti provenienti dall'estero riflettono solo in parte le condizioni del mercato svizzero. In parte da noi sono diffusi altri prodotti, e singoli fornitori rilevanti sul mercato svizzero non compaiono affatto nelle ricerche internazionali.

2.4 Perché esiste una ciberminaccia

Rilevante sotto il profilo della sicurezza è soprattutto il fatto che gli impianti moderni sono per lo più collegati a Internet e al cloud del produttore. Ciò rende praticabile influenzare simultaneamente e in modo coordinato un gran numero di impianti. Anche il gestore della rete di distribuzione può in parte comandare molti impianti contemporaneamente, ad esempio per ridurre l'immissione in rete. Questa via si distingue però sotto diversi aspetti: arriva solo fin dove si estende il comprensorio di rete del rispettivo gestore, è in mano a un'impresa regolamentata e utilizza spesso un canale di comando proprio, separato da Internet (telecomando centralizzato). Un cloud del produttore raggiunge invece un parco di dispositivi attraverso Internet, oltre i comprensori di rete e oltre i confini nazionali. Che cosa significherebbe per la stabilità della rete una manipolazione simultanea di molti impianti è trattato nel capitolo *6 Effetti sulla stabilità della rete*.

Questa minaccia incontra condizioni quadro sfavorevoli. I gestori di regola non dispongono di competenze specifiche in materia di cibersicurezza e per l'esercizio dei loro impianti nessuno è tenuto a garantire la cibersicurezza. Mentre i gestori di rete e i produttori di energia elettrica molto grandi soggiacciono a prescrizioni in materia di cibersicurezza come lo standard minimo TIC, gli impianti di piccole dimensioni, e quindi praticamente tutti gli impianti fotovoltaici svizzeri, sfuggono a queste maglie. Per i produttori di energia elettrica lo standard si applica solo a partire da 100 MW, ossia da 100'000 kW. Un tipico impianto sul tetto si colloca nell'ordine delle decine di kilowatt e quindi oltre mille volte più in basso.

Questa valutazione è condivisa dalla società di rete nazionale. Nel suo white paper «Systemverträgliche Integration Photovoltaik»[5] (Integrazione del fotovoltaico compatibile con il sistema) Swissgrid annovera espressamente i rischi di cibersicurezza tra le sfide dell'esercizio del sistema: gli inverter e altri impianti come le stazioni di ricarica e i sistemi di gestione dell'energia sarebbero sempre più controllabili a distanza tramite Internet. Prescrizioni insufficienti e una scarsa consapevolezza del problema aumenterebbero il rischio che attori esterni destabilizzino per questa via il sistema elettrico.

2.5 Il contesto di politica di sicurezza

Questa situazione di partenza tecnica coincide con un contesto di politica di sicurezza in via di

[5] Swissgrid SA, white paper «Systemverträgliche Integration Photovoltaik» (Integrazione del fotovoltaico compatibile con il sistema), marzo 2026, https://www.swissgrid.ch/it/home/newsroom/blog/2026/20260330-01.html

inasprimento. Nel suo rapporto sulla situazione «La sicurezza della Svizzera 2026»[6] il Servizio delle attività informative della Confederazione (SIC) constata un peggioramento marcato e duraturo del contesto di politica di sicurezza. Le infrastrutture critiche vi sono espressamente classificate come minacciate sia da attacchi fisici sia da ciberattacchi. Il SIC rileva inoltre che le infrastrutture dei Paesi europei non possono essere considerate isolatamente. Un attacco all'infrastruttura svizzera per colpire altri Stati che ne dipendono sarebbe altrettanto ipotizzabile quanto, all'inverso, danni collaterali derivanti da attacchi a infrastrutture estere. Il SIC segnala inoltre che l'attrattiva di simili obiettivi cresce quanto più gli Stati della NATO e dell'UE proteggono la propria infrastruttura critica senza che la Svizzera faccia altrettanto.

Che questa valutazione non sia astratta lo dimostra il ciberattacco coordinato all'approvvigionamento energetico e termico polacco del dicembre 2025. Tra le realtà colpite figurano oltre 30 parchi eolici e fotovoltaici[7]. Il Regno Unito e l'UE hanno attribuito ufficialmente l'attacco, nel luglio 2026, al servizio segreto russo FSB (Centro 16).[8] Sullo sfondo delle reti europee strettamente interconnesse e della valutazione del SIC, sviluppi analoghi sono rilevanti anche per la Svizzera.

Che il fotovoltaico distribuito sia concretamente nel mirino lo dimostra un avviso di sicurezza congiunto dell'Ufficio federale tedesco per la protezione della Costituzione (BfV) e dell'Ufficio federale tedesco per la sicurezza informatica (BSI) del 3 giugno 2026[9]. Secondo le loro constatazioni, attori cibernetici russi svolgono attivamente attività di ricognizione su impianti fotovoltaici collegati a Internet senza protezione. Al centro dell'attenzione vi sono i sistemi di monitoraggio, che consentono anche un accesso di comando agli impianti. Sono interessati prevalentemente impianti di privati e di cooperative senza un retroterra nel settore energetico. In una parte di questi impianti l'accesso è possibile senza credenziali, e le versioni del software sono in parte molto datate. Si tratta di attività di ricognizione e non di un attacco. L'avviso mostra però che proprio quella classe di impianti che il presente rapporto esamina viene rilevata sistematicamente da attori statali.

2.6 Delimitazione: sistemi di accumulo a batteria, infrastruttura di ricarica e altri dispositivi connessi

Non sono oggetto della presente analisi, ma acquistano importanza crescente, i consumatori e gli accumulatori connessi come i sistemi di accumulo a batteria, le stazioni di ricarica per veicoli elettrici e le pompe di calore. Proprio i sistemi di accumulo a batteria si stanno diffondendo rapidamente. Nei nuovi impianti fotovoltaici sulle case unifamiliari svizzere una quota considerevole è ormai dotata di un accumulatore.[10] Dal punto di vista della cibersicurezza sono particolarmente rilevanti gli attacchi che sfruttano il fotovoltaico in combinazione con i sistemi di accumulo a batteria o con l'infrastruttura di ricarica, poiché in questo modo si possono manipolare sia l'immissione in rete sia il prelievo. L'infrastruttura di ricarica è già stata esaminata dall'NTC in un rapporto precedente[11].

[6] Servizio delle attività informative della Confederazione (SIC), «La sicurezza della Svizzera 2026»: https://www.vbs.admin.ch/it/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, comunicazione sulle sanzioni del 13 luglio 2026: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions
[9] Ufficio federale tedesco per la protezione della Costituzione (BfV) e Ufficio federale tedesco per la sicurezza informatica (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure» (Avviso di sicurezza congiunto: ricognizione di impianti fotovoltaici mal protetti da parte di attori cibernetici statali), 3 giugno 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html
[10] Ufficio federale dell'energia UFE, «Statistik Sonnenenergie 2025», https://pubdb.bfe.admin.ch/it/sammlungen/statistik-sonnenenergie
[11] Istituto nazionale di test per la cibersicurezza NTC, rapporto sulla cibersicurezza dell'infrastruttura di ricarica, 2023: https://it.ntc.swiss/news/2023-analisi-mobilita-elettrica-infrastrutture-di-ricarica

3 L'ecosistema di un impianto fotovoltaico

Questo capitolo descrive di quali elementi si compone un impianto fotovoltaico. Spiega come questi comunicano tra loro e con Internet e chi può controllarli. L'esposizione resta deliberatamente descrittiva e mostra dove l'architettura offre una superficie di attacco. Se queste superfici si siano poi effettivamente rivelate un rischio nella verifica non è tema di questo capitolo. Quali componenti siano stati verificati e perché è indicato nel capitolo *4 Metodologia*. I risultati seguono nel capitolo *5 Rilievi e rischi*.

3.1 I componenti e la loro interazione

Un tipico impianto fotovoltaico è composto da pochi elementi di base. A seconda della costruzione, questi sono integrati fra loro in misura diversa. Per la trattazione seguente vengono rappresentati separatamente in base alla loro funzione. I **moduli solari** producono corrente continua (DC). L'**inverter** la converte in corrente alternata (AC) conforme alla rete e la immette nella rete. È quindi il componente centrale dell'impianto, attivamente controllabile. Per il monitoraggio remoto l'inverter viene collegato a Internet tramite un **modulo di comunicazione** (spesso già integrato nell'inverter), per lo più via Wi-Fi, rete mobile o cavo. Questo collegamento non è tecnicamente indispensabile, nella pratica è però la regola. Negli impianti moderni la sorveglianza avviene per lo più tramite il portale Internet del produttore e, dove non è installato alcun modulo di comunicazione oppure dove vengono controllati anche altri dispositivi come sistemi di accumulo a batteria, stazioni di ricarica o pompe di calore, si occupa spesso della comunicazione verso l'esterno un **sistema di gestione dell'energia**. Attraverso questo collegamento i dati di esercizio confluiscono in un **cloud del produttore**, che li memorizza e li visualizza. A seconda del produttore, esso consente inoltre il monitoraggio remoto, il controllo a distanza e l'aggiornamento del firmware dell'impianto. L'**app mobile o web**, infine, è l'interfaccia di comando per il gestore e accede a sua volta al cloud. In aggiunta sono spesso integrati altri consumatori e accumulatori connessi, ad esempio **sistemi di accumulo a batteria**, **stazioni di ricarica per veicoli elettrici, oppure pompe di calore**. Simili componenti supplementari accrescono ulteriormente la superficie di attacco e le possibili ripercussioni. Nel punto di raccordo alla rete si trova inoltre il contatore del gestore della rete di distribuzione. Esso misura l'energia prelevata e quella immessa e in Svizzera viene progressivamente sostituito da un sistema di misurazione intelligente (**smart meter**), che rende i valori di misura leggibili a distanza. Il contatore non appartiene al gestore dell'impianto, bensì al gestore di rete, e costituisce quindi un collegamento verso l'esterno proprio e indipendente dal produttore.

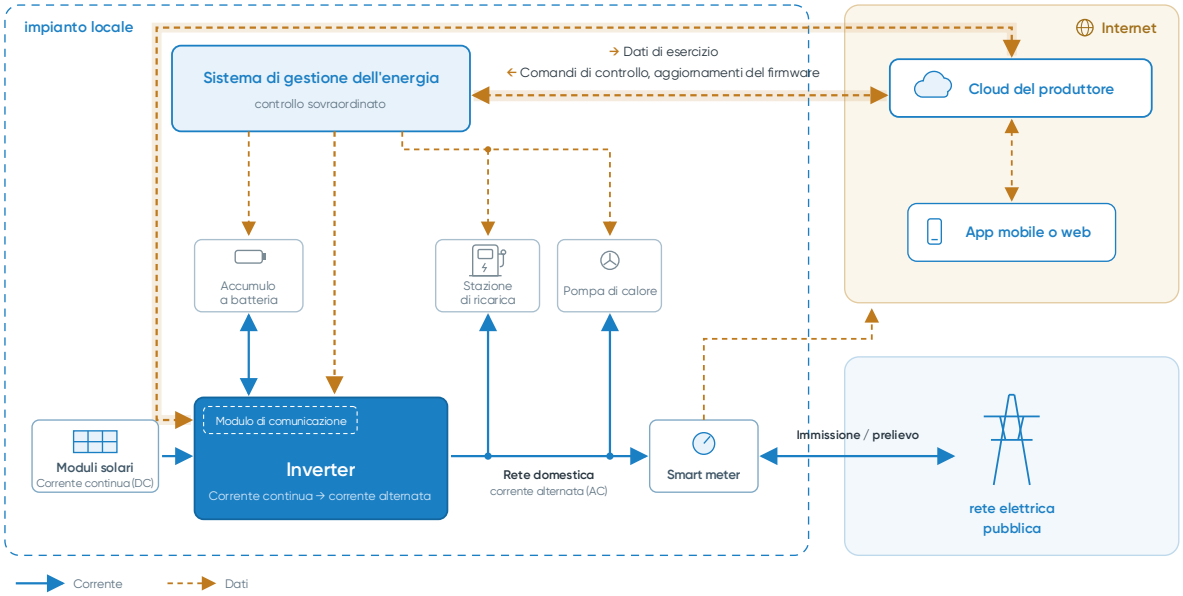


Figura 1: panoramica schematica di un tipico impianto fotovoltaico

3.2 Inverter e sistema di gestione dell'energia

Per comprendere la controllabilità è centrale la distinzione tra inverter e sistema di gestione dell'energia (EMS), perché nel linguaggio corrente i due termini vengono spesso confusi.

L'**inverter** converte la corrente e la immette nella rete. Attraverso le sue funzioni a supporto della rete, come le prescrizioni di potenza attiva e reattiva o le curve caratteristiche, è l'elemento che influenza direttamente l'immissione in rete.

Il **sistema di gestione dell'energia** è un controllo di livello superiore. Coordina più dispositivi di un impianto, tipicamente inverter, sistema di accumulo a batteria, stazione di ricarica e pompa di calore, e ne ottimizza l'esercizio, ad esempio in funzione del consumo proprio.

Ne deriva un duplice carattere che rende l'EMS particolarmente significativo per la cibersicurezza. Come parte della soluzione, un EMS può ridurre la dipendenza dai singoli cloud dei produttori: non ogni dispositivo deve essere necessariamente collegato al cloud del proprio produttore, e un EMS collocato in modo sensato tra la rete locale e l'inverter può limitare la raggiungibilità diretta dei singoli apparecchi. Come aggravamento del problema vale però quanto segue: chi controlla l'EMS controlla tutti i dispositivi a esso collegati e può quindi arrecare almeno altrettanti danni quanti ne arrecherebbe tramite un singolo inverter, potenzialmente di più, perché l'EMS controlla anche altri componenti come il sistema di accumulo a batteria e la stazione di ricarica. I fornitori di EMS indipendenti dal produttore aggregano inoltre questo controllo attraverso marche di dispositivi diverse. Nel suo nucleo l'EMS è quindi un componente locale, ma al tempo stesso un punto di concentrazione la cui compromissione ha una portata maggiore di quella di un singolo inverter.

3.3 Vie di comunicazione e vulnerabilità note

Rilevanti per la sicurezza sono due domande: quali componenti comunicano tra loro e quanto bene sono protette queste connessioni. Il modulo di comunicazione trasmette i dati di esercizio al cloud del produttore e da lì riceve comandi. L'app accede tipicamente a sua volta al cloud, non direttamente all'impianto. Se il modulo di comunicazione è integrato nell'inverter, questa connessione si svolge all'interno del dispositivo. È diverso non appena un dispositivo esterno deve comunicare direttamente con l'inverter, ad esempio un sistema di gestione dell'energia. In tal caso la connessione passa localmente per la rete dell'edificio o per la rete domestica.

Per questa connessione locale sono diffusi protocolli industriali, in primo luogo Modbus: in passato tramite un collegamento seriale via cavo (RS485), sempre più tramite la rete (Modbus TCP). Accanto a essi si incontrano protocolli proprietari dei produttori. Modbus è stato concepito per impianti isolati e di per sé non offre né cifratura né autenticazione. Singoli produttori aggiungono meccanismi di autorizzazione proprietari. Un'estensione di sicurezza su base TLS, aggiunta nel 2018, è nella pratica poco diffusa. Per questo motivo tale interfaccia è rilevante per i rilievi descritti più avanti.

Secondo questa architettura l'inverter non è direttamente raggiungibile da Internet. La via dall'esterno passa invece per il cloud del produttore. Il cloud del produttore, a sua volta, può per costruzione monitorare, controllare e aggiornare contemporaneamente moltissimi impianti.

Questo quadro coincide con la ricerca esistente. Un'analisi[12] di 93 vulnerabilità divulgate dal 2012 con numero CVE presso 34 produttori attribuisce la maggior parte al livello di monitoraggio e cloud, circa il 38 per cento al solar monitoring e circa il 25 per cento al cloud, mentre l'inverter con modulo di comunicazione era interessato per quasi il 30 per cento. Circa l'80 per cento di tutti i casi è considerato elevato o critico. Queste cifre vanno lette con cautela, perché contano casi rilevati e non rischio, e il livello connesso è incomparabilmente più facile da verificare a distanza. Non restano però teoriche: sei delle vulnerabilità catalogate vengono sfruttate regolarmente da botnet dal 2022. Determinante alla fine è meno il numero delle vulnerabilità che il fatto che un unico cloud raggiunge contemporaneamente moltissimi impianti.

[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

3.4 Controllo centrale e controllo locale

Gli elementi costitutivi si possono ordinare in base a quanti impianti può influenzare un componente compromesso. Un'istanza centrale come il cloud del produttore agisce su molti impianti contemporaneamente. Chi la controlla può inviare comandi a tutti i dispositivi collegati. Un'istanza locale come l'inverter stesso, l'app mobile o un'unità di comando locale influenza invece soltanto il proprio impianto. Questa distinzione separa gli attacchi scalabili, che colpiscono a distanza molti impianti, dagli attacchi non scalabili, che restano limitati al singolo impianto. È la ragione per cui i singoli piccoli impianti sono di per sé irrilevanti, ma diventano rilevanti nella massa interconnessa. Per una manipolazione con effetti sulla rete il livello centrale è l'obiettivo di attacco più interessante per un aggressore. Questa controllabilità centrale si può però anche limitare deliberatamente per via tecnica. Il rapporto raccomanda pertanto di concepire i dispositivi in modo che il cloud possa soltanto monitorare l'impianto e rifornirlo di aggiornamenti firmati, ma non più controllarlo (cfr. capitolo *8.4.2*).

Accanto al cloud del produttore si aggiunge sempre più un secondo livello di controllo centrale: gli aggregatori e le centrali elettriche virtuali. In questo caso un fornitore raggruppa molti impianti distribuiti tramite interfacce Internet e commercializza la loro potenza aggregata, ad esempio come energia di bilanciamento. Un esempio è il progetto pilota «PV4Balancing»[13] della società di rete nazionale Swissgrid, nel quale impianti fotovoltaici aggregati riducono su richiesta la loro immissione in rete come riserva terziaria negativa. Ancora più vicino alla massa degli impianti di piccole dimensioni è un secondo esempio: Helion ha ottenuto da Swissgrid l'autorizzazione a raggruppare tramite la propria piattaforma impianti fotovoltaici privati di piccole dimensioni, accumulatori domestici e stazioni di ricarica e a offrire la potenza aggregata sul mercato dell'energia di bilanciamento[14]. Finiscono così sotto un controllo a distanza centrale proprio quegli impianti che singolarmente non soggiacciono ad alcun requisito di cibersicurezza. L'aggregatore stesso è invece coperto non appena può accedere ad almeno 100 MW tramite un unico sistema (cfr. capitolo *7.4).* Il «Flexpool»[15] di CKW, ad esempio, riunisce già oltre 1'000 MW provenienti da circa 1'700 impianti di clienti in un unico punto di controllo, sebbene tecnologicamente misti e non composti unicamente da fotovoltaico. Questo sviluppo è a doppio taglio: impiegati a supporto della rete, gli impianti controllabili e aggregati sono uno strumento di stabilizzazione. Al tempo stesso, con l'aggregatore nasce un ulteriore punto di controllo centrale che, in caso di compromissione, apre un controllo a distanza già coordinato su molti impianti. Questo raggruppamento non è un sottoprodotto, bensì parte dell'architettura di destinazione. Swissgrid rileva che la partecipazione di unità decentralizzate ai mercati dell'energia di bilanciamento dovrebbe avvenire attraverso aggregatori nel modo più agevole possibile, e indica come variante più idonea una piattaforma di flessibilità centrale con meccanismo di coordinamento. Ciò viene sperimentato in un ulteriore progetto pilota, la «TSO-DSO-Koordination».[16] Il numero di impianti raggiungibili attraverso un singolo punto di controllo dovrebbe crescere ulteriormente. Tanto più importante è chiarire i requisiti di sicurezza per questo livello finché esso è ancora in fase di costruzione. L'NTC non ha verificato queste piattaforme; la valutazione riguarda la struttura, non la sicurezza dei singoli fornitori.

[13] Swissgrid, progetto pilota «PV4Balancing»: https://www.swissgrid.ch/it/home/newsroom/blog/2025/20250225-01.html
[14] Helion Energy AG, centrale elettrica virtuale per clienti privati basata sulla piattaforma «Helion ONE»: https://www.gebaeudetechnik.ch/de/news/virtuelles-kraftwerk-fuer-die-schweiz--252
[15] CKW (Gruppo Axpo), «Flexpool»: https://www.ckw.ch/ueber-ckw/medienstelle/medienmitteilungen/2025/1000-megawatt-virtuelles-grosskraftwerk-von-ckw-erreicht-meilenstein
[16] Swissgrid SA, white paper «Systemverträgliche Integration Photovoltaik» (Integrazione del fotovoltaico compatibile con il sistema), marzo 2026, https://www.swissgrid.ch/it/home/newsroom/blog/2026/20260330-01.html

3.5 Tipi di impianto e gestori

Il collegamento in rete e il livello di protezione dipendono fortemente dal tipo di impianto. In analogia alle categorie di promozione della Confederazione, gli impianti fino a 100 kW sono considerati **impianti di piccole dimensioni**: comprendono case unifamiliari, case plurifamiliari e piccoli edifici commerciali. Gli impianti di piccole dimensioni si trovano per lo più nella normale rete dell'edificio o rete domestica e sono gestiti da privati o da piccole imprese, che di regola non dispongono di competenze specifiche in materia di cibersicurezza. Gli **impianti di grandi dimensioni** oltre i 100 kW sono più spesso seguiti da professionisti e segmentati dietro un firewall. Gli impianti più grandi sono collegati a una sottostazione propria e al gestore della rete di distribuzione e rinunciano più spesso a un collegamento al cloud del produttore. Al contrario, per gli impianti di piccole dimensioni il collegamento al cloud è sì la regola, ma nemmeno lì è obbligatorio.

2025	N. impianti	Potenza in MW	Ø Potenza in kW
fino a 4 kW	1'132	3,0	2,7
oltre 4 kW fino a 10 kW	9'073	68,9	7,6
oltre 10 kW fino a 20 kW	14'864	211,9	14,3
oltre 20 kW fino a 30 kW	4'831	117,8	24,4
oltre 30 kW fino a 50 kW	3'134	119,8	38,2
oltre 50 kW fino a 100 kW	1'977	138,9	70,3
oltre 100 kW fino a 1000 kW	2'175	536,2	246,6
oltre 1000 kW	72	136,4	1'882,5
Totale impianti allacciati alla rete	**37'257**	**1'332,9**	**35,8**

Figura 2: impianti allacciati alla rete per classe di grandezza. Fonte: Statistik Sonnenenergie 2025[17], UFE

La ripartizione per dimensione mostra chiaramente la sproporzione. Dei 37'257 impianti allacciati alla rete installati ex novo nel 2025, 35'011, ossia il 94 per cento, si collocavano al massimo a 100 kW. A essi è andata circa la metà della potenza installata ex novo. L'impianto medio misura circa 25 kW, la mediana circa 11 kW. Al tempo stesso circa il 40 per cento della produzione fotovoltaica svizzera proviene da impianti sotto i 30 kW. Il parco impianti per il quale non valgono prescrizioni operative di cibersicurezza copre quindi una parte considerevole della produzione.

3.6 Concentrazione del mercato

Rilevante per la sicurezza non è soltanto quanti impianti siano installati, bensì da quanti produttori diversi provengano: firmware, accessi di manutenzione e catena di aggiornamento sono determinati dal produttore, motivo per cui un singolo rilievo può valere per l'intero parco dispositivi di quest'ultimo, anche per impianti senza collegamento al cloud. In Svizzera questo campo si è spostato più volte. Il PV-Barometer 2026[18] analizza a tal fine le progettazioni: nel 2017 Fronius deteneva il 45,7 per cento di quota di mercato; nel 2020 il mercato si ripartiva su tre fornitori di dimensioni simili (FIMER 23,5 per cento, Fronius 22,9, SolarEdge 22,8); nel 2025 a Huawei è andato il 52,3 per cento, a Fronius il 13,3, a Sungrow il 9,2 e a SolarEdge l'8,2 per cento. La quota del maggiore fornitore è quindi oggi più alta che mai nel periodo di osservazione. Il numero dei fornitori non è però diminuito; a cambiare è stata la ripartizione.

[17] Ufficio federale dell'energia UFE, «Statistik Sonnenenergie 2025», https://pubdb.bfe.admin.ch/it/sammlungen/statistik-sonnenenergie
[18] Berner Fachhochschule & Eturnity AG, «PV-Barometer 2026»: https://www.pv-barometer.ch/

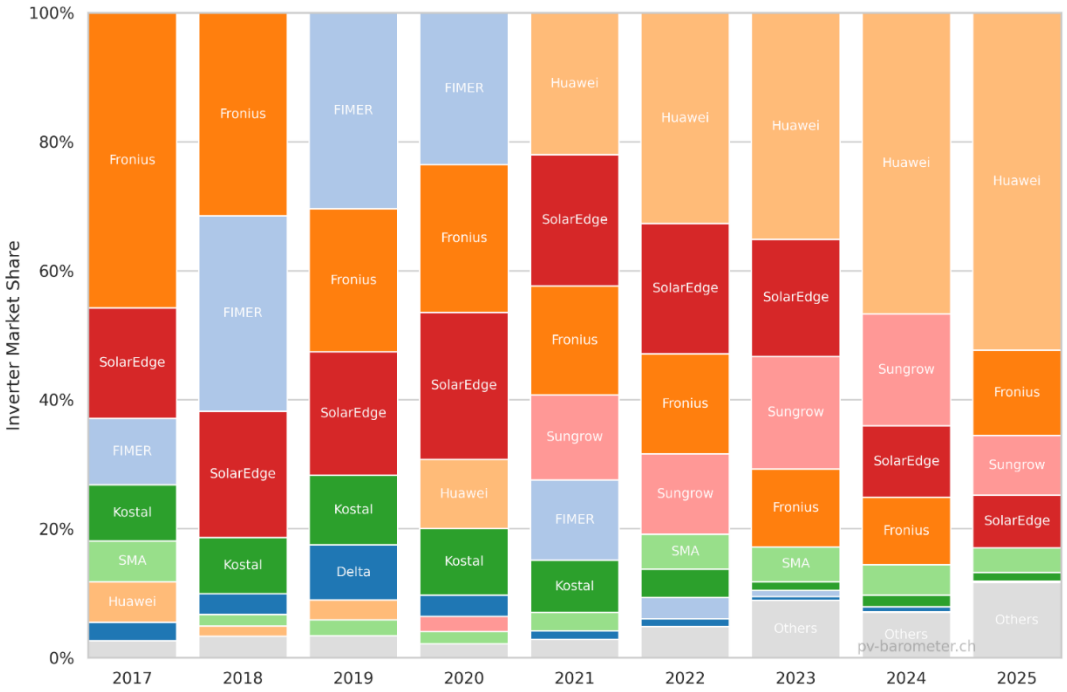


Figura 3: quote di mercato dei produttori di inverter in Svizzera. Fonte: PV-Barometer 2026

4 Metodologia

L'NTC ha sottoposto inverter e sistemi di gestione dell'energia a un'analisi tecnica di sicurezza approfondita. La verifica è stata orientata a tre principi:

- **Vicinanza al mercato:** una selezione dei dispositivi orientata alla loro diffusione sul mercato svizzero.
- **Indipendenza:** nessun coinvolgimento dei produttori nella selezione, nello svolgimento e nel finanziamento; contatti esclusivamente nell'ambito della segnalazione delle vulnerabilità.
- **Scalabilità:** concentrazione sulle vulnerabilità con cui è possibile manipolare molti impianti contemporaneamente.

Nell'arco di circa un anno l'NTC ha dedicato all'indagine complessivamente circa 1'300 ore di lavoro. L'indagine è stata sostenuta da numerose organizzazioni del settore energetico, che hanno messo a disposizione dispositivi di test e hanno partecipato ai costi. I produttori dei prodotti verificati non vi hanno preso parte. Le sezioni seguenti descrivono l'oggetto dell'indagine e la sua delimitazione, la selezione e l'approvvigionamento dei dispositivi, la configurazione di test, il focus analitico nonché il trattamento delle vulnerabilità riscontrate.

4.1 Oggetto dell'indagine e delimitazione

Il focus della verifica è stato posto deliberatamente sugli inverter e sui sistemi di gestione dell'energia nonché sugli impianti in edifici abitativi e in piccoli edifici commerciali. Entrambe le scelte derivano dall'architettura descritta nel capitolo *3 L'ecosistema di un impianto fotovoltaico*: gli inverter e i sistemi di gestione dell'energia sono i componenti centrali di un impianto fotovoltaico, collegati alla rete e al cloud, e possono controllare attivamente l'immissione in rete. Tali impianti di piccole dimensioni, a loro volta, non soggiacciono ad alcuna prescrizione operativa di cibersicurezza. Sul versante del prodotto, per i dispositivi immessi in commercio ex novo valgono da agosto 2025 i requisiti di cibersicurezza della direttiva UE sulle apparecchiature radio, se dispongono di un'interfaccia radio (cfr. capitolo *7.3.2*). Questi fissano un livello di base, ma non dicono nulla sulla configurazione, sull'esercizio e sulla manutenzione dell'impianto installato e si fondano sull'autodichiarazione del produttore. Gli impianti sono gestiti per lo più da privati o da piccole imprese senza competenze specifiche in materia di cibersicurezza, e finora non sono quasi mai stati verificati in modo indipendente.

Deliberatamente non sono stati esaminati i moduli solari. Alcuni moduli contengono sì elettronica attiva come gli ottimizzatori di modulo. Questi sono però collegati, ammesso che siano connessi in rete, soltanto all'inverter e si collocano quindi al di fuori del quadro di attacco scalabile. Non facevano inoltre parte dell'indagine componenti come smart meter, sistemi di accumulo a batteria e stazioni di ricarica per l'elettromobilità. Anche questi componenti sono rilevanti per la sicurezza e acquistano importanza: i sistemi di accumulo a batteria, ad esempio, sono collegati alla rete e al cloud in modo analogo agli inverter, e una carica o scarica coordinata di molti accumulatori avrebbe un effetto paragonabile sulla rete.

Al di fuori della portata dell'indagine si collocavano inoltre i dispositivi fotovoltaici da presa di dimensioni molto ridotte («impianti da balcone»). Sul mercato svizzero sono nettamente meno diffusi che in Germania e sono già oggetto di studi indipendenti. Che anche in questa categoria esistano vulnerabilità da prendere sul serio lo mostrano ad esempio le vulnerabilità radio divulgate dal Chaos Computer Club (CCC)[19] dei microinverter Hoymiles (2026) (cfr. capitolo *5.3.4*).

Il quadro giuridico ha concorso a determinare la profondità della verifica. I dispositivi stessi sono stati acquistati dall'NTC, che ha potuto esaminarli senza restrizioni. I cloud dei produttori sono invece sistemi altrui, in esercizio produttivo: gli accessi a essi possono essere punibili ai sensi dell'art. 143bis del Codice penale CP senza il consenso del gestore. Una perizia giuridica

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

commissionata dall'NTC nel 2023[20] delimita quali attività di verifica siano ammissibili senza tale consenso.

Un consenso sarebbe stato ottenibile soltanto tramite i produttori. Ciò avrebbe comportato il loro coinvolgimento nell'indagine e sarebbe stato in contrasto con il principio dell'indipendenza. L'NTC si è pertanto limitato deliberatamente al quadro ammissibile senza consenso e ha rinunciato a una verifica approfondita del livello cloud.

Il presente rapporto valuta la fattibilità tecnica, non l'intenzione di possibili attori e non lo svolgimento di una gestione di crisi.

4.2 Selezione dei dispositivi

Una statistica completa degli inverter installati nel Paese non esiste. Sul numero di impianti e sulla distribuzione della potenza sono disponibili dati ufficiali (statistiche Pronovo[21], Statistik Sonnenenergie[22] dell'UFE). Per le quote di mercato dei produttori esiste invece soltanto la rilevazione del PV-Barometer, di cui risponde un operatore del mercato, che tuttavia indica le quote annualmente dal 2017 e rende così visibile l'evoluzione nel tempo. Non se ne possono ricavare cifre esatte, ma sì ordini di grandezza, e questi sono univoci. Nel 2025 poco più della metà degli inverter installati ex novo è ricaduta su un unico produttore, circa due terzi su due e circa l'80 per cento su quattro. Sono stati perciò esaminati sette inverter di sei produttori, tra cui i fornitori che determinano il mercato.

Per i sistemi di gestione dell'energia la disponibilità di dati è ancora più scarsa. Una statistica comparabile non esiste. Determinanti sono stati qui i colloqui con specialisti del settore. Sono stati verificati quattro sistemi.

La selezione copre così entrambi gli orizzonti temporali. Guardando all'indietro aiuta la considerazione pluriennale: poiché la maggior parte del parco impianti svizzero è stata costruita soltanto negli ultimi anni, le quote di mercato di questi anni riproducono approssimativamente il parco installato. Guardando in avanti, ciò che viene installato oggi determina il rischio per più di un decennio.

4.3 Approvvigionamento

I dispositivi sono stati acquistati tramite organizzazioni partner e per la stessa via che utilizzerebbe anche una clientela ordinaria. Questo modo di procedere garantisce che siano stati verificati stati di consegna e configurazioni reali e non campioni di prova appositamente predisposti. I contatti con i produttori sono avvenuti esclusivamente nell'ambito della segnalazione delle vulnerabilità.

La verifica è avvenuta su iniziativa dell'NTC. Concezione, svolgimento e valutazione sono stati interamente a carico dell'NTC e hanno avuto luogo nel suo laboratorio. È stata finanziata in misura sostanziale con mezzi dell'NTC, integrati da diverse organizzazioni partner del settore energetico che hanno partecipato ai costi e messo a disposizione dispositivi di test. I produttori non vi hanno preso parte e le organizzazioni partner non hanno avuto alcuna influenza sulla portata della verifica e sui risultati.

4.4 Configurazione di test

Per l'esercizio degli inverter è necessaria un'alimentazione in corrente continua sul lato d'ingresso. Poiché l'esercizio di moduli solari reali in laboratorio non è praticabile, i moduli sono stati sostituiti

[20] Walder Wyss AG, «Rechtsgutachten zur Strafbarkeit von Ethical Hacking» (Perizia giuridica sulla punibilità dell'ethical hacking): https://www.walderwyss.com/it/news/2023-06-26_rechtsgutachten-zur-strafbarkeit-von-fuer-das-nationale-testinstitut-fuer-cybersicherheit-ntc
[21] Pronovo AG, statistiche: https://pronovo.ch/it/servizi/rapporti-e-pubblicazioni/
[22] Ufficio federale dell'energia UFE, «Statistik Sonnenenergie 2025», https://pubdb.bfe.admin.ch/it/sammlungen/statistik-sonnenenergie

da una sorgente di corrente continua controllabile. In questo modo i dispositivi hanno potuto essere verificati in condizioni riproducibili. Il focus è stato posto sull'analisi di firmware, interfacce, collegamento al cloud e configurazione. Resta una riserva di fondo: un dispositivo potrebbe cambiare il proprio comportamento non appena riconosce di essere sottoposto a verifica. Una simile modalità da banco di prova non sarebbe necessariamente riconoscibile con un approccio di laboratorio. L'NTC è consapevole di questa possibilità e vi ha contrapposto quanto era fattibile: i dispositivi sono stati acquistati attraverso i canali di distribuzione ordinari e fatti funzionare nello stato di consegna, e la configurazione di test è stata concepita in modo da differenziarsi il meno possibile da un'installazione reale.

4.5 Focus sulle vulnerabilità scalabili

Al centro dell'analisi si sono trovate le vulnerabilità con cui è possibile manipolare contemporaneamente un gran numero di impianti. Le vulnerabilità che riguardano soltanto il singolo impianto, ad esempio quelle che presuppongono l'accesso fisico al dispositivo, non erano al centro dell'analisi. Questa distinzione tra vulnerabilità scalabili e non scalabili attraversa l'intero rapporto e determina il peso attribuito ai singoli rilievi.

4.6 Processo di segnalazione delle vulnerabilità

Tutte le vulnerabilità identificate sono state segnalate in via confidenziale ai produttori interessati nell'ambito di un processo di divulgazione coordinata (responsible disclosure), per consentirne l'eliminazione prima della pubblicazione. Questo modo di procedere corrisponde alla responsible disclosure policy[23] dell'NTC e alla prassi corrente nel settore. Il presente rapporto pubblico rinuncia pertanto deliberatamente a dettagli tecnici e all'indicazione dei prodotti interessati e illustra invece gli schemi di rischio soggiacenti.

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

5 Rilievi e rischi

5.1 Panoramica

L'NTC ha esaminato undici prodotti: sette inverter di sei produttori e quattro sistemi di gestione dell'energia. Due dei sistemi di gestione dell'energia provengono da produttori che fabbricano anche uno degli inverter verificati, sicché gli undici prodotti si ripartiscono su otto produttori. Complessivamente sono state identificate oltre 50 vulnerabilità, di cui sette con criticità «critico» e sei con «elevato». Almeno un rilievo elevato o critico è ricaduto su cinque degli undici prodotti.

In quattro prodotti l'NTC ha ottenuto il controllo completo del dispositivo, ossia il livello di privilegi più alto (accesso root). In un prodotto vi hanno condotto tre vulnerabilità che consentono l'esecuzione di codice di programma arbitrario sul dispositivo (Remote Code Execution) e che sono tutte classificate come critiche. In tre prodotti è bastato a tale scopo un accesso di manutenzione del produttore protetto in modo insufficiente. Questo livello di privilegi è significativo perché non consente soltanto di controllare l'impianto, bensì di modificare il firmware e con esso il comportamento complessivo del dispositivo.

Sei degli oltre 50 rilievi agiscono attraverso un'istanza centrale su molti impianti contemporaneamente e sono quindi scalabili. I restanti rimangono limitati al singolo impianto. Questi sei sono la parte della statistica determinante per la stabilità della rete, perché una vulnerabilità diventa rilevante per la rete non per la sua gravità tecnica, bensì per il fatto di poter essere applicata a un intero parco di dispositivi. Anche il BSI, nel suo avviso[24] del giugno 2026, indica espressamente l'«utilizzo di effetti di scala» come via dal singolo impianto alla stabilità della rete. Due dei sei rilievi sono classificati come «critico», uno come «elevato» e tre come «medio». Questa classificazione valuta l'effetto sul prodotto verificato e non le conseguenze per la rete elettrica. Un rilievo classificato come «medio» in un cloud che controlla un parco di dispositivi può pesare sul lato rete più di un rilievo critico sul singolo dispositivo. Cinque dei sei rilievi provengono dal livello con la maggiore leva, il cloud del produttore, e precisamente da interfacce raggiungibili dall'esterno. Una verifica approfondita del cloud stesso non è stata possibile per motivi giuridici (cfr. capitolo *4.1*). Già la vista dall'esterno è però bastata a trovare vulnerabilità con portata estesa a tutta la rete.

Per una parte dei rilievi, tra cui diversi di quelli critici, il processo di divulgazione coordinata non è ancora concluso al momento della pubblicazione. Ciò dipende dalla natura della cosa e non da una cooperazione carente: sono interessate in parte più serie di modelli in tutto il mondo, che necessitano di un nuovo firmware.

Il livello di sicurezza dei singoli prodotti non è peraltro generalmente peggiore di quello di altri dispositivi molto diffusi dell'«Internet of Things» (IoT), in singoli aspetti è addirittura migliore. Questa valutazione si fonda sull'esperienza di verifica dell'NTC con classi di dispositivi comparabili, segnatamente sulle verifiche di periferiche[25] e di prodotti nel campo di applicazione della direttiva RED[26]. Vanno però presi sul serio gli schemi ricorrenti e soprattutto i rischi strutturali, che dominano il quadro complessivo e sono al centro di questo capitolo. Proprio qui sta il nocciolo: ciò che negli elettrodomestici connessi resta un fastidio riguarda qui una classe di dispositivi che nel complesso è rilevante per il sistema.

Che queste debolezze non esistano soltanto in laboratorio lo confermano le autorità di sicurezza tedesche: esse osservano impianti fotovoltaici in cui l'accesso è in parte possibile senza credenziali e le cui versioni del software sono molto datate (cfr. capitolo *2.5*).

---

[24] Ufficio federale tedesco per la protezione della Costituzione (BfV) e Ufficio federale tedesco per la sicurezza informatica (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure» (Avviso di sicurezza congiunto: ricognizione di impianti fotovoltaici mal protetti da parte di attori cibernetici statali), 3 giugno 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

[25] NTC, rapporto sommario sulla cibersicurezza delle periferiche: https://it.ntc.swiss/news/2026-rapporto-periferiche

[26] NTC, rapporto sulla cibersicurezza dei dispositivi connessi in relazione alla direttiva RED: https://it.ntc.swiss/news/2025-relazione-red

5.2 Due prospettive sulla minaccia

I rilievi vanno letti sullo sfondo di due prospettive di minaccia fondamentalmente diverse:

- **L'attaccabilità da parte di terzi**: vulnerabilità tecniche che un aggressore esterno sfrutta. Si presenta presso tutti i produttori e si può ridurre con una migliore qualità del prodotto e con verifiche indipendenti.
- **Il produttore o la sua catena di approvvigionamento come aggressore:** Qui non si tratta di vulnerabilità tecniche, bensì di dipendenze. I mezzi legittimi della manutenzione remota e della distribuzione del firmware possono essere abusati dal produttore stesso, da un aggressore che compromette il produttore, da collaboratori malintenzionati oppure in seguito a un'ingiunzione statale nei confronti del produttore. Questo rischio è specifico del produttore e non si può eliminare con precauzioni tecniche di sicurezza. Lo si può ridurre soltanto rendendo più piccola la dipendenza stessa: con garanzie verificabili anziché con la mera fiducia, con la diversificazione e con una limitazione tecnica di ciò che è in generale possibile fare da remoto (cfr. capitolo 7.6).

Entrambe le prospettive attraversano i rilievi che seguono. Questa distinzione non è inconsueta. Il BSI tedesco, nel suo documento di posizione[27] sulla cibersicurezza nel settore energetico, indica espressamente tra i nuovi vettori di attacco la «manipolazione dell'infrastruttura energetica da parte di produttori o di terzi» e cita a questo proposito gli inverter come esempio.

5.3 Risultati della verifica tecnica

5.3.1 I cloud dei produttori

Per gli attacchi scalabili il livello cloud è quello di maggior peso. Un cloud amministra un intero parco di dispositivi, motivo per cui una singola vulnerabilità a quel livello riguarda potenzialmente un gran numero di impianti, a differenza di una falla nel singolo dispositivo.

Proprio questo livello si è però potuto verificare solo in misura limitata. I test su un cloud del produttore accedono a un sistema altrui, in esercizio produttivo, e senza il consenso del gestore sono ammissibili soltanto con restrizioni ai sensi dell'art. 143bis del Codice penale CP[28]. Ottenere un simile consenso avrebbe significato coinvolgere i produttori nell'indagine, il che sarebbe stato in contrasto con il principio dell'indipendenza. La verifica si è pertanto limitata al quadro ammissibile senza consenso. Tanto più notevole è il risultato: già entro questo quadro ristretto sono state trovate vulnerabilità presso più cloud di produttori, tra cui alcune delle categorie SQL injection e cross-site scripting. I produttori le hanno eliminate dopo la segnalazione.

Vi si manifesta al tempo stesso un problema strutturale: il livello con la maggiore leva è proprio quello che gli enti di verifica indipendenti non possono esaminare integralmente senza la collaborazione del produttore.

Un rilievo emerso da questa verifica è istruttivo sotto più aspetti. Una vulnerabilità classificata come critica riguardava il sistema di gestione dell'energia del produttore svizzero Solar Manager. Avrebbe consentito a un aggressore l'accesso da remoto a singoli sistemi, e non soltanto a uno, bensì in successione anche ad altri. Il produttore ha reagito in modo esemplare e ha chiuso la falla nel giro di poche ore. Ha inoltre concesso all'NTC il consenso a verificare anche il proprio cloud. È così venuta meno la barriera giuridica descritta più sopra, che altrimenti rende difficile una verifica del livello cloud. Il caso mostra che questa barriera si può dissolvere quando un produttore intende la trasparenza come un'opportunità. Diversamente dal resto del rapporto, citiamo qui il produttore per nome, con il suo consenso e come esempio positivo di gestione di

[27] Ufficio federale tedesco per la sicurezza informatica (BSI), «Positionspapier: Cybersicherheit im Energiesektor Deutschlands» (Documento di posizione: cibersicurezza nel settore energetico tedesco): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Positionspapier_Cybersicherheit_Energiesektor.html

[28] Walder Wyss AG, «Rechtsgutachten zur Strafbarkeit von Ethical Hacking» (Perizia giuridica sulla punibilità dell'ethical hacking): https://www.walderwyss.com/it/news/2023-06-26_rechtsgutachten-zur-strafbarkeit-von-fuer-das-nationale-testinstitut-fuer-cybersicherheit-ntc

una segnalazione di vulnerabilità.

Il caso è istruttivo anche per una seconda ragione. Solar Manager è diffuso soprattutto nell'area DACH, con circa 50'000 installazioni stimate. Prodotti con una diffusione regionale di questo tipo non compaiono di regola nelle ricerche internazionali, che provengono per lo più dagli Stati Uniti o da società di sicurezza attive a livello globale. Sfuggono alle maglie, benché nel nostro Paese controllino decine di migliaia di impianti. Questa lacuna si può colmare soltanto con verifiche che partano dal mercato svizzero effettivo.

Quanto grande possa essere la leva di un unico cloud e quanto difficile possa rivelarsi l'eliminazione lo mostra un caso documentato a livello internazionale[29]. Il Dutch Institute for Vulnerability Disclosure (DIVD), che analogamente all'NTC cerca e segnala vulnerabilità, si è imbattuto, nella piattaforma di monitoraggio Solarman, in credenziali di un account di amministrazione che si trovavano in chiaro in un repository pubblico di software (GitHub) e non erano protette da un secondo livello di sicurezza (autenticazione a più fattori). Attraverso questo unico account era possibile visualizzare e controllare in tutto il mondo quasi un milione di impianti con complessivamente oltre 10 GW di potenza, fino alla lettura e alla sovrascrittura del firmware. Significativo è stato il modo in cui la cosa è stata gestita: il gestore non ha reagito per mesi, dopo una prima correzione la password esposta è stata addirittura riportata al valore divulgato, e si è arrivati a una soluzione soltanto attraverso canali diplomatici e il coinvolgimento del CERT cinese. Il caso è quindi rappresentativo di due schemi al tempo stesso: l'enorme portata di un cloud centrale e la collaborazione talvolta difficile con i produttori nell'eliminazione. Nei Paesi Bassi ha in seguito dato luogo a interrogazioni parlamentari e a una maggiore attenzione delle autorità per la cibersicurezza degli inverter. Che non si trattasse di un caso isolato lo mostra una divulgazione successiva e nettamente più ampia[30]: nel 2024 la società di sicurezza Bitdefender ha trovato nelle stesse piattaforme Solarman e Deye nuove vulnerabilità che, secondo i resoconti dei media, avrebbero teoricamente riguardato un parco ancora più grande (circa 195 GW di potenza distribuiti su più di due milioni di impianti).

5.3.2 Interfacce locali e accessi dei produttori

I restanti rilievi si distribuiscono su classi ricorrenti. Più di frequente, e trasversalmente a molti dei dispositivi verificati, si sono presentate carenze nell'autenticazione e nel controllo degli accessi (ad esempio l'assenza di scadenza della sessione nonché password predefinite mancanti o non modificate), oltre a una cifratura assente o debole delle interfacce locali. Altri rilievi riguardavano interfacce non disattivabili (ad esempio un punto di accesso Wi-Fi non spegnibile) nonché accessi di manutenzione dei produttori non sicuri attraverso un accesso remoto (SSH, in parte con credenziali identiche per l'intero parco di dispositivi).

Che non si tratti di casi isolati lo confermano ricerche indipendenti. Nello studio SUN:DOWN, Forescout ha documentato[31] debolezze analoghe presso diversi leader di mercato (tra l'altro interfacce cloud non sicure, credenziali immutabili memorizzate in modo fisso nel dispositivo nonché aggiornamenti del firmware privi di firma crittografica). Il ricercatore Ruben Santamarta, specializzato in cibersicurezza nel settore energetico, descrive[32] accessi di manutenzione remota non sicuri presso produttori europei.

Quanto poco siano talvolta protetti simili accessi di manutenzione lo mostra con particolare chiarezza un rilievo. In un dispositivo era possibile, attraverso il punto di accesso Wi-Fi integrato, reimpostare e riassegnare la password dell'account installatore senza alcuna autenticazione. Con i diritti amministrativi così ottenuti era poi possibile attivare l'accesso remoto (SSH) e l'accesso root. Quest'ultimo è protetto nello stato di consegna da una password predefinita che deve essere modificata al primo accesso. Nell'esercizio normale l'accesso resta però inutilizzato, e

[29] Dutch Institute for Vulnerability Disclosure (DIVD), caso «Solarman» (DIVD-2022-00009): https://csirt.divd.nl/cases/DIVD-2022-00009/
[30] Bitdefender, studio sulle vulnerabilità nelle piattaforme Solarman e Deye, agosto 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», maggio 2026: https://www.reversemode.com/2026/05/a-practical-analysis-of-cyber-physical.html

con esso resta in vigore anche la password predefinita. Chi accede per primo assegna da sé la nuova password. Per la compromissione completa è bastato l'accesso al Wi-Fi integrato nel dispositivo.

Istruttiva è la concatenazione: sono presenti tre meccanismi di protezione, ossia un'autenticazione all'account, un accesso remoto disattivabile e un cambio di password al primo accesso. Nessuno è efficace, perché il primo può essere aggirato senza autenticazione e il terzo agisce soltanto quando qualcuno effettua l'accesso, cosa che non si può presupporre.

Altre vulnerabilità sono emerse soltanto dall'analisi del firmware dei dispositivi. In un prodotto sono stati trovati servizi che funzionano con i privilegi più elevati ed elaborano gli input già prima che sia avvenuta un'autenticazione. In un caso, nel firmware consegnato era ancora attivo un servizio di debug che riprende senza verifica un parametro di una richiesta di rete in un'area di memoria di dimensione fissa (buffer overflow). Poiché questo servizio funziona con i privilegi più elevati, attraverso un simile overflow è possibile introdurre ed eseguire codice di programma proprio. Senza credenziali e con il solo accesso alla rete locale era così raggiungibile il controllo completo del dispositivo (accesso root). È in ciò notevole che il servizio non sia necessario in esercizio e che fosse comunque raggiungibile nel firmware consegnato. È esattamente a questo che mira il principio formulato dalle linee guida citate nel capitolo *8.4.2 Blocco preimpostato in fabbrica delle funzioni di controllo rilevanti per la rete elettrica*: ciò che non serve in ogni modalità d'impiego dovrebbe essere disattivato di fabbrica.

Particolarmente ricca di conseguenze è l'interfaccia di comando locale. Attraverso di essa, in quasi tutti gli inverter verificati, è possibile non soltanto leggere valori di misura, bensì anche modificare le impostazioni del dispositivo rilevanti per la rete elettrica, e questo spesso senza autenticazione. Tecnicamente ciò avviene attraverso il protocollo industriale Modbus. Che il produttore utilizzi a tal fine i modelli di registro standardizzati SunSpec o uno schema proprio non cambia nulla: SunSpec[33] descrive soltanto il significato dei registri e non è uno strato di sicurezza. Presso diversi produttori questa interfaccia è disattivata di fabbrica. Per l'esercizio con un sistema di gestione dell'energia deve però essere attivata. Se è attiva, l'accesso avviene senza alcuna autenticazione, sicché ogni dispositivo nella stessa rete può inviare comandi. Tra sistema di gestione dell'energia e inverter molto spesso non esiste quindi alcuna sicurezza.

Tutti i rilievi descritti in questa sezione hanno in comune il fatto di presupporre l'accesso alla rete locale. Essi consentono il controllo completo di un singolo dispositivo, non di molti.

5.3.3 Dall'attacco locale all'attacco scalabile

Le vulnerabilità locali, prese di per sé, riguardano soltanto il singolo impianto e non sono scalabili. Una considerazione ridimensiona questa rassicurazione: un aggressore che si trovi già nella rete locale può controllare gli inverter attraverso il Modbus TCP non protetto. Lì l'effetto è raggiungibile per costruzione perfino senza vulnerabilità. Nella rete locale un aggressore entra ad esempio attraverso dispositivi IoT infettati. Che i dispositivi domestici vengano compromessi su larga scala lo mostrano sia le botnet classiche formate da computer e dispositivi IoT infetti (ad esempio del tipo Mirai) sia il rapido aumento dei cosiddetti residential proxy network, nei quali connessioni domestiche dirottate vengono subaffittate come nodi di accesso.[34] Anche il SIC descrive reti di anonimizzazione composte da dispositivi domestici mal protetti ed esposti a Internet, come i router, in parte attraverso infrastruttura noleggiata in Svizzera.[35] Se molte reti domestiche vengono compromesse in questo modo, da un vettore locale ne nasce uno di ampia efficacia.

5.3.4 Che cosa non è stato esaminato: il danneggiamento permanente dei

[33] SunSpec Alliance, specifica «Modbus»: https://sunspec.org/modbus/
[34] BSI, rapporto sull'abuso di residential proxy, «Steckbriefe aktueller Botnetze: Mirai» (Schede dei botnet attuali: Mirai), 2026: https://www.bsi.bund.de/dok/12820010
[35] Servizio delle attività informative della Confederazione (SIC), «La sicurezza della Svizzera 2026»: https://www.vbs.admin.ch/it/newnsb/jyRmuld1hBVy

dispositivi

Non era oggetto dell'indagine condotta dall'NTC la possibilità di danneggiare permanentemente i dispositivi facendoli funzionare in determinati stati. Che non si tratti di un pericolo puramente ipotetico lo mostra il caso Hoymiles. Ricercatori del Chaos Computer Club hanno dimostrato nel 2026 che i microinverter possono essere resi permanentemente inservibili attraverso il protocollo radio non protetto, caricando un firmware manipolato.[36] In quattro dispositivi l'NTC ha ottenuto il controllo completo del dispositivo (accesso root, il livello di privilegi più elevato), non ha però testato un danneggiamento permanente. Inoltre possono intervenire ulteriori meccanismi di protezione, ad esempio a livello di elettronica. Un simile attacco avrebbe, a differenza di un disturbo di rete temporaneo, conseguenze di lungo periodo.

5.3.5 Che cosa non è stato trovato

Altrettanto significativo quanto le vulnerabilità identificate è ciò che non è stato constatato. Non sono emersi indizi di backdoor inserite intenzionalmente o di componenti di comunicazione nascosti e non documentati, quali vengono discussi nella stampa internazionale.[37] In un dispositivo è sì stato dapprima scoperto un microfono, cosa che ha dato adito ad accertamenti. L'analisi ha però evidenziato una funzione di comando documentata (interazione mediante colpetti) e nessun indizio di una funzione occulta. Il caso non è però con ciò chiuso: il componente può rilevare più di quanto richieda il comando e, dopo un aggiornamento del firmware, si potrebbe eventualmente abusarne. Poiché la stessa funzione sarebbe possibile anche senza un microfono, questa scelta è da valutare come una vulnerabilità, del tutto a prescindere da un'intenzione malevola. È esattamente questo lo schema di fondo del rapporto: i rischi constatati sono di natura strutturale e non richiedono di presupporre un'intenzione malevola per essere seri.

5.4 Rischi strutturali

Il messaggio vero e proprio di questo rapporto non sta nei singoli rilievi, bensì in cinque rischi strutturali che sussistono indipendentemente dalla qualità dei singoli prodotti.

5.4.1 Dipendenza dal cloud del produttore

La controllabilità centrale descritta nel capitolo «L'ecosistema di un impianto fotovoltaico» è voluta dal punto di vista funzionale, ma sposta il controllo su un gran numero di impianti verso un unico punto. Ne deriva un rischio in caso di malfunzionamenti o di compromissione del produttore, nel caso estremo anche il possibile utilizzo come strumento di pressione geopolitica. La dipendenza è rafforzata dal fatto che molti dispositivi sono collegati stabilmente al cloud, in parte incentivati da vantaggi come garanzie prolungate. Allo stesso livello appartiene il canale di aggiornamento del firmware: è necessario, ma agisce anch'esso simultaneamente sull'intero parco, e ciò che viene distribuito attraverso di esso modifica il dispositivo in profondità.

Che questo canale venga realmente sfruttato lo ha mostrato l'attacco alla rete satellitare KA-SAT del febbraio 2022. Gli aggressori sono giunti al server attraverso il quale vengono distribuiti gli aggiornamenti software ai modem e hanno diffuso per questa via un software malevolo che ha sovrascritto la memoria dei dispositivi. È stato interessato tra l'altro il monitoraggio remoto di 5'800 impianti eolici del produttore Enercon con complessivamente 11 gigawatt. Gli impianti hanno continuato a immettere in rete, ma non era più possibile monitorarli o riavviarli da remoto. L'attacco era diretto contro l'Ucraina, gli impianti tedeschi sono stati un danno collaterale, ossia

[36] Chaos Computer Club (B. Heinz «Hunz»), «Analyse der Funk- und Firmware-Schwachstellen von Hoymiles-Wechselrichtern» (Analisi delle vulnerabilità radio e firmware degli inverter Hoymiles), 2026: https://www.ccc.de/updates/2026/blinkenlights-hoymiles
[37] Reuters, servizio giornalistico su moduli di comunicazione non documentati, maggio 2025: https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/

esattamente quello scenario che il SIC ritiene possibile anche per la Svizzera (cfr. capitolo *2.5*).[38]

5.4.2 Accesso remoto privilegiato per la manutenzione

Indipendentemente dal cloud, la maggior parte dei produttori mantiene un accesso privilegiato al proprio parco di dispositivi, ad esempio attraverso account di manutenzione o accessi remoti. Non si tratta di un errore isolato, bensì di un principio costruttivo: un unico procedimento di accesso compromesso o ricostruibile riguarda potenzialmente l'intero parco, e un accesso di questo tipo non si può eliminare come una vulnerabilità ordinaria. Sono interessati anche gli impianti di grandi dimensioni che non sono collegati a un cloud del produttore ma dispongono di interfacce proprie di comando e di manutenzione raggiungibili da remoto. Quanto sia reale questa possibilità lo ha mostrato nel novembre 2024 il caso degli inverter Deye: nell'ambito di una controversia sulla distribuzione, il produttore ha disattivato in modo mirato numerosi dispositivi propri distribuiti senza autorizzazione in diversi Paesi, del tutto senza alcuna vulnerabilità.[39]

Lo stesso schema va oltre il produttore: anche le aziende installatrici, i fornitori di servizi e gli aggregatori hanno spesso accesso remoto a tutti gli impianti da loro seguiti, senza che per essi valgano prescrizioni di cibersicurezza. Fin dove ciò arrivi lo ha mostrato nell'aprile 2022 un attacco mirato al fornitore di servizi di manutenzione di Brema Deutsche Windtechnik, che segue oltre 7'600 impianti eolici: l'impresa ha in seguito disattivato tutti i collegamenti del monitoraggio remoto dei dati, sicché per uno o due giorni non è più stato possibile alcun monitoraggio remoto. Gli impianti stessi non sono stati interessati.[40] Non è stato attaccato né un produttore né un gestore, bensì il fornitore di servizi che sta in mezzo.

5.4.3 Protocolli di comando locali non sicuri come caratteristica costruttiva

Il comando locale di molti inverter si basa su protocolli industriali diffusi che non prevedono alcuna autenticazione. Non si tratta di un errore di singoli dispositivi, bensì dello standard di un'intera categoria di dispositivi. Esso è aggravato dallo spostamento di questo comando da collegamenti ad accesso fisicamente limitato (RS485) a interfacce di rete (Ethernet, Wi-Fi), perché con ciò ogni dispositivo nella stessa rete diventa un possibile mittente di comandi di controllo.

5.4.4 Concentrazione del mercato come rischio cumulativo

La concentrazione descritta nel capitolo «L'ecosistema di un impianto fotovoltaico» agisce, sotto il profilo della sicurezza, come un «Single Point of Failure»: quanto maggiore è la quota di un produttore, tanti più dispositivi raggiunge un singolo rilievo. Quanto sia concreto questo rischio lo mostra una valutazione della società olandese di cibersicurezza Secura: nei Paesi Bassi due produttori (Huawei e Sungrow) hanno ciascuno per sé una quota di mercato così grande che un attacco ai sistemi di uno solo di essi basterebbe a raggiungere l'ordine di grandezza necessario per un effetto sulla rete. Su scala europea, secondo Secura, diversi produttori supererebbero questa soglia.[41]

5.4.5 Ubicazione e provenienza come sicurezza apparente

Diversi produttori pubblicizzano il fatto che il loro cloud sia gestito in centri di calcolo europei e amministrato da organizzazioni europee. L'ubicazione dell'hosting da sola dice però poco sul controllo effettivo del dispositivo, tra l'altro perché firmware e software provengono dal

[38] SentinelOne, «AcidRain – A Modem Wiper Rains Down on Europe», 31 marzo 2022: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
[39] Servizio giornalistico sugli inverter Deye disattivabili a distanza, 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» (Ciberattacco: paralizzato il monitoraggio remoto di impianti eolici), 27 aprile 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

produttore e non vengono sviluppati nel luogo dell'hosting. Nei test propri si è sì confermato che il traffico di dati osservato era diretto a endpoint dell'UE. Non se ne può però dedurre un controllo o una conservazione dei dati esclusivamente europei. Altrettanto poco la provenienza del dispositivo risolve il problema: anche i dispositivi di fornitori europei contengono spesso chip o componenti software provenienti da Paesi terzi oppure vengono fabbricati in tali Paesi.

6 Effetti sulla stabilità della rete

6.1 Principio di base: l'equilibrio tra produzione e consumo

Una rete a corrente alternata deve funzionare costantemente in prossimità della sua frequenza nominale (in Europa 50 Hz). Ciò presuppone un equilibrio in tempo reale tra produzione e consumo. Se la frequenza devia, nella rete interconnessa europea intervengono riserve scaglionate: una riserva primaria che entra in azione nel giro di secondi (circa 3'000 MW), nonché una riserva secondaria e una terziaria con tempi di attivazione più lunghi.[42] Una brusca variazione di potenza che superi il cosiddetto guasto di riferimento di 3'000 MW non può più essere assorbita dalla sola riserva primaria. A 49 Hz interviene un distacco di carico prescritto per via regolatoria.[43]

Un fattore strutturale aggravante è la diminuzione dell'inerzia di rete. Le centrali classiche stabilizzano la frequenza attraverso le masse rotanti dei loro generatori, mentre la produzione basata su inverter non fornisce di per sé questa inerzia.[44] Gli inverter moderni dovrebbero compensare progressivamente questo aspetto mediante funzioni «grid-forming». Il tema viene ripreso più avanti, tra i fattori mitiganti.

6.2 Evidenza reale: la rete può collassare anche senza un ciberattacco

Quanto fragile possa essere un sistema in presenza di un'elevata produzione basata su inverter lo ha mostrato il blackout iberico del 28 aprile 2025, e questo senza alcuna partecipazione malevola. A tratti una quota molto elevata dell'elettricità proveniva da fonti rinnovabili. Una catena di problemi legati alla tensione e alla potenza reattiva, una grandezza a supporto della rete che concorre a determinare la tensione nella rete e che viene spiegata più avanti in modo più dettagliato in relazione al tipo B, ha condotto a un rapido aumento della tensione, a distacchi a cascata della produzione e infine al collasso completo del sistema in Spagna e in Portogallo. Per la proporzionalità è importante l'attribuzione delle cause da parte di ENTSO-E, l'associazione dei gestori europei delle reti di trasmissione: determinante non è stato un «eccesso» di produzione rinnovabile, bensì lacune nella regolazione della tensione e della potenza reattiva.[45]

Che molti impianti configurati in modo analogo reagiscano simultaneamente non è un esperimento mentale. In Germania una direttiva del 2005 prescriveva che gli impianti fotovoltaici si distaccassero immediatamente dalla rete a una frequenza di rete di 50,2 Hz. Con lo sviluppo del settore ne è derivato un rischio sistemico: al raggiungimento di tale frequenza si sarebbero distaccati di colpo impianti per diversi gigawatt di potenza. L'ordinanza tedesca sulla stabilità del sistema del 2012 ha perciò obbligato i gestori di rete ad adeguare a posteriori circa 300'000 impianti esistenti con all'incirca un milione di inverter, affinché il distacco avvenga in modo scaglionato anziché simultaneo.[46]

6.3 Tre tipi di attacco di un inverter compromesso

L'idea diffusa che un attacco consista nell'«accendere e spegnere» in massa è riduttiva. Il ricercatore in sicurezza Ruben Santamarta distingue tre tipi di attacchi ciberfisici di complessità

[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] Regolamento (UE) 2017/2196 della Commissione, del 24 novembre 2017, che istituisce un codice di rete in materia di emergenza e ripristino dell'energia elettrica, articolo 15 (distacco automatico del carico a bassa frequenza) e allegato: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32017R2196
[44] ENTSO-E, «Frequency stability in long-term scenarios», studio sulla diminuzione dell'inerzia di sistema nell'area sincrona dell'Europa continentale, dicembre 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, problema dei 50,2 hertz: https://www.bdew.de/energie/systemstabilitaetsverordnung/502-hertz-problem/

crescente.[47]

6.3.1 Tipo A: potenza attiva e frequenza (inserzione e disinserzione)

Distaccando o inserendo in modo coordinato molti impianti si perturba l'equilibrio tra produzione e consumo e si sposta la frequenza. Lo si può ottenere con comandi di distacco diretti, con la manipolazione della funzione di protezione che distacca automaticamente un impianto dalla rete in caso di interruzione della rete stessa (anti-islanding), oppure con prescrizioni modificate a quale tensione un impianto debba restare in rete o distaccarsi (le cosiddette curve di ride-through HVRT e LVRT, «High/Low Voltage Ride-Through»). Particolarmente efficace è un attacco che ripete la manipolazione al ritmo della regolazione propria della rete, amplificando così l'oscillazione, in modo analogo a quando si spinge un'altalena al ritmo giusto.

Che la simultaneità produca effetti sulla rete anche senza un attacco lo mostra un fenomeno dell'esercizio di mercato. Se molti impianti adattano bruscamente la loro immissione in rete al cambio dell'intervallo di mercato, sorgono scostamenti di frequenza in corrispondenza del cambio di ora o di quarto d'ora, noti come «deterministic frequency deviations». Swissgrid intende perciò prescrivere che anche gli impianti fotovoltaici eseguano simili modifiche pianificate seguendo una rampa. Un aggressore che commuta molti impianti simultaneamente sfrutta lo stesso effetto, soltanto in modo intenzionale e senza rampa.[48]

6.3.2 Tipo B: potenza reattiva e tensione

Secondo la valutazione di Santamarta questa è la via più efficace verso guasti locali. Gli inverter sostengono la rete non soltanto con potenza attiva, bensì anche con potenza reattiva, che concorre a determinare la tensione nella rete. Il modo in cui un inverter deve reagire è stabilito da curve caratteristiche, ad esempio la curva Volt-Var: se la tensione sale, l'inverter assorbe potenza reattiva e riabbassa la tensione. Ciò stabilizza la rete. Un attacco inverte questa reazione. Una curva caratteristica manipolata costringe l'inverter a immettere potenza reattiva supplementare quando la tensione è già elevata, spingendo così la tensione ulteriormente verso l'alto. Già pochi impianti possono in questo modo spingere la tensione locale oltre i limiti ammessi; a quel punto i dispositivi di protezione di impianti vicini e di sottostazioni possono disinserirsi e innescare un effetto a cascata. Quanto alla verosimiglianza: attraverso una logica di comando modificata, ad esempio dopo una compromissione del firmware, un simile ribaltamento è plausibile. L'attacco non richiede né codice malevolo complesso né una grande scala. Alla stessa conclusione giungono le simulazioni di rete che DNV ha effettuato su incarico di SolarPower Europe con i modelli di rete di ENTSO-E:[49] se grandi capacità vengono commutate simultaneamente tra potenza reattiva induttiva e capacitiva, sorgono rapidi sbalzi di tensione che possono far scattare i dispositivi di protezione di impianti di produzione vicini e di sottostazioni e innescare un effetto a cascata. Lo studio rileva al tempo stesso che resta poco chiaro quanto rapidamente e quanto ampiamente i meccanismi esistenti per il mantenimento della tensione vi si opporrebbero.

6.3.3 Tipo C: instabilità indotta dai convertitori (oscillazioni)

L'eccitazione mirata di oscillazioni proprie della rete fino a oscillazioni forzate è il vettore più complesso. Esso è considerato, anche secondo la valutazione dello stesso Santamarta, al momento irrealistico, in particolare come attacco coordinato attraverso una moltitudine di piccoli inverter domestici eterogenei. Come fenomeno è tuttavia reale. Nel blackout iberico un'oscillazione forzata proveniente da una singola grande centrale fotovoltaica (secondo l'analisi di Santamarta l'impianto Núñez de Balboa), e non da impianti di piccole dimensioni distribuiti, ha

[47] Santamarta, «Cyber-Physical Attacks on Solar Inverters», maggio 2026: https://www.reversemode.com/2026/05/a-practical-analysis-of-cyber-physical.html
[48] Swissgrid SA, white paper «Systemverträgliche Integration Photovoltaik» (Integrazione del fotovoltaico compatibile con il sistema), marzo 2026, https://www.swissgrid.ch/it/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

eccitato un'oscillazione sovraregionale.[50]

6.3.4 Valutazione: il vettore più pericoloso non è quello più oneroso

Sorprendente è al riguardo che il vettore più pericoloso non sia quello più oneroso. Rispetto a perdite di sola produzione la rete è relativamente robusta. L'attacco basato sulla tensione attraverso la potenza reattiva richiede invece una scala ridotta e una complessità modesta, il che rende la minaccia più reale, come mostra il blackout iberico proprio su questo livello (cfr. capitolo *6.2*).

6.4 Lo scenario cibernetico: manipolazione coordinata del carico e della produzione

L'idea che dispositivi compromessi e collegati a Internet possano essere raggruppati in un insieme con effetti sulla rete è affermata nella ricerca da circa un decennio (sotto le denominazioni «load-altering» ossia MaDIoT, «Manipulation of Demand via IoT»). I lavori vanno dai primi modelli di Dabrowski et al.[51] (2017) e Soltan et al.[52] (2018) fino a Goerke et al.[53] (2024), che quantificano in dettaglio quanti impianti per ciascun tipo sarebbero necessari per un effetto sulla rete interconnessa europea. La prima formulazione specifica per il fotovoltaico di questa idea di fondo proviene dallo «Horus Scenario»[54] di Willem Westerhof, pubblicato nell'agosto 2017 e basato su una divulgazione al produttore del dicembre 2016.

Gli inverter si prestano particolarmente a simili attacchi perché, in quanto sistemi in tempo reale, seguono con precisione la frequenza di rete e possono così eseguire un attacco in modo molto accurato.

Oltre alla pura destabilizzazione della rete va menzionato un secondo percorso di danno. Aggressori con accesso di ampia portata possono mettere permanentemente fuori servizio i dispositivi mediante un firmware malevolo, sicché essi devono essere sostituiti o riprogrammati in loco. Ipotizzabile è anche un'estorsione («ransomware sugli inverter»). Simili effetti distruttivi avrebbero conseguenze nettamente più durature di un disturbo di rete temporaneo.

6.5 Ordine di grandezza (calcolo approssimativo illustrativo)

A titolo di inquadramento, espressamente non come previsione autonoma di blackout, l'ordine di grandezza si può ricavare dalla letteratura. Secondo Dabrowski et al., in condizioni favorevoli per un aggressore basta il controllo su circa 4'500 MW per spingere la frequenza nella rete interconnessa europea sotto la soglia di distacco del carico di 49 Hz, ossia una volta e mezza il guasto di riferimento. Il valore vale per un attacco che modula la potenza al ritmo della regolazione di rete amplificando così lo scostamento; un'unica brusca variazione di potenza dovrebbe ammontare, a parità di condizioni di rete, a circa 6'000 MW. La soglia designa uno squilibrio di potenza raggiungibile tanto dal lato del consumo quanto dal lato della produzione: Dabrowski la deriva dal lato del carico, Goerke et al. e dos Santos et al. la trasferiscono al fotovoltaico. Per il fotovoltaico ciò significa concretamente una giornata soleggiata con carico basso, ad esempio in un fine settimana estivo o in un giorno festivo.

A titolo di inquadramento: 4'500 MW corrispondono a poco meno della metà dei 9,5 GW installati in Svizzera. La soglia è quindi europea e non svizzera. Su scala europea, all'inverso, basta una quota ridotta: rapportati al parco installato nell'UE alla fine del 2025, pari a circa 406 GW, 4'500

[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/

MW rappresentano poco più dell'un per cento, e anche la variante prudente di 6'000 MW resta sotto il due per cento; questa quota diminuisce con ogni ulteriore anno di sviluppo.[55] Una simulazione indipendente giunge a un ordine di grandezza analogo: per la rete europea DNV indica una compromissione mirata di 3 GW come soglia a partire dalla quale sono possibili effetti considerevoli.[56]

Per la Svizzera non ne deriva alcuna rassicurazione, bensì una domanda diversa: quanto fortemente il parco impianti svizzero sia concentrato in singoli punti di controllo. Poiché a un unico produttore spetta poco più della metà della quota di mercato (cfr. capitolo *3.6*), già un solo cloud del produttore raggiunge una parte considerevole e crescente del parco impianti svizzero. Una concentrazione analoga nasce dagli aggregatori e dalle centrali elettriche virtuali (cfr. capitolo *3.4*). Per un attacco coordinato su scala europea non è determinante la somma nazionale, bensì il numero delle piattaforme attraverso le quali essa è raggiungibile.

Un calcolo autonomo e attendibile per la rete svizzera si colloca al di fuori della portata dell'indagine. Attendibile resta l'affermazione centrale: già una quota inferiore al due per cento del parco di inverter europeo basta, sul piano del calcolo, a innescare effetti rilevanti sulla rete, laddove la cifra concreta dipende fortemente dalla distribuzione dei dispositivi e dallo stato della rete. Il vettore della potenza reattiva (tipo B) richiede secondo Santamarta nettamente meno potenza controllata, agisce però a livello locale e non sovraregionale.

6.6 Precedente reale: Polonia, 29 dicembre 2025

Un ciberattacco coordinato ha colpito più di 30 parchi eolici e fotovoltaici nonché una centrale termica e un'impresa industriale. Negli impianti da fonti rinnovabili è andata persa la comunicazione con i gestori delle reti di distribuzione. La produzione di elettricità in sé non è stata pregiudicata, e il gestore della rete di trasmissione non ha in alcun momento ritenuto minacciata la stabilità del sistema polacco. La produzione è sì proseguita, ma era disaccoppiata dalle esigenze della rete. Il gestore polacco della rete di trasmissione ha rilevato che erano state osservate e corrette irregolarità nell'esercizio di produttori di energia elettrica più piccoli, ma che il sistema aveva potuto essere riequilibrato con i mezzi disponibili. Il software malevolo impiegato era distruttivo (wiper). Il rapporto dell'autorità competente paragona gli attacchi a un incendio doloso.

L'importanza dell'episodio non sta in un blackout evitato per poco, bensì nel fatto che un attore capace ha comprovatamente ottenuto l'accesso al livello di comando (Operational Technology, OT) di numerosi parchi di impianti da fonti rinnovabili e ha manifestato un'intenzione distruttiva. Con ciò lo scenario perde il suo carattere puramente teorico. Il 13 luglio 2026 il Regno Unito e l'UE hanno attribuito ufficialmente l'attacco al servizio segreto russo FSB (Centro 16) e hanno adottato un pacchetto di sanzioni congiunto. Secondo la valutazione britannica, in inverno l'attacco avrebbe potuto tagliare fuori dall'approvvigionamento elettrico circa 500'000 persone.[57] La documentazione tecnica è fornita da CERT Polska.[58]

6.7 Valutazione di specialisti indipendenti

Anche al di fuori degli organi statali il pericolo viene preso sul serio. Il DIVD olandese (cfr. capitolo *5*) esamina in un proprio programma inverter, stazioni di ricarica, smart meter e sempre più anche sistemi di gestione dell'energia. Nel luglio 2026 alcuni specialisti hanno messo pubblicamente in guardia, a seguito dell'attacco in Polonia, sul fatto che nello scenario peggiore un attacco

[55] SolarPower Europe, «EU Solar Market Outlook 2025-2030», dicembre 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, comunicazione sulle sanzioni del 13 luglio 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/

riuscito potrebbe portare a interruzioni di corrente su vasta scala e della durata di giorni.[59]

6.8 Fattori mitiganti

La rete non è indifesa. Riserve scaglionate, sistemi di protezione e l'inerzia tuttora presente assorbono molti disturbi, e non ogni manipolazione innesca un effetto a cascata. L'eterogeneità del parco, con i suoi numerosi produttori, versioni del firmware e configurazioni, rende inoltre più difficile un unico exploit valido per tutti i produttori. All'interno di un cloud dominante di un produttore la concentrazione resta però reale, e in Svizzera è marcata (cfr. capitolo *3).*

Al tempo stesso, con la diminuzione delle centrali classiche cala l'inerzia di rete. Gli inverter grid-forming dovrebbero compensarla. Se però proprio questi inverter sono l'obiettivo dell'attacco, con la produzione viene meno anche la componente di stabilizzazione. Nel complesso il livello di protezione di base dovrebbe aumentare grazie agli aggiornamenti continui dei produttori nonché alla regolamentazione UE dei prodotti vigente e futura (RED, CRA). I rischi strutturali e geopolitici non vengono però con ciò eliminati.

[59] Dutch Institute for Vulnerability Disclosure (DIVD), avvertimento pubblico sulla vulnerabilità della rete elettrica (Chris van 't Hof), luglio 2026: https://www.nu.nl/klimaat/6403086/stroomnet-kwetsbaar-voor-cyberaanval-geen-kwestie-van-of-maar-wanneer.html

7 Confronto internazionale e regolamentazione

Negli ultimi due anni circa la cibersicurezza degli impianti fotovoltaici è entrata nell'agenda normativa a livello internazionale. Questo capitolo offre una panoramica delle misure di altri Stati e dell'UE e vi colloca la Svizzera. Le valutazioni riportate provengono dalle rispettive autorità e dai rispettivi governi. Esse vengono qui illustrate, non valutate.

7.1 Uno schema comune

Colpisce il fatto che le iniziative di diversi Paesi mirino agli stessi due punti: la possibilità del controllo a distanza attraverso i cloud dei produttori e la forte concentrazione del mercato su pochi produttori, in prevalenza cinesi. Nel 2024 nove dei dieci maggiori produttori mondiali di inverter provenivano dalla Cina; a Huawei e Sungrow da sole spettava circa il 55 per cento delle forniture mondiali.[60] Questa situazione di partenza è classificata come rischio strategico da diverse autorità nazionali di sicurezza.

All'inquadramento appartiene anche la posizione contraria. Nel maggio 2026 il Ministero del commercio cinese ha definito la classificazione come Stato ad alto rischio priva di prove concrete e ha parlato di una stigmatizzazione dei prodotti cinesi.[61] La Camera di commercio cinese presso l'UE ha a sua volta respinto l'accusa secondo cui la Cina potrebbe impiegare l'energia come strumento di pressione, e ha richiamato il contributo delle imprese cinesi alla transizione energetica europea.[62]

7.2 Panoramica degli strumenti impiegati

Le iniziative si possono ordinare secondo la loro incisività, dalla semplice informazione fino al rifiuto dell'allacciamento alla rete.

- **Mettere in guardia:** l'Estonia e la Repubblica Ceca puntano su avvertimenti delle autorità. Nel febbraio 2024 il servizio informazioni estero estone ha messo espressamente in guardia[63] dagli inverter cinesi e ha rilevato che quanto più l'Estonia punta sull'energia solare, tanto maggiore sarebbe l'effetto di una possibile manipolazione. Il direttore del servizio informazioni ha parlato di un rischio di ricatto.[64] Il 3 settembre 2025 l'autorità ceca per la cibersicurezza NÚKIB ha messo in guardia dal trasferimento di dati verso la Cina e dall'amministrazione remota dalla Cina nelle infrastrutture critiche, citando gli inverter fotovoltaici come uno di vari esempi. Si tratta di un avvertimento, non di un divieto: le entità regolamentate devono tenerne conto nella loro analisi dei rischi.[65] Nel giugno 2026 la Germania ha messo in guardia, in un avviso congiunto dell'Ufficio federale tedesco per la protezione della Costituzione e del BSI, dall'attività di ricognizione condotta da attori russi su impianti fotovoltaici collegati a Internet senza protezione.[66]
- **Raccomandare:** l'Australia ha affrontato il tema per tempo. Nell'agosto 2023 il Cyber

[60] EUISS, Caspar Hobhouse, «The dragon in the grid: Limiting China's influence in Europe's energy system», gennaio 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», maggio 2026: https://english.mofcom.gov.cn/News/SpokesmansRemarks/art/2026/art_29f372ba6bfc4cde81fd567ea440cc60.html
[62] Euronews, «EU moves to ban high-risk inverters from China over cybersecurity threats», 4 maggio 2026: https://www.euronews.com/my-europe/2026/05/04/eu-moves-to-ban-high-risk-inverters-from-china-over-cybersecurity-threats
[63] Estonian Foreign Intelligence Service (Välisluureamet), «International Security and Estonia 2024», febbraio 2024: https://raport.valisluureamet.ee/2024/en/6-china/6-3-the-advance-of-chinese-technology/
[64] Reuters, servizio giornalistico su moduli di comunicazione non documentati, maggio 2025: https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/
[65] Autorità ceca per la cibersicurezza NÚKIB, settembre 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] Ufficio federale tedesco per la protezione della Costituzione (BfV) e Ufficio federale tedesco per la sicurezza informatica (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure» (Avviso di sicurezza congiunto: ricognizione di impianti fotovoltaici mal protetti da parte di attori cibernetici statali), 3 giugno 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

Security Cooperative Research Centre ha pubblicato il rapporto «Power Out? Solar Inverters and the Silent Cyber Threat» e ha raccomandato tre misure: valutazioni del ciberrischio per tutti gli inverter venduti, rating obbligatori di cibersicurezza nonché il richiamo o la correzione dei dispositivi con vulnerabilità gravi.[67] Indipendentemente da ciò, in Australia vige dal 4 marzo 2026 un requisito generale di prodotto per i dispositivi di consumo connessi: il Cyber Security Act 2024 australiano e le Security Standards for Smart Devices Rules che vi si fondano esigono tra l'altro password univoche, un punto di contatto per le segnalazioni di vulnerabilità e l'indicazione del periodo di supporto.[68]

- **Verificare e divulgare:** i Paesi Bassi sono passati dalla ricerca alla vigilanza. Tra il 2021 e il 2023 l'ispettorato olandese per le infrastrutture digitali (RDI) ha verificato nove inverter di uso commerciale di otto marche rispetto alla norma ETSI EN 303 645, una norma europea di base che pone unicamente requisiti minimi ai dispositivi di consumo connessi e che deve proteggere espressamente solo da attacchi elementari a debolezze costruttive fondamentali, ad esempio da password predefinite identiche per tutti i dispositivi di un produttore. Nessun dispositivo soddisfaceva tutti i requisiti. L'autorità ha messo in guardia dal fatto che i dispositivi potessero essere spenti da remoto o abusati per attacchi.[69] Indipendentemente da ciò, le divulgazioni descritte nel capitolo «Rilievi e rischi» hanno dato luogo nei Paesi Bassi a interrogazioni parlamentari.
- **Prendere posizione su un progetto legislativo proprio:** la Germania mostra con particolare chiarezza il conflitto di obiettivi tra controllo a supporto della rete e cibersicurezza (cfr. capitolo *7.3.1*).
- **Vincolare i fondi di promozione:** l'Unione europea esclude dai fondi di promozione dell'UE gli inverter di fornitori ad alto rischio e innalza parallelamente, attraverso RED e CRA, il livello di protezione di base dei prodotti connessi (cfr. capitolo *7.3.2*).
- **Vincolare l'accesso al mercato a una verifica:** Taiwan rende la prova di cibersicurezza parte integrante dell'omologazione (cfr. capitolo *7.3.3*).
- **Vincolare l'allacciamento alla rete alla sicurezza:** la Lituania vieta ai produttori provenienti da Stati considerati una minaccia l'accesso remoto agli impianti oltre i 100 kW e consente ai gestori di rete di distaccare gli impianti non conformi (cfr. capitolo *7.3.4*).
- **Autoregolamentazione:** nel 2025 l'associazione di settore europea SolarPower Europe ha presentato un'analisi elaborata dalla società di test DNV sui ciberrischi del fotovoltaico per la stabilità della rete. Essa contiene una valutazione dei rischi, simulazioni di rete e un catalogo di requisiti minimi per produttori, gestori e politica. Il settore ha così affrontato il tema di propria iniziativa.[70]

7.3 Quattro approcci in dettaglio

I quattro approcci menzionati per ultimi vengono illustrati più da vicino qui di seguito, perché sono immediatamente riconducibili alla discussione svizzera.

7.3.1 Germania: il conflitto di obiettivi tra controllo della rete e cibersicurezza

La Germania mostra con particolare chiarezza il conflitto di obiettivi tra controllo a supporto della rete e cibersicurezza. Secondo l'art. 14a della legge tedesca sull'industria energetica (EnWG), dal 1° gennaio 2024 i gestori di rete possono, in caso di sovraccarico locale incombente della rete, ridurre temporaneamente il prelievo di elettricità di apparecchi di consumo controllabili come pompe di calore, wallbox e sistemi di accumulo a batteria fino a una potenza minima di 4,2 kW. In

[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» (Indagine sulle problematiche di disturbo e sulla cibersicurezza degli inverter per pannelli solari), maggio 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

cambio il corrispettivo di rete viene ridotto.[71]

Quando con la cosiddetta legge tedesca sui picchi solari (Solarspitzengesetz) è stata prevista anche la limitazione della potenza degli impianti fotovoltaici attraverso gli inverter esistenti, l'Ufficio federale tedesco per la sicurezza informatica (BSI) ha espresso riserve considerevoli. A suo giudizio sarebbe molto critico realizzare un controllo a distanza degli inverter a supporto della rete passando dai produttori. Il fatto che i produttori, eventualmente attraverso un cloud gestito all'estero, avrebbero accesso diretto a un numero così elevato di dispositivi nella rete interconnessa europea comporterebbe un potenziale di pericolo considerevole. Oltre al produttore stesso, anche lacune di sicurezza potrebbero aprire a terzi un accesso non autorizzato. Come alternativa il BSI ha proposto di far funzionare tali impianti il più possibile in locale e di realizzare il controllo a supporto della rete attraverso sistemi di misurazione intelligenti anziché attraverso i cloud dei produttori.[72] Commenti specialistici hanno obiettato che gli inverter controllabili a distanza si lasciano comunque spegnere attraverso il backend del rispettivo produttore e che l'accesso temuto dal BSI, vista la posizione dominante dei produttori cinesi sul mercato, esiste quindi già da tempo anche senza la legge. [73]

Degno di nota per la Svizzera è inoltre il fatto che la Germania conosce la stessa lacuna normativa. L'ordinanza tedesca sulle infrastrutture critiche (BSI-KritisV)[74] si applica solo a partire da 104 MW di potenza dell'impianto; gli impianti fotovoltaici più piccoli non rientrano nelle prescrizioni per le infrastrutture critiche.

7.3.2 Unione europea

Il passo finora più netto è costituito dalla «Economic Security Doctrine» pubblicata il 3 dicembre 2025, che designa espressamente la dipendenza dagli inverter solari come dipendenza ad alto rischio e la motiva con la concentrazione dei fornitori, con i rischi di cibermanipolazione e con l'accesso a dati di esercizio rilevanti per la rete. Come strumenti essa indica tra l'altro valutazioni coordinate del ciberrischio e la certificazione sotto il Cyber Resilience Act. L'associazione dei produttori ESMC chiede inoltre che gli Stati membri possano escludere dall'allacciamento alla rete l'hardware ad alto rischio.[75]

Nella primavera 2026 è seguita una misura concreta: la Commissione limita i fondi di promozione dell'UE, tra l'altro della Banca europea per gli investimenti, per progetti solari, eolici e di accumulo che impiegano inverter di fornitori ad alto rischio provenienti da Cina, Russia, Iran o Corea del Nord. I fornitori di Paesi partner affidabili restano ammissibili alla promozione.[76] Importante per l'inquadramento: si tratta di una restrizione della promozione, non di un divieto di mercato. Un passo ulteriore in direzione di restrizioni di mercato durature è previsto con la proposta di revisione del Cybersecurity Act (CSA2). Resta una lacuna strutturale: la direttiva NIS2, fondamentale per molte di queste misure, si applica principalmente a partire dalle imprese di medie dimensioni e di regola non comprende impianti di produzione più piccoli come il fotovoltaico privato sui tetti.

Indipendentemente da ciò, l'UE innalza il livello di protezione di base dei prodotti connessi. I requisiti di cibersicurezza della direttiva sulle apparecchiature radio (RED) valgono dal 1° agosto 2025 ed esigono, per gli apparecchi radio abilitati a Internet, la protezione della rete, la

[71] Agenzia federale tedesca delle reti (Bundesnetzagentur), «Integration von steuerbaren Verbrauchseinrichtungen (§14a EnWG)» (Integrazione di apparecchi di consumo controllabili, art. 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» (Legge sui picchi solari: il BSI mette in guardia dall'accesso di produttori cinesi a impianti fotovoltaici tedeschi), gennaio 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» (Clamore attorno alla sorveglianza negli inverter cinesi): https://www.zfk.de/energie/strom/wirbel-um-ueberwachung-in-chinesischen-wechselrichtern
[74] BSI-KritisV (ordinanza tedesca sulle infrastrutture critiche), allegato 1, parte 3 n. 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 dicembre 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 aprile 2026: https://www.pv-magazine.com/2026/04/23/eu-moves-to-restrict-funding-for-projects-using-inverters-from-high-risk-suppliers/

protezione dei dati personali nonché la prevenzione delle frodi. Dall'11 dicembre 2027 il Cyber Resilience Act subentra a essa; gli obblighi di notifica per le vulnerabilità attivamente sfruttate e per gli incidenti gravi valgono già dall'11 settembre 2026. Il CRA è tecnologicamente neutro e orientato al ciclo di vita ed esige tra l'altro meccanismi di aggiornamento sicuri e una gestione strutturata delle vulnerabilità lungo l'intera vita del prodotto. Poiché queste regole valgono per l'accesso al mercato e i prodotti interessati sono in larga misura gli stessi che in Svizzera, esse dovrebbero innalzare il livello di sicurezza anche nel nostro Paese.

7.3.3 Taiwan: verifica di prodotto con una profondità considerevole

Taiwan dispone di uno dei pochi regimi di test riferiti al prodotto per gli inverter solari e del più dettagliato tra quelli documentati pubblicamente. Nell'ottobre 2025 l'autorità taiwanese per la normazione e la verifica BSMI ha pubblicato una specifica tecnica di verifica e ha reso vincolanti le prove di cibersicurezza con una revisione dell'omologazione del maggio 2026. Per gli inverter solari, accanto all'infrastruttura di ricarica, ai convertitori di potenza e agli accumulatori stazionari al litio, esse diventano parte obbligatoria dell'omologazione dal 1° gennaio 2028, e la via semplificata della dichiarazione di conformità decade allora.[77]

Vengono verificate separatamente due unità, l'inverter stesso e l'unità di monitoraggio. Per l'unità di monitoraggio valgono quattro dimensioni di sicurezza, ossia sicurezza fisica, di sistema, di comunicazione e di autenticazione; per l'inverter tre, fondate su standard internazionali come IEC 62443-4-2. La profondità della verifica è notevole. Viene richiesta la consegna del codice sorgente per un'analisi statica, laddove le vulnerabilità con un valore di gravità (CVSS) pari o superiore a 7 conducono alla non conformità in assenza di una contromisura motivata. Vi si aggiunge una verifica dell'integrità dell'aggiornamento del firmware, nella quale l'inverter deve respingere un firmware manipolato di proposito oppure ripiegare su uno stato sicuro. Per l'unità di monitoraggio è inoltre prevista un'analisi del traffico su almeno 24 ore, nella quale gli indirizzi di destinazione effettivi vengono confrontati con i server dichiarati dal produttore.

Analiticamente istruttivi sono due limiti. In primo luogo si tratta di un esame del tipo al momento della certificazione: la specifica esige sì che il dispositivo riconosca un firmware manipolato, ma non prescrive a tal fine alcun procedimento crittografico determinato, e non prevede una nuova verifica specifica in caso di successive modifiche del firmware. In secondo luogo essa esclude espressamente dalla portata della verifica la sicurezza delle informazioni del sistema di gestione, ossia del livello cloud; viene incluso soltanto se esso possa amministrare account utente e aggiornare il firmware da remoto. Questo regime di test tralascia così proprio quel livello che, secondo i rilievi della presente analisi, ha la maggiore leva. L'insegnamento per la Svizzera e per l'UE è di conseguenza duplice: un regime di test riferito al prodotto è possibile e sensato, ma resta incompleto finché non comprende né una componente di ciclo di vita né il livello di controllo centrale.

7.3.4 Lituania: la sicurezza come condizione per l'allacciamento alla rete

La Lituania si è spinta più lontano di tutti. Con l'articolo 73^3 approvato il 12 novembre 2024, ai produttori provenienti da Stati che secondo la strategia nazionale di sicurezza sono considerati una minaccia, e tra i quali figura la Cina, è vietato l'accesso remoto ai sistemi di comando di impianti solari, eolici e di accumulo oltre i 100 kW, concretamente la modifica a distanza di parametri di potenza nonché l'accensione e lo spegnimento. Vengono richiesti tra l'altro l'autenticazione a più fattori, una comunicazione sicura, controlli sulla catena di approvvigionamento nonché un audit. Per i nuovi impianti la regolamentazione vale dal 1° maggio 2025; gli impianti esistenti hanno dovuto adeguarsi entro il 1° giugno 2026. La conformità è presupposto per l'allacciamento alla rete e, dalla scadenza del termine transitorio, i gestori di rete possono anche distaccare dalla rete gli impianti non conformi.[78] L'associazione europea dei

[77] Taiwan, Bureau of Standards, Metrology and Inspection (BSMI), revisione delle regole di omologazione del maggio 2026: https://www.bsmi.gov.tw/wSite/public/Attachment/f1761016956224.pdf; sintesi: https://www.gmalabs.com/post/taiwan-bsmi-type-approval-update-new-cybersecurity-files

[78] pv magazine, «Lithuania's grid operators can now disconnect solar plants without cybersecurity measures», giugno 2026: https://www.pv-magazine.com/2026/06/05/lithuanias-grid-operators-can-now-disconnect-solar-plants-without-cybersecurity-measures/

produttori solari ha sostenuto la regolamentazione.[79]

Degno di nota è ciò che la legge non richiede. I dispositivi cinesi non sono vietati, e gli impianti già installati non devono essere sostituiti. I loro gestori devono però attuare misure di protezione supplementari.

L'esperienza lituana mostra al tempo stesso dove ricade l'onere. Per i nuovi impianti la conformità si raggiunge in modo relativamente conveniente, perché può essere considerata fin dall'inizio in sede di acquisto e di allacciamento. Oneroso e lungo è invece l'adeguamento a posteriori del parco impianti esistente, nel quale si sono formati arretrati di attuazione. Per la Svizzera ne consegue che un simile approccio dispiega il proprio effetto soprattutto attraverso i nuovi impianti e che il parco impianti esistente resta per anni il fianco scoperto più ampio.

7.4 Regolamentazione in Svizzera

In Svizzera lo standard minimo TIC per il settore elettrico è vincolante dal 1° luglio 2024. L'ordinanza sull'approvvigionamento elettrico riveduta (OAEl, allegato 1a) prescrive livelli di protezione e gradi di maturità, il cui adempimento può essere verificato dalla Commissione federale dell'energia elettrica (ElCom). La classificazione si orienta alla capacità: il livello di protezione A vale ad esempio per i gestori di rete a partire da 450 GWh all'anno, il livello di protezione B per i gestori di rete a partire da 112 GWh all'anno nonché per produttori di energia elettrica, gestori di accumuli e fornitori di servizi, sempre che esercitino impianti con una potenza complessiva di almeno 100 MW e possano controllarli tramite un unico sistema.[80] In aggiunta vige dal 1° aprile 2025 un obbligo di notifica: i ciberattacchi alle infrastrutture critiche vanno notificati entro 24 ore all'Ufficio federale della cibersicurezza (UFCS).

La lacuna decisiva riguarda gli impianti di piccole dimensioni e quindi praticamente tutti gli impianti fotovoltaici svizzeri. I produttori di energia elettrica soggiacciono allo standard solo a partire da 100 MW di potenza complessiva controllabile tramite un unico sistema. Il parco di piccoli impianti, distribuito su centinaia di migliaia di gestori, non è coperto da alcun singolo soggetto assoggettato. La regolamentazione UE dei prodotti, vigente e futura, dovrebbe innalzare il livello dei dispositivi. Le questioni strutturali e geopolitiche, ossia la concentrazione del mercato e la controllabilità a distanza, essa non le affronta però.

Che questa lacuna sia riconosciuta lo mostra un documento della società di rete nazionale. Nel white paper «Systemverträgliche Integration Photovoltaik»[81] del marzo 2026 Swissgrid rileva che l'approvvigionamento energetico svizzero è già oggi distribuito su centinaia di migliaia di impianti decentralizzati. Ciò richiederebbe anche per questi impianti e per il loro controllo un livello di protezione definito nei confronti dei ciberattacchi. Vengono chiesti requisiti minimi vincolanti per gli impianti fotovoltaici, che dovrebbero inoltre essere effettivamente attuati e controllati anche negli impianti esistenti. La raccomandazione è indirizzata al legislatore e all'Ispettorato federale degli impianti a corrente forte (ESTI). La necessità di intervento descritta nel presente rapporto è così condivisa da quel soggetto che risponde della stabilità del sistema complessivo.

Va considerato che cosa lo standard minimo TIC realizza e che cosa no. Esso si rivolge a organizzazioni e chiede loro di identificare i rischi, di attuare misure di protezione, di riconoscere gli incidenti e di reagirvi. A un impianto privato, gestito da una persona senza un'organizzazione informatica, non è sensatamente applicabile. La lacuna presso gli impianti di piccole dimensioni non si può quindi colmare abbassando la soglia di potenza. Efficaci sono qui altri strumenti: requisiti al prodotto, condizioni per l'allacciamento alla rete oppure l'inclusione di quel soggetto che concentra l'accesso a molti impianti.

[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] Ufficio federale della cibersicurezza (UFCS), standard minimo TIC: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html
[81] Swissgrid SA, white paper «Systemverträgliche Integration Photovoltaik» (Integrazione del fotovoltaico compatibile con il sistema), marzo 2026, https://www.swissgrid.ch/it/home/newsroom/blog/2026/20260330-01.html

7.5 Inquadramento per la Svizzera

La tendenza internazionale è univoca: diversi Stati trattano il fotovoltaico distribuito sempre più come una questione di infrastruttura critica e non soltanto di politica climatica. Gli strumenti impiegati vanno dagli avvertimenti (Repubblica Ceca, Estonia, Germania) e dalle prese di posizione delle autorità su progetti legislativi (Germania) alle verifiche di mercato in sede di vigilanza (Paesi Bassi) e ai regimi di test riferiti al prodotto (Taiwan), fino ai criteri di promozione e di acquisto (UE) e alle condizioni vincolanti di allacciamento alla rete (Lituania).

Sul versante dell'applicazione si aggiunge un ulteriore strumento. Con l'attribuzione dell'attacco alla rete elettrica polacca al servizio segreto russo FSB e con il pacchetto di sanzioni congiunto del 13 luglio 2026 (cfr. capitolo *6.6*) l'UE e il Regno Unito mostrano che una simile attribuzione e le sanzioni vengono impiegate a complemento della protezione tecnica e regolatoria.[82]

La regolamentazione svizzera copre i gestori di rete, i grandi produttori di energia elettrica e i gestori di accumuli nonché i fornitori di servizi con una corrispondente portata di controllo. Mancano prescrizioni vincolanti di cibersicurezza per l'esercizio del singolo impianto di piccole dimensioni. La raccomandazione di settore NA/EEA-NE7 contiene sì dal 2025 un capitolo sull'accesso remoto e sugli aggiornamenti del firmware, ma vi si limita alla protezione mediante password e agli aggiornamenti. Quali di questi approcci entrino in linea di conto per la Svizzera viene ripreso nel capitolo *8 Raccomandazioni*.

7.6 Prospettive normative

Il livello di protezione di base dei prodotti connessi aumenta, le questioni strutturali restano però da ciò impregiudicate.

Sul versante del prodotto i requisiti di cibersicurezza della direttiva sulle apparecchiature radio RED valgono dall'agosto 2025; in Svizzera sono attuati attraverso l'ordinanza sugli impianti di telecomunicazione, e l'autorità di sorveglianza del mercato è l'Ufficio federale delle comunicazioni UFCOM. Diventano verificabili grazie alla serie di norme EN 18031, che concretizza il controllo degli accessi, i meccanismi di aggiornamento sicuri e la gestione delle credenziali. Da dicembre 2027 il Cyber Resilience Act sostituisce i requisiti della RED e li estende a tutti i prodotti con elementi digitali, quindi anche ai dispositivi privi di interfaccia radio. Parallelamente sorgono regimi di test specifici per questa classe di dispositivi: l'omologazione taiwanese, UL 2941 e la certificazione della SunSpec Alliance (cfr. capitoli *7.3.3* e *8.3*).

Ciò che questi corpi normativi realizzano è un livello di base più elevato: essi rendono più difficile l'accesso non autorizzato da parte di terzi. Non affrontano però né la concentrazione del mercato né la controllabilità a distanza da parte del produttore stesso. Ai produttori e ai gestori si raccomanda pertanto di attuare le raccomandazioni del prossimo capitolo non soltanto con l'entrata in vigore di obblighi futuri, bensì già oggi.

[82] OFSI/GOV.UK, comunicazione sulle sanzioni del 13 luglio 2026: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions

8 Raccomandazioni

Le raccomandazioni seguenti discendono dal rilievo centrale del presente rapporto: il rischio determinante è di natura strutturale, ossia una questione di dipendenza dal cloud, di concentrazione del mercato e di protocolli di comando non protetti per costruzione, e meno una questione di singoli dispositivi difettosi. Esse sono articolate per destinatari e mantenute deliberatamente su un piano generale. Il rapporto non si pronuncia contro il fotovoltaico. Le raccomandazioni devono renderne possibile l'ulteriore sviluppo sicuro. Va premesso che la soluzione unica, semplice e completa non esiste: tutti gli approcci hanno svantaggi e permangono rischi residui.

8.1 Per i gestori di impianti di piccole dimensioni

Un'installazione una tantum non basta: gli impianti devono essere configurati correttamente e aggiornati regolarmente, e nel caso di incidente qualcuno deve essere competente. Chi non è in grado di svolgere personalmente questi compiti dovrebbe affidarli contrattualmente all'azienda installatrice o a un terzo. Un'offerta di esercizio da sola non è una prova di competenza. Se un fornitore sia idoneo lo si vede dal fatto che affronti di propria iniziativa i punti seguenti e li assicuri per iscritto.

Punti concreti per il singolo impianto:

- Modificare immediatamente le password predefinite e attivare gli aggiornamenti automatici del firmware oppure installare tempestivamente gli aggiornamenti.
- Non rendere raggiungibile da Internet alcun componente dell'impianto, in particolare non configurare alcun inoltro di porta.
- Decidere consapevolmente se l'impianto debba essere collegato stabilmente al cloud del produttore. Questo collegamento non è tecnicamente indispensabile, nella pratica è però la preimpostazione, e raramente viene messo in discussione. In molti dispositivi la produzione si può leggere localmente anche senza cloud. Un simile esercizio senza collegamento al cloud riduce la superficie di attacco, costa però in comodità, ad esempio il monitoraggio agevole tramite l'app. Va inoltre ponderato che senza collegamento non arrivano più aggiornamenti automatici del firmware e che vulnerabilità note possono così permanere. Dove il dispositivo lo consente, un blocco del controllo è perciò spesso il compromesso migliore: esso continua a consentire gli aggiornamenti, ma non un controllo a distanza attivo (cfr. capitolo *8.4.2*). Gli accessi remoti non necessari andrebbero disattivati.
- Scegliere un sistema di gestione dell'energia secondo caratteristiche verificabili anziché secondo l'ampiezza delle funzioni: comandabilità locale senza cloud permanente, un periodo di aggiornamento e di supporto assicurato e, dove possibile, una verifica indipendente. Un EMS concentra in un punto il controllo su tutti i dispositivi collegati, sicché una singola vulnerabilità riguarda l'intero impianto.
- Farsi confermare alla consegna che sono state impostate password individuali e che l'impianto non è raggiungibile da Internet.
- Fissare contrattualmente chi provvede a che gli aggiornamenti del firmware vengano installati e chi è competente nel caso di incidente.

8.2 Per i gestori di impianti più grandi

Per i gestori di rete e per i gestori di grandi impianti commerciali e industriali valgono i principi consolidati degli ambienti OT e IoT:

- **Inventariare il parco impianti:** rilevare e tenere aggiornati gli inverter, i sistemi di gestione dell'energia e le loro interfacce, compresi tutti gli accessi remoti (produttore, installatore, fornitore di servizi, aggregatore). Ciò che non è noto non si può proteggere.
- **Non raggiungibile da Internet:** gli inverter e i sistemi di gestione dell'energia con le loro interfacce di amministrazione non appartengono a Internet. Se l'accesso remoto è necessario, dovrebbe avvenire attraverso canali protetti, ad esempio attraverso una rete privata virtuale (VPN).

- **Segmentazione della rete:** separare singolarmente il fotovoltaico, la gestione dell'energia e l'infrastruttura di ricarica dal resto della rete, perché un accesso combinato all'immissione in rete e al consumo è particolarmente efficace (cfr. capitolo *2.6*).
- **Separazione del comando locale dalla rete lato Internet:** se viene impiegato il Modbus TCP, l'inverter si trova spesso nello stesso segmento di rete di un sistema di gestione dell'energia collegato a Internet. Un normale firewall di rete protegge qui soltanto da accessi dall'esterno, non però da un aggressore che si trovi già nella rete locale, ad esempio attraverso un dispositivo IoT compromesso (cfr. capitolo *5.3.3).* Più robusto è perciò un sistema di gestione dell'energia con due porte di rete fisicamente separate, una per la parte locale (inverter, senza Internet) e una per la rete lato Internet. Un cambio deliberato del supporto trasmissivo (ad esempio RS485 anziché Ethernet su tutta la linea) riduce il rischio che un dispositivo diventi involontariamente raggiungibile da Internet.
- **Trattare il sistema di gestione dell'energia come punto di concentrazione**: esso controlla tutti i dispositivi collegati e ha quindi una portata maggiore di un singolo inverter.
- **Disciplinare contrattualmente gli accessi dei produttori:** regolare per iscritto portata, scopo e durata di un accesso remoto privilegiato e prevedere un diritto di revoca (cfr. capitolo *5.4.2*).
- **Configurare consapevolmente la controllabilità centrale:** dove l'impianto non necessita di un controllo a distanza da parte del produttore, questo andrebbe limitato e il comando delle funzioni rilevanti per la rete elettrica andrebbe riservato all'entità regolamentata (cfr. capitoli *3.4* e *8.4.2*).
- **Sorveglianza e registrazione**: sorvegliare costantemente gli inverter, i sistemi di gestione dell'energia e i loro accessi remoti e raccogliere e valutare centralmente la registrazione lato dispositivo.
- **Gestire un processo di aggiornamento:** verificare in modo regolato, per il proprio parco, se sia disponibile un firmware nuovo, in particolare rilevante per la sicurezza, e installarlo tempestivamente dopo una ponderazione dei rischi.
- **Prendere precauzioni per il caso di incidente:** stabilire in anticipo chi è competente in caso di incidente di sicurezza, compresi i contatti con il produttore o con l'aggregatore e con le autorità di cibersicurezza. Gli impianti dovrebbero inoltre potersi separare in modo ordinato dal canale di comando interessato, senza spegnersi simultaneamente in modo incontrollato (cfr. capitolo *8.4.2*).
- **Sicurezza negli acquisti:** inserire requisiti di sicurezza nei bandi di concorso e fare della cibersicurezza un criterio di acquisto.
- **Applicare volontariamente lo standard minimo TIC:** applicarlo anche a sistemi che non rientrano nel suo campo di applicazione obbligatorio (cfr. capitolo *7.4).*

8.3 Per le aziende installatrici

Le aziende installatrici decidono nella pratica il livello di sicurezza del singolo impianto. Alla messa in servizio nasce ciò che in seguito è attaccabile: chi imposta le credenziali, configura le interfacce e allaccia l'impianto alla rete stabilisce se una password predefinita resti in vigore, se l'inverter sia raggiungibile da Internet e se l'interfaccia di comando locale resti aperta senza protezione. Queste decisioni non le prende di regola il gestore, bensì l'azienda installatrice. Il BSI ritiene probabile che l'installazione e la configurazione avvengano spesso a opera di imprese specializzate nel solare che portano con sé poca competenza in materia di sicurezza informatica.[83] Tanto più importante è che alla messa in servizio vengano rispettati alcuni principi:

- Impostare per ogni impianto credenziali individuali e non utilizzare password uniformi per l'intero portafoglio clienti. Un codice installatore valido per l'intero parco trasferisce sul piano dell'azienda installatrice lo stesso rischio che il presente rapporto descrive presso i produttori (cfr. capitolo *5.4.2*).
- Non rendere raggiungibile da Internet alcun componente dell'impianto, in particolare non

[83] Ufficio federale tedesco per la protezione della Costituzione (BfV) e Ufficio federale tedesco per la sicurezza informatica (BSI): «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure» (Avviso di sicurezza congiunto: ricognizione di impianti fotovoltaici mal protetti da parte di attori cibernetici statali), 3 giugno 2026. https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

configurare alcun inoltro di porta.
- Disattivare le interfacce non necessarie, ad esempio un punto di accesso Wi-Fi inutilizzato o un'interfaccia di comando locale aperta (cfr. capitolo *5.3.2*).
- Separare l'impianto dal resto della rete domestica o aziendale, in modo che un dispositivo compromesso nella stessa rete non raggiunga senz'altro l'inverter (cfr. capitolo *5.3.3*).
- Alla consegna appartengono una documentazione della configurazione scelta e un accordo chiaro su chi provveda in futuro a che gli aggiornamenti del firmware vengano installati e su chi sia competente nel caso di incidente.
- Negli acquisti, preferire prodotti che funzionino anche senza cloud, offrano interfacce locali protette e per i quali sia assicurato un periodo di aggiornamento.

Affinché questi punti vengano rispettati nella pratica, occorre la corrispondente competenza nell'azienda installatrice. Le basi della cibersicurezza dovrebbero perciò essere parte integrante della formazione e del perfezionamento.

8.4 Per i produttori

8.4.1 Requisiti di base

La responsabilità per il livello di sicurezza fondamentale è dei produttori. Centrali sono:

- **Sicurezza come principio costruttivo:** considerare la sicurezza fin dall'inizio e non aggiungerla a posteriori («Security by Design»).
- **Aggiornamenti sicuri del firmware:** firmati crittograficamente, con protezione contro il ripristino di versioni precedenti vulnerabili.
- **Proteggere gli accessi di manutenzione e di servizio:** le credenziali devono essere specifiche del dispositivo e non ricostruibili, affinché un singolo procedimento di accesso compromesso non riguardi l'intero parco. Un accesso remoto privilegiato dovrebbe inoltre essere limitato nel tempo e revocabile da parte dell'entità responsabile.
- **Registrazione degli eventi rilevanti per la sicurezza:** le autenticazioni, le modifiche ai parametri rilevanti per la rete elettrica, i cambi di firmware e gli accessi tramite account di manutenzione devono essere registrati nel dispositivo e leggibili.
- **Interfacce cloud protette:** autenticazione e autorizzazione integrali in tutte le API.
- **Gestione delle vulnerabilità segnalate:** un processo strutturato di responsible disclosure con un punto di contatto per le segnalazioni raggiungibile e un'eliminazione entro un termine adeguato.
- **Stato sicuro alla fine del supporto:** se il supporto del produttore cessa, ad esempio per cessazione dell'attività, ritiro dal mercato, sanzioni o una controversia sulla distribuzione, il dispositivo deve restare funzionante in locale e non deve poter essere disattivato o bloccato a distanza.
- **Salvataggio e ripristino:** la configurazione e le impostazioni rilevanti per la rete elettrica devono poter essere salvate e ripristinate, e il produttore dovrebbe mettere a disposizione un livello di base verificato del firmware in modo tale che un impianto possa essere rimesso in esercizio anche senza la sua collaborazione.
- **Limitare la portata del proprio accesso remoto:** anche un accesso legittimo non dovrebbe poter comandare o aggiornare simultaneamente l'intero parco di dispositivi. Ciò va garantito tecnicamente mediante reti, server di comando e applicazioni cloud separati (cfr. capitolo *8.5.2*).
- **Offrire un'interfaccia locale protetta:** per il comando locale manca uno standard sicuro diffuso, e un obbligo di cifratura romperebbe l'accoppiamento con i sistemi di gestione dell'energia correnti. I produttori dovrebbero perciò offrire in aggiunta una variante autenticata e cifrata, come già fanno alcuni (cfr. capitolo *3.3*), e disattivare l'interfaccia di fabbrica finché non è necessaria.

Una parte di questi requisiti non è una raccomandazione, bensì normativa di prodotto: per i dispositivi con interfaccia radio valgono dall'agosto 2025 i requisiti di cibersicurezza della direttiva sulle apparecchiature radio RED, che per questi prodotti vengono sostituiti dal CRA a partire da dicembre 2027, il quale vale allora per tutti i prodotti con elementi digitali (cfr. capitolo *7.3.2*). I rilievi della presente analisi mostrano che nella pratica questi requisiti non sono soddisfatti

in modo uniforme. Ai produttori si raccomanda pertanto di non puntare al minimo indispensabile per la dichiarazione di conformità, bensì di attuare i principi che vi stanno dietro: preimpostazione sicura e sicurezza come principio costruttivo.

8.4.2 Blocco preimpostato in fabbrica delle funzioni di controllo rilevanti per la rete elettrica

Oltre all'igiene di base si raccomanda di limitare sul dispositivo ciò che è modificabile da remoto. Il principio non è nuovo: le linee guida per inverter del National Institute of Standards and Technology statunitense (NIST IR 8498)[84] raccomandano di disattivare di fabbrica le capacità non necessarie in ogni modalità d'impiego e di abilitarle solo consapevolmente.

Il blocco è efficace soltanto in un punto che sia in grado di distinguere il contenuto dei comandi e che non sia aggirabile. Un normale firewall di rete non soddisfa la prima condizione, perché i dati di esercizio e i comandi di controllo passano per la stessa connessione verso lo stesso endpoint. Esso è applicabile nell'inverter stesso oppure in un sistema di gestione dell'energia posto a monte (cfr. capitolo *8.2*), quest'ultimo però soltanto se l'inverter non ha alcuna via propria aperta verso il cloud del produttore e rifiuta gli accessi in scrittura locali non autenticati. La raccomandazione distingue tre classi di capacità, per ciascuna delle quali vale un regime diverso: l'accesso remoto nello stato di consegna, i parametri rilevanti per la rete elettrica e i valori di riferimento dell'immissione in rete.

Stato di consegna: da remoto sono ammessi esclusivamente la lettura dei dati di esercizio e gli aggiornamenti del firmware firmati crittograficamente. L'impianto deve continuare a funzionare integralmente senza questo canale, con un comportamento invariato nei confronti della rete.

La raccomandazione di settore svizzera NA/EEA-NE7[85] raccomanda per contro di disattivare dove possibile la funzione per gli aggiornamenti del firmware da remoto e di eseguire gli aggiornamenti soltanto in loco. La considerazione è comprensibile, perché il canale di aggiornamento è effettivamente l'accesso remoto più potente. Con un parco di centinaia di migliaia di impianti di piccole dimensioni essa conduce però, dal punto di vista dell'NTC, al rischio maggiore: senza un canale di aggiornamento funzionante, le vulnerabilità note restano aperte per anni. Il BSI tedesco consiglia vivamente di verificare regolarmente se siano disponibili nuove versioni del software e di installare al più presto, dopo una ponderazione dei rischi, almeno quelle che eliminano lacune di sicurezza.[86] Il rapporto segue questa linea, ma la collega a requisiti posti alla catena di aggiornamento stessa: firma crittografica, protezione contro l'installazione di versioni più vecchie e una versione accertabile, le cui modifiche al comportamento verso la rete siano documentate.

Parametri rilevanti per la rete elettrica: i parametri rilevanti per la rete elettrica vengono impostati alla messa in servizio e sono poi bloccati. Si intendono i valori che determinano il comportamento dell'impianto nei confronti della rete: ad esempio l'impostazione del Paese nel suo insieme, i parametri di protezione per tensione e frequenza, le condizioni di inserzione e reinserzione, il comportamento in potenza reattiva e attiva in funzione di tensione e frequenza nonché il comportamento in caso di guasti di rete. L'estensione è definita dall'allegato E della raccomandazione di settore NA/EEA-NE7. Al tempo stesso essi costituiscono un vettore di attacco particolarmente efficace (cfr. capitolo *6.3*, tipo B). Lo stesso tipo di protezione è richiesto da Swissgrid senza alcun riferimento a un attacco: il comportamento degli impianti in caso di distacco dalla rete e le loro condizioni per la reinserzione dovrebbero essere fissati direttamente nell'impianto, per ridurre una grande componente di incertezza nella fase impegnativa del

[84] National Institute of Standards and Technology statunitense NIST, Cybersecurity for Smart Inverters – Guidelines for Residential and Light Commercial Solar Energy Systems, NIST IR 8498, dicembre 2024; https://doi.org/10.6028/NIST.IR.8498

[85] AES, raccomandazione di settore «Netzanschluss für Energieerzeugungsanlagen an das Niederspannungsnetz NA/EEA-NE7 – CH 2025» (Allacciamento di impianti di produzione di energia alla rete a bassa tensione): https://www.strom.ch/de/dokument/netzanschluss-fuer-energieerzeugungsanlagen-das-niederspannungsnetz-naeea-ne7-ch-2025-0

[86] Ufficio federale tedesco per la protezione della Costituzione (BfV) e Ufficio federale tedesco per la sicurezza informatica (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure» (Avviso di sicurezza congiunto: ricognizione di impianti fotovoltaici mal protetti da parte di attori cibernetici statali), 3 giugno 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

ripristino della rete. Questi valori vanno dunque protetti non soltanto perché si lasciano manipolare, bensì anche perché l'esercizio della rete fa affidamento su di essi.

La protezione particolare di questi valori è raccomandata anche a livello internazionale:

- Le raccomandazioni del NIST per gli inverter raccomandano interfacce disattivate di fabbrica, software proveniente soltanto da fonti verificate e una separazione delle funzioni di regolazione dalle interfacce di comunicazione. Una password da sola non vi è più considerata adeguata per accessi con effetto su infrastrutture critiche.
- Lo studio di Secura raccomanda di mantenere immutabili i parametri critici e di consentire la configurazione a distanza soltanto con un'approvazione locale.[87]

Per la Svizzera non esiste al riguardo alcuna prescrizione uniforme. Determinante sarebbe che un simile blocco non si fondi soltanto su un'autenticazione. Un titolo di autorizzazione disponibile centralmente si lascia impiegare simultaneamente su molti impianti, ed è proprio questa simultaneità l'effetto che il presente rapporto descrive come rilevante per il sistema. È quindi opportuno vincolare la revoca del blocco a un'autorizzazione locale sul dispositivo, in modo che essa non possa essere attivata simultaneamente su molti impianti attraverso un accesso disponibile centralmente, ad esempio mediante un'azione fisica in loco. Il blocco vale per tutti i percorsi di scrittura su questi valori, quindi interfaccia di comando, interfacce di comunicazione locali, collegamento al cloud e accesso di manutenzione. Lo stesso principio è perseguito da tempo dalla piombatura di contatori e dispositivi di protezione. Si intende con ciò la protezione da modifiche non autorizzate e non l'immutabilità in quanto tale. Se le condizioni di allacciamento cambiano, un adeguamento nel parco impianti esistente deve restare possibile.

Valori di riferimento dell'immissione in rete: bloccati, ma abilitabili in loco non appena l'impianto partecipa a un servizio di rete. Una semplice limitazione dell'intervallo dei valori di riferimento non basta, perché la riduzione della potenza fino a zero è proprio il servizio di rete previsto e corrisponde al tempo stesso allo schema di attacco di tipo A. Vi appartengono due condizioni:

- Se la capacità è abilitata, non dovrebbe passare per il cloud del produttore, bensì per il gestore di rete o per l'aggregatore vincolato contrattualmente (cfr. capitolo *8.5.1*).
- Se il collegamento di comando cade o resta assente, il dispositivo ripiega dopo un tempo di mantenimento su uno stato fissato alla messa in servizio. Il tempo di mantenimento impedisce che un disturbo della comunicazione provochi simultaneamente in molti impianti una brusca variazione di potenza.
  Lo stesso requisito viene posto anche senza uno scenario di attacco. Swissgrid raccomanda di costruire i nuovi impianti «fail-safe»: dovrebbero poter continuare a funzionare in sicurezza anche senza comando esterno e senza una comunicazione funzionante, per cui i gestori di rete dovrebbero elaborare prescrizioni per uno stato stabilito in anticipo. Il fattore scatenante è lì l'ordinaria interruzione della comunicazione, ossia lo stesso caso che il tempo di mantenimento descritto sopra affronta. La raccomandazione non presuppone quindi l'ipotesi di un aggressore.[88]

In questo modo lo stato protetto è la preimpostazione, e ogni ulteriore controllabilità a distanza diventa una decisione consapevole, visibile e presa in loco. Contro un firmware manipolato un dispositivo non si protegge però così, perché il codice sul dispositivo può aggirare qualsiasi blocco lato dispositivo. Contro il produttore stesso e contro una catena di aggiornamento compromessa agiscono perciò soltanto l'integrità di questa catena, una nuova verifica in caso di modifiche sostanziali del firmware (cfr. capitolo *8.5.3*), la diversificazione e la verificabilità indipendente.

Per concludere, sul rapporto tra questa raccomandazione e l'orientamento della politica energetica: il settore si muove verso una maggiore controllabilità. Nel suo white paper sull'integrazione del fotovoltaico Swissgrid rileva che per gli impianti fotovoltaici la flessibilità non sarà in futuro un'opzione, bensì un presupposto. Il blocco preimpostato in fabbrica delle funzioni

[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 «Systemverträgliche Integration Photovoltaik» (Integrazione del fotovoltaico compatibile con il sistema), marzo 2026, https://www.swissgrid.ch/it/home/newsroom/blog/2026/20260330-01.html

di controllo qui proposto non è in contraddizione con ciò. Esso non richiede alcuna rinuncia alla flessibilità, bensì soltanto che la sua abilitazione avvenga in loco e che il comando rilevante per la rete elettrica passi in seguito attraverso l'entità regolamentata.

8.5 Per la politica e la regolamentazione

8.5.1 Competenza

Colmare la lacuna di responsabilità per gli impianti di piccole dimensioni: le prescrizioni esistono, ma sono insufficienti. I requisiti di cibersicurezza della direttiva sulle apparecchiature radio comprendono soltanto i dispositivi con interfaccia radio e si fondano sulla dichiarazione del produttore, e la raccomandazione di settore sull'allacciamento alla rete si limita alla protezione mediante password e agli aggiornamenti. Efficaci sono gli strumenti che non fanno leva sul singolo gestore. Interventi normativi sono qui prevedibilmente necessari, perché questa protezione non nasce da sé. Come approcci si offrono modelli che altri Stati già utilizzano: condizioni di allacciamento alla rete per la controllabilità degli impianti (come in Lituania) oppure criteri di acquisto e di promozione (come a livello UE). Nessuna di queste vie è perfetta (cfr. capitolo *7*). Questa necessità di intervento non discende soltanto dai rilievi tecnici. Il SIC segnala espressamente che la Svizzera guadagna attrattiva come obiettivo quando i Paesi vicini proteggono maggiormente la propria infrastruttura critica e la Svizzera non fa altrettanto (cfr. capitolo *2.5*).

Assicurare la sovranità di controllo sulle funzioni rilevanti per la rete elettrica: l'obiettivo non è un divieto del cloud, bensì una risposta chiara alla domanda su chi possa impartire a un impianto comandi rilevanti per la rete elettrica. Questa facoltà dovrebbe spettare a un'entità che sia essa stessa regolamentata e che risponda della stabilità della rete: al gestore della rete di distribuzione oppure a un aggregatore vincolato contrattualmente che soggiace allo standard minimo TIC. Lo stesso modello è raccomandato dall'associazione di settore europea, che distingue tra funzioni critiche e non critiche: avviare, arrestare e modificare la potenza attiva e reattiva soltanto attraverso l'entità regolamentata; sorveglianza e aggiornamenti software anche attraverso altri canali, sempre che questi si lascino interrompere in caso di sospetto.[89] Per la Svizzera questo principio è già impostato nei suoi tratti essenziali: il gestore della rete di distribuzione può utilizzare la flessibilità di un impianto soltanto a supporto della rete.[90] Swissgrid segnala al tempo stesso le lacune pratiche:[91] mancano una comunicazione standardizzata tra l'impianto, rispettivamente il sistema di gestione dell'energia, e il gestore della rete di distribuzione, una cascata di comandi standardizzata tra i gestori di rete nonché l'attuazione tecnica della regola legale secondo cui la flessibilità garantita a supporto della rete prevale su tutti gli altri segnali di comando. Chi vuole disciplinare in modo vincolante la sovranità di controllo deve perciò creare anche l'interfaccia necessaria a tal fine. Senza di essa la via attraverso il cloud del produttore resta l'unica che funziona nella pratica. Resta da chiarire se un collegamento permanente a un cloud del produttore sia in generale necessario dal lato della rete e, in caso affermativo, quali requisiti questa infrastruttura debba soddisfare. La sola ubicazione dell'hosting non basta a tal fine (cfr. capitolo *5.4.5*). Attuabile sul dispositivo sarebbe la prescrizione che gli inverter abbiano attivo di fabbrica un blocco delle funzioni di controllo rilevanti per la rete elettrica (cfr. capitolo *8.4.2*). Questo orientamento coincide con la posizione del BSI tedesco (cfr. capitolo *7.3.1*).

Designare una competenza per il rischio aggregato: per il singolo impianto di piccole dimensioni nessuno è responsabile e, per il rischio che nasce solo dalla somma di molti impianti, manca un'entità designata. Resta da chiarire quale entità osservi questo rischio aggregato, coordini nel caso di incidente e sorvegli l'efficacia delle misure sul prodotto e sull'allacciamento.

Prendere precauzioni per il caso di incidente: accanto alla prevenzione occorre la capacità di riconoscere un abuso in corso e di porvi fine in modo ordinato. Un interruttore di emergenza

[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 LAEI (RS 734.7) e art. 19a OAEI (RS 734.71). Per l'inquadramento: AES, «Potenzial und Limiten der neuen Flexibilitätsregulierung» (Potenziale e limiti della nuova regolamentazione della flessibilità), dicembre 2025, https://www.strom.ch/it/perspective/potenziale-e-limiti-della-nuova-regolamentazione-sulla-flessibilita
[91] Swissgrid SA, white paper «Systemverträgliche Integration Photovoltaik» (Integrazione del fotovoltaico compatibile con il sistema), marzo 2026, https://www.swissgrid.ch/it/home/newsroom/blog/2026/20260330-01.html

centrale non esiste, e uno spegnimento di massa a scopo difensivo metterebbe esso stesso in pericolo la stabilità della rete. Un canale di comando compromesso si lascia separare senza pericolo soltanto se gli impianti ripiegano allora su uno stato sicuro e conforme alla rete (cfr. capitolo *8.4.2*) e se un'entità designata tiene il quadro della situazione e coordina le parti coinvolte. Questa capacità serve soprattutto a respingere una compromissione persistente e a gestire le conseguenze dopo un incidente, non a impedire il primo attacco, che si svolge nell'arco di secondi.

8.5.2 Portata di un singolo accesso

Limitare la portata di un singolo accesso: rilevante per la rete non è la gravità di una vulnerabilità, bensì la sua portata. Ne discende una misura che agisce indipendentemente dalle quote di mercato e dalla qualità dei prodotti: nessun singolo punto dovrebbe poter modificare simultaneamente un intero parco di dispositivi. Nella produzione classica questo limite risultava da sé, perché una centrale comprende raramente più di circa 1,5 gigawatt e il suo sistema di conduzione raggiunge soltanto quella singola centrale. Con i cloud dei produttori e con gli aggregatori esso viene meno. L'associazione di settore europea propone perciò di prescriverlo espressamente e di sostenerlo tecnicamente:[92]

- un limite massimo per la potenza di produzione controllabile tramite un unico sistema di controllo: chi ne esercita di più deve impiegare a tal fine sistemi separati privi di cause di guasto comuni
- una segmentazione dell'accesso remoto proprio del produttore, in modo che non si possa comandare l'intero parco in una sola volta
- accorgimenti tecnici contro l'aggiornamento simultaneo di tutti i dispositivi, affinché resti tempo per intervenire quando un aggiornamento è difettoso o manipolato
- ritardi casuali specifici per ogni dispositivo per comandi di controllo selezionati. Quali comandi siano interessati e per quanto tempo si ritardi va stabilito mediante norme e in accordo con l'esercizio della rete

Queste misure non richiedono alcuna rinuncia al controllo a distanza e alcuna modifica delle quote di mercato. Esse limitano soltanto quanto può ottenere un singolo comando. Vi appartengono tre riserve: il valore di soglia è aperto e dovrebbe prima essere stabilito. L'attuazione risiede nell'architettura del produttore ed è dall'esterno difficilmente verificabile; senza un obbligo di prova resta quindi un'autodichiarazione. Ed essa limita la portata, non la dipendenza stessa: un accesso remoto segmentato procura nel caso di incidente il tempo per intervenire, ma lascia al produttore il controllo su ogni singolo segmento.

Promuovere per tempo la diversificazione: il mercato degli inverter si sta fortemente consolidando. Per la cibersicurezza ciò è immediatamente rilevante, perché un campo eterogeneo di produttori è esso stesso un fattore di protezione: produttori, piattaforme e versioni del firmware differenti rendono più difficile raggiungere molti impianti con un unico attacco. Al contrario, con ogni ulteriore consolidamento del mercato nasce un «Single Point of Failure» più grande. L'obiettivo dovrebbe perciò essere quello di avere durevolmente a disposizione produttori in più regioni del mondo, e non il privilegiamento di una determinata provenienza. Strumenti sono ad esempio criteri di acquisto che premiano le strategie multifornitore. Il punto tocca il diritto degli acquisti e il diritto commerciale ed è attuabile unilateralmente solo in misura limitata. La finestra temporale potrebbe restringersi, perché diversi fornitori dispongono sì ancora di capacità, ma perdono quote di mercato. Come ciò si sviluppi resta aperto. La diversificazione riduce il rischio di un unico exploit valido per tutti i produttori, ma non risolve il problema strutturale di fondo: con una soglia inferiore al due per cento del parco europeo (cfr. capitolo *6.5)* praticamente ogni produttore rilevante sul mercato resta di per sé rilevante per il sistema. Secondo Secura, nei Paesi Bassi basta l'attacco a un singolo produttore; due entrano in linea di conto a tal fine per quota di mercato (cfr. capitolo *5.4*). La diversificazione è perciò un complemento sensato, ma non un sostituto delle altre misure qui indicate.

[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

8.5.3 Verifica e adeguamento del parco impianti esistente

Verifica di prodotto con una componente di ciclo di vita: un regime di test di cibersicurezza riferito al prodotto per inverter e sistemi di gestione dell'energia è possibile e sensato. Taiwan mostra, con l'analisi del codice sorgente, l'analisi del traffico e la verifica dell'integrità del firmware, quanto in profondità possa spingersi una simile verifica. Determinante è però che un tale regime non si fermi a un esame del tipo una tantum: sono necessari un procedimento crittografico di aggiornamento prescritto e una nuova verifica in caso di modifiche sostanziali del firmware. Va considerato il limite di ogni verifica di prodotto: essa affronta l'attaccabilità da parte di terzi, ma non rende indipendenti dal produttore stesso. Contro lo scenario dell'attore interno o statale che controlla la catena di aggiornamento legittima agiscono soltanto la diversificazione e una limitazione tecnica di ciò che il cloud può comandare a distanza (cfr. capitolo *5.2*).

Non tutto ciò richiede nuove disposizioni normative. Per gli inverter con interfaccia radio la conformità con i requisiti di cibersicurezza della direttiva sulle apparecchiature radio e con la relativa norma EN 18031 si potrebbe verificare già oggi nell'ambito della sorveglianza del mercato (cfr. capitolo 7.4 Regolamentazione in Svizzera). Regimi di test riferiti al prodotto per questa classe di dispositivi sorgono inoltre a livello internazionale: accanto all'omologazione taiwanese esistono con UL 2941[93] e con la certificazione della SunSpec Alliance programmi[94] a cui un requisito svizzero o europeo potrebbe rifarsi.

Utilizzare per la cibersicurezza il controllo dell'impianto già esistente: gli impianti fotovoltaici sono soggetti a controllo obbligatorio secondo l'ordinanza sugli impianti elettrici a bassa tensione (OIBT). Un organo di controllo indipendente verifica l'impianto dopo la realizzazione, il rapporto di sicurezza va al gestore di rete e il controllo si ripete periodicamente. Esiste così una procedura obbligatoria che rileva l'impianto nello stato installato e il cui risultato finisce presso un'entità regolamentata. Essa fa leva là dove i requisiti di prodotto e le prescrizioni al singolo gestore non bastano. Si raccomanda di completare il relativo protocollo di controllo con pochi punti accertabili in modo univoco: ad esempio password predefinite modificate, nessuna raggiungibilità da Internet, interfacce non necessarie disattivate e lo stato del blocco del controllo (cfr. capitolo *8.4.2*). Swissgrid propone la stessa via per le impostazioni di esercizio e chiede separatamente, per la cibersicurezza, requisiti minimi che devono essere anche controllati, senza indicare una procedura a tal fine.[95] Necessario a tal fine è un adeguamento delle prescrizioni, però su una procedura consolidata anziché in un regime nuovo, e verificabile resta soltanto ciò che si lascia accertare senza margine di interpretazione.

Non dimenticare il parco impianti esistente: tutte le misure precedenti agiscono soprattutto attraverso i nuovi impianti. Soltanto il controllo periodico dell'impianto raggiunge anche il parco esistente, per quanto lentamente. Il parco impianti esistente resta per anni il fianco scoperto più ampio (cfr. capitolo *7.3.4*). Attuabile sarebbe lì un'unità di comunicazione posta a monte, che collabori con gli inverter esistenti e attribuisca il comando al gestore di rete. Essa trasferisce così al parco esistente ciò che propone il capitolo *8.5.1 Competenza*.

Comune a tutte queste raccomandazioni è una direzione: il fotovoltaico deve poter continuare a crescere, ma il controllo su centinaia di migliaia di dispositivi rilevanti per la rete elettrica non deve stare in mano a pochi soggetti, i cui interventi sono tecnicamente illimitati e non verificabili dall'esterno. La finestra temporale per farlo è aperta. Si chiude con ogni impianto che viene costruito oggi e che fra vent'anni sarà ancora collegato alla rete.

[93] UL Solutions, UL 2941, Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources, 2023; programma di certificazione da febbraio 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 «Systemverträgliche Integration Photovoltaik» (Integrazione del fotovoltaico compatibile con il sistema), marzo 2026, https://www.swissgrid.ch/it/home/newsroom/blog/2026/20260330-01.html