National Test Institute for Cybersecurity

Cybersecurity of Photovoltaic Systems

Findings and Recommendations

Version	1.0
Date	17 September 2026
Classification	Public
Authors	Tobias Castagna, Stefan Gloor, Andreas Leisibach, Dilip Many, Raphael M. Reischuk, Lukas Sohrmann, Fabio Zuber
Responsible	Tobias Castagna

With the Support of swissenergy

Table of Contents

Acknowledgements

Special thanks go to the organizations and experts who supported this investigation, whether by providing test devices, by sharing insights into how such devices are used in different environments, or by contributing to the costs. Through their commitment, they made a substantial contribution to the success of this security analysis. They include:

• SwissEnergy, Swiss Federal Office of Energy SFOE
• Federal Electricity Commission ElCom
• Federal Office of Communications OFCOM
• National Cyber Security Centre NCSC
• Aziende Industriali di Lugano (AIL) SA
• ch-solar AG
• HHM Gruppe (HEFTI. HESS. MARTIGNONI.)
• Stadt Zürich Organisation und Informatik (OIZ)
• Swisscom (Switzerland) Ltd
• Swissgrid Ltd
• Swissolar
• Verband Schweizerischer Elektrizitätsunternehmen (VSE)
• Zurich Airport Ltd

• Prof. Dr. Christof Bucher, Bern University of Applied Sciences BFH
• Prof. Roger Buser, Lucerne University of Applied Sciences and Arts HSLU
• Prof. Dr. Andreas Heinzelmann, ZHAW Zurich University of Applied Sciences
• Ruben Santamarta, independent cybersecurity researcher
• Dr. Leonard Schliesser, Center for Security Studies CSS, ETH Zurich
• Arrigo Triulzi Lampugnani, independent cybersecurity expert
• Bastian Widmer, independent cybersecurity expert

Special thanks also go to Robin Seidel, who, as part of his studies at ETH Zurich and in cooperation with the NTC, identified serious vulnerabilities in a connected device of a photovoltaic system. This preliminary work reinforced the NTC's sense of the need for action and provided key impetus for the present analysis.

1 Management Summary

Key Points at a Glance

Photovoltaics is systemically important: By the end of 2025, around 338,000 grid-connected photovoltaic systems were installed in Switzerland. Their annual output covered 13.7 percent of final electricity consumption. Around midday on sunny days, these systems regularly cover more than half of instantaneous consumption.

The investigation: The National Test Institute for Cybersecurity NTC assessed seven inverters and four energy management systems on its own initiative. The NTC was supported in this by industry organizations and SwissEnergy.

More than 50 findings across eleven products: Seven findings are critical, six high. Five products had at least one critical or high finding. Four devices could be completely taken over.

Manufacturers respond quickly: The NTC has already reported the findings to the affected manufacturers before this report was published. Many responded immediately and have already remediated the vulnerabilities.

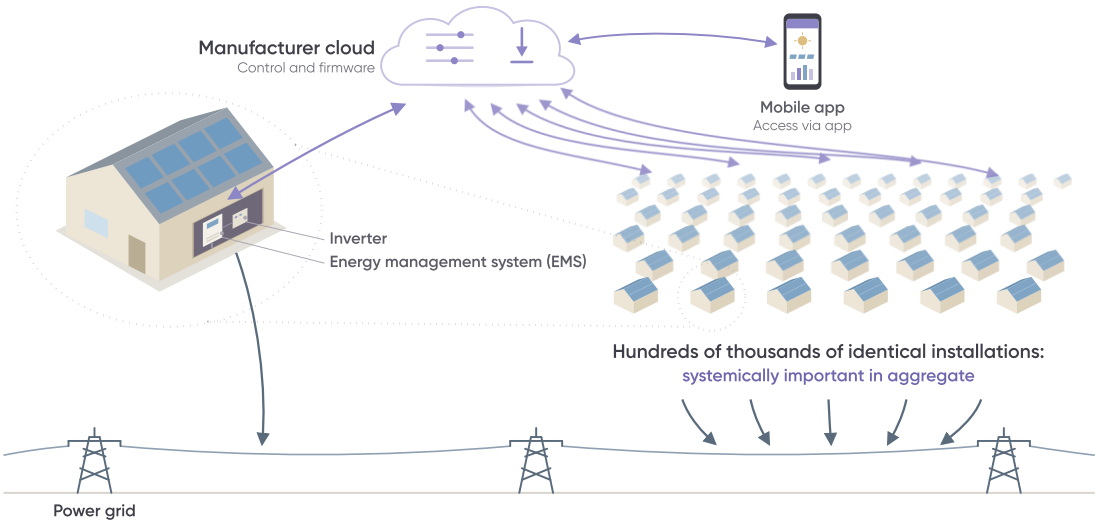
It is not only severity that matters, but reach: A single vulnerability in a relevant component can affect thousands of connected installations. Six findings are of this kind. The individual installation is insignificant to the grid; the installed base as a whole is critical infrastructure.

Structural risk: The greatest risk cannot be remedied through improved product security. It arises from the connection of the devices to the manufacturers' clouds, through which firmware updates, for example, are delivered.

Lack of responsibility: The requirements fall short for small-scale installations, and no one is responsible for the risk arising from their sum.

By the end of 2025, around 338,000 grid-connected photovoltaic systems with a peak output of roughly 9.5 gigawatts (GW) were installed in Switzerland (for comparison: the Gösgen nuclear power plant produces around 1 GW). Their annual output of just under 8 terawatt-hours (TWh) covered 13.7 percent of final electricity consumption, roughly at the level of the Gösgen nuclear power plant. By 2030, output is set to more than double according to the Federal Council's new interim targets (18.7 TWh). For grid operation, however, it is not the annual total that counts but the instantaneous contribution: around midday on sunny days, photovoltaics regularly covers more than half of consumption; on 4 July 2026 at 2 p.m., close to 85 percent.

This changes the structure of electricity generation: alongside a few large, regulated power plants, there are now hundreds of thousands of small, cloud-connected, and largely identically configured installations, insignificant individually but systemically important in aggregate.



The Swiss installed base consists almost entirely of small installations on residential and commercial rooftops, operated by private individuals and smaller companies without expertise in operating and maintaining critical infrastructure. What used to require physical access to a power plant is today possible via central remote access. The risk lies not in photovoltaics itself, but in the way its control is organized.

So far, privately operated installations have rarely been independently assessed for vulnerabilities: incentives, clear responsibilities, and appropriate regulation are lacking. The electricity industry's cybersecurity requirements (ICT minimum standard) are aimed at organizations and only apply to producers of at least 100 megawatts that can be controlled via a single system. They are neither applicable to nor intended for a photovoltaic installation on a single-family home.

On its own initiative, the National Test Institute for Cybersecurity NTC therefore assessed eleven digital products widely used in the Swiss photovoltaic sector over about a year: seven inverters and four energy management systems from a total of eight manufacturers. The testing team and a substantial part of the funding came from the NTC; several organizations, mostly from the energy sector, provided test devices and contributed to the costs. The analysis was also financially supported by SwissEnergy. Neither the manufacturers nor the supporting organizations influenced the selection, scope of testing, or results. All findings were reported confidentially to the manufacturers. As a rule, this report does not name any products or technical details; instead, it describes typical risk patterns and the recommendations derived from them.

In total, the assessments produced more than 50 findings, seven of them critical and a further six rated high. Five of the eleven products had at least one high or critical finding. For four products, the NTC gained complete control over the device, in some cases via remote code execution, in others through an inadequately protected manufacturer maintenance access.

Four recurring patterns were identified:

- deficiencies in authentication and access control, such as default passwords
- insecure maintenance access, for example with identical credentials for the entire device fleet
- missing or weak encryption of communication over local interfaces
- interfaces that cannot be disabled

For nearly all inverters assessed, the local control interface can be used, without authentication, to change how much power the installation feeds in, down to zero. This interface is active above all where an energy management system controls the installation. Taken on its own, such access affects only one installation. If many installations are manipulated simultaneously, however, this can endanger the stability of the power grid. The grid must ensure a balance between generation and consumption at all times. A vulnerability therefore becomes grid-relevant not through its severity alone, but through its reach: six findings act through a central entity on an entire device base and thus on many installations at once.

The security level of the individual products is no worse than that of other widely used connected devices the NTC has assessed in comparable analyses. No evidence of deliberately built-in backdoors or hidden communication components was found. Most manufacturers responded quickly to the reported vulnerabilities; for some findings the disclosure process is still ongoing, among other reasons because new firmware has to be provided worldwide for several model ranges. What distinguishes solar installations from other connected devices is not the quality of the products but their role: what usually remains a nuisance for a household appliance carries more weight here, because these installations are systemically important in aggregate.

The decisive risk for the Swiss power grid therefore lies not in the individual device but in dependence on a few manufacturers: their cloud infrastructure is used to control the installations and supply them with firmware, and in addition most vendors retain privileged maintenance access to their entire device base.

Market concentration increases the number of affected installations: in 2025, more than half of the newly installed inverters came from a single manufacturer, and around 80 percent from four (Huawei, Fronius, Sungrow, and SolarEdge). This risk cannot be addressed through improved product security, but only by reducing dependencies: verifiable assurances, multiple vendors in

the market, and a technical limitation of what is possible remotely at all. Internationally, distributed photovoltaics is increasingly being treated as a matter of critical infrastructure, no longer merely of climate policy. Estonia, the Czech Republic, and Germany have issued official warnings. Taiwan is making proof of cybersecurity part of product approval; Lithuania ties grid connection to security requirements. Switzerland has yet to take this step.

Based on the risks identified, this report derives recommendations for five groups of stakeholders.

Operators of small-scale installations have the greatest influence through their choice of an established provider to whom they entrust not only the installation but also the technical operation. At handover, they should ensure that individual passwords have been set and that the installation is not directly reachable from the internet, contractually specify who is responsible for updates and incident response, and forgo unnecessary remote control.

Operators of larger installations have expertise and bargaining power that operators of small-scale installations lack. They should inventory their installed base including interfaces and remote access points, separate photovoltaics, energy management, and charging infrastructure from the rest of the network, configure central controllability deliberately, put manufacturer access on a contractual basis, and include security requirements in their tenders. Where the ICT minimum standard does not apply, voluntary adoption is worthwhile.

Installation companies determine the security level of the individual installation in practice, because commissioning decisions determine what can later be exploited. For each installation they should set individual credentials and not use passwords that are identical across their customer base, do not expose the inverter to the internet, disable unnecessary interfaces, and separate the installation from the rest of the home or company network. Handover includes documentation of the configuration and a clear agreement on who will install updates in the future. In procurement, they should favor products that can function without the cloud, offer protected local interfaces, and have a guaranteed update period.

Manufacturers should understand security as a design principle: device-specific and non-reconstructible credentials, no hardcoded secrets, secured local interfaces, and signed firmware updates. Maintenance access must be time-limited, logged, and revocable by the operator. One safeguard is central here: by default, the ability to control grid-relevant functions remotely is disabled at the factory and can be re-enabled only on site. This limits large-scale remote control by technical means, not just by policy. Operation must also remain possible without the cloud.

Policymakers and authorities should close the gap for small-scale installations. Effective requirements are those that target the product and not the operator: minimum requirements for placing inverters and energy management systems on the market, security requirements as a condition for grid connection, and recurring testing that does not end with a one-time approval. Equally necessary is a designated responsibility for the risk that arises only from the sum of the small-scale installations. The growing aggregation of small-scale installations by aggregators and virtual power plants must be taken into account. For installations, a mandatory inspection procedure already exists in the form of the safety certificate, which could be extended to include cybersecurity items.

There is no simple and complete solution; all approaches have advantages and disadvantages, and residual risks remain.

This report is not an argument against photovoltaics, but one for its secure expansion. The expansion reduces the need for energy imports. This independence, however, should not be replaced by a new dependence: dependence on a few manufacturers with remote access to thousands of grid-relevant devices. The expansion should continue, with the same expectation of controllability that is already taken for granted for other critical infrastructure today.

2 Background and Motivation

2.1 From a Few Large Power Plants to Many Small Ones

Switzerland's electricity generation was long based predominantly on a limited number of large, centrally operated, and regulated power plants. Smaller installations such as small hydropower plants do exist as well, but neither their number nor their connectivity is significant in this respect. With the expansion of photovoltaics, a second world has emerged alongside them: hundreds of thousands of small, decentralized "power plants" on the roofs of residential and commercial buildings. With this second world come new cyber risks affecting the entire electricity supply, which this report addresses.

2.2 Photovoltaics Has Become Systemically Important

Photovoltaics has developed in Switzerland from a niche technology into a mainstay of the electricity supply. By the end of 2025, around 338,000 systems with a cumulative peak output of around 9.5 gigawatts were installed. Their annual output of just under 8 terawatt-hours covered 13.7 percent of final electricity consumption[1] and thus corresponded roughly to the planned annual output of the Gösgen nuclear power plant.[2]

The instantaneous contribution at peak times is more telling than these annual figures. Around midday on sunny days, photovoltaics regularly covers more than half of instantaneous consumption, and considerably more on peak days. On 4 July 2026 at 2 p.m., for example, it was around 6,100 megawatts against a load of around 7,200 megawatts, and thus close to 85 percent[3].

Photovoltaics has thus become relevant to security of supply. Considered on its own, a single installation remains insignificant to the grid. In aggregate, however, it becomes significant, and because these installations are connected and similarly configured, they can also be influenced collectively, whether as intended and in a grid-serving manner by the grid operator or abusively by an attacker. It is therefore not the individual installation that becomes critical infrastructure, but the installed base as a whole.

This installed base continues to grow. On 26 November 2025, the Federal Council set technology-specific interim targets for the first time in the Energy Ordinance: of the 23 terawatt-hours that renewables excluding hydropower are to contribute by 2030, 18.7 fall to photovoltaics. Compared with just under 8 terawatt-hours in 2025, that is more than double within five years. The overarching goal of the Energy Act requires 35 terawatt-hours by 2035 and 45 terawatt-hours by 2050 for renewables excluding hydropower. The Federal Council has so far set technology-specific interim targets only for 2030.[4] As the installed base grows, so too does the need to make it controllable.

2.3 Why the Topic Has Received Little Attention So Far

Internationally, the cybersecurity of photovoltaic systems has recently gained attention. The devices common in Switzerland, however, have so far rarely been assessed independently and systematically. There are several reasons for this:

- **Little incentive for installation operators**: The installations are operated predominantly by

[1] Swiss Federal Office of Energy (SFOE), "Solar Energy Statistics 2025": https://pubdb.bfe.admin.ch/de/sammlungen/statistik-sonnenenergie
[2] Swissolar, "Swiss Solar Monitor 2025": https://www.swissolar.ch/de/markt-und-politik/markt-schweiz/solarmonitor-schweiz
[3] Instantaneous values: energy-charts.info (Fraunhofer ISE), net electricity generation Switzerland, week 27/2026 (4 July 2026, 2:00 p.m.: load 7,209 MW, solar 6,121 MW): https://www.energy-charts.info/charts/power/chart.htm?c=CH&l=de&year=2026&week=27
[4] Federal Council, media release "Federal Council approves amendments to ordinances in the energy sector", 26 November 2025: https://www.admin.ch/de/newsb/dvb52hRdMmNdS3aNKL96C

private individuals and smaller companies. For private individuals in particular, what makes their connected installation vulnerable is unlikely to be a priority. If an installation is knocked out by a cyberattack, they simply buy in the electricity they lack. Measured against these electricity costs, a security assessment would be disproportionately expensive. The actual risk arises only when many installations are manipulated simultaneously, and then affects not the individual operators but the electricity supply as a whole.

- **No responsibility for the cybersecurity of individual small-scale installations**: Grid operators are responsible for the stability of the overall system and thus bear the risk. Through the connection conditions they can impose technical requirements, but for the cybersecurity of private small-scale installations in operation they lack the authority (see chapter 7.4).
- **Costly procurement and risky testing**: The devices are comparatively expensive and cumbersome to procure for independent testing, and testing requires work on grid-connected devices, in part under high voltage, and thus special precautions and expertise.
- **Limited transferability of international studies**: Existing analyses from abroad reflect Swiss market conditions only to a limited extent. In part, different products are common here, and some vendors relevant in the Swiss market do not appear in international studies at all.

2.4 Why a Cyber Threat Exists

What matters most for security is that modern installations are usually connected to the internet and to the manufacturer's cloud. This makes it practicable to influence a large number of installations simultaneously and in a coordinated way. The distribution system operator, too, can in part address many installations at once, for example to curtail feed-in. This path differs in several respects, however: it extends only as far as the grid area of the operator concerned, it lies in the hands of a regulated company, and it often uses a dedicated control channel separated from the internet (ripple control). A manufacturer cloud, by contrast, reaches a device fleet over the internet, across grid areas and national borders. What the simultaneous manipulation of many installations would mean for grid stability is addressed in chapter *6 Impact on Grid Stability*.

This threat meets unfavorable conditions. The operators generally have no particular cyber expertise, and no one is obliged to ensure cybersecurity for the operation of their installations. While grid operators and very large generators are subject to cyber requirements such as the ICT minimum standard, small-scale installations, and thus practically all Swiss photovoltaic systems, fall through this net. For generators, the standard applies only from 100 MW, that is, from 100,000 kW. A typical rooftop installation is in the double-digit kilowatt range, and thus more than three orders of magnitude smaller.

This assessment is shared by the national grid company. In its white paper "System-Compatible Integration of Photovoltaics"[5] Swissgrid explicitly lists the cybersecurity risks among the challenges of system operation: inverters, as well as other installations such as charging stations and energy management systems, are increasingly remotely controllable over the internet. Inadequate requirements and a lack of problem awareness increase the risk that external actors could destabilize the electricity system through them.

2.5 The Security Policy Environment

This technical starting point coincides with a deteriorating security policy situation. In its situation report "Security Switzerland 2026"[6] the Federal Intelligence Service (FIS) notes a marked and lasting deterioration of the security policy environment. Critical infrastructure is explicitly classified as threatened by physical as well as cyberattacks. The FIS also states that the infrastructures of European countries cannot be considered in isolation. An attack on Swiss infrastructure in order to hit other states dependent on it is just as conceivable as, conversely, collateral damage from attacks on foreign infrastructure. The FIS likewise points out that the attractiveness of such targets grows the more NATO and EU states protect their critical infrastructure without

[5] Swissgrid AG, white paper "System-Compatible Integration of Photovoltaics" March 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html
[6] Federal Intelligence Service (FIS), "Security Switzerland 2026": https://www.vbs.admin.ch/de/newnsb/jyRmuld1hBVy

Switzerland following suit.

That this assessment is not an abstract one is shown by the coordinated cyberattack on Poland's electricity and heat supply in December 2025. Among those affected were more than 30 wind and solar farms[7]. The United Kingdom and the EU officially attributed the attack to the Russian intelligence service FSB (Center 16) in July 2026.[8] Against the backdrop of the closely interconnected European grids and the FIS's assessment, comparable developments are also relevant for Switzerland.

That distributed photovoltaics is specifically in focus here is shown by a joint security advisory from the German Federal Office for the Protection of the Constitution (BfV) and the Federal Office for Information Security (BSI) of 3 June 2026[9]. According to their findings, Russian cyber actors are actively reconnoitering photovoltaic systems that are connected to the internet without protection. The focus is on monitoring systems that also permit controlling access to the installations. Those affected are predominantly installations of private individuals and cooperatives with no energy-industry background. For some of these installations, access is possible without credentials, and the software versions are in part severely outdated. This is reconnaissance, not an attack. The advisory shows, however, that precisely the class of installation this report examines is being systematically cataloged by state actors.

2.6 Out of Scope: Battery Storage, Charging Infrastructure, and Other Connected Devices

Not the subject of this analysis, but of growing importance, are connected consumers and storage such as battery storage, charging stations for electric vehicles, and heat pumps. Battery storage in particular is spreading rapidly. Among new photovoltaic systems on Swiss single-family homes, a considerable share is now equipped with storage.[10] From a cybersecurity perspective, attacks that use photovoltaics in combination with battery storage or charging infrastructure are especially relevant, because they allow both feed-in and consumption to be manipulated. Charging infrastructure has already been examined by the NTC in an earlier report[11].

[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, sanctions notice of 13 July 2026: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions
[9] Federal Office for the Protection of the Constitution (BfV) and Federal Office for Information Security (BSI), "Joint Security Advisory (BfV and BSI): Reconnaissance of Poorly Protected PV Installations by State Cyber Actors" 3 June 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html
[10] Swiss Federal Office of Energy (SFOE), "Solar Energy Statistics 2025" https://pubdb.bfe.admin.ch/de/sammlungen/statistik-sonnenenergie
[11] National Test Institute for Cybersecurity NTC, Report on the Cybersecurity of Charging Infrastructure, 2023: https://en.ntc.swiss/news/2023-analysis-electric-mobility-charging-infrastructure

3 The Ecosystem of a Photovoltaic System

This chapter describes the building blocks a photovoltaic system consists of. It explains how they communicate with one another and with the internet, and who can control them. The account remains deliberately descriptive and shows where the architecture offers an attack surface. Whether these surfaces actually proved to be a risk in the assessment is not the subject of this chapter. Which components were assessed, and why, is set out in chapter *4 Methodology*. The results follow in chapter *5 Findings and Risks*.

3.1 The Components and How They Interact

A typical photovoltaic system consists of a few basic building blocks. Depending on the design, they are integrated into one another to varying degrees. For the following discussion, they are presented in a functionally separated way. The **solar modules** generate direct current (DC). The **inverter** converts it into grid-compliant alternating current (AC) and feeds it into the grid. It is thus the central, actively controllable component of the system. For remote monitoring, the inverter is connected to the internet via a **communication module** (often already integrated into the inverter), usually via Wi-Fi, cellular, or cable. This connection is not technically mandatory, but is the rule in practice. In modern systems, monitoring usually takes place via the manufacturer's internet portal, and where no communication module is installed, or where additional devices such as battery storage, a charging station, or a heat pump are also controlled, an **energy management system** often handles communication with the outside. Via this connection, the operating data flow to a **manufacturer cloud**, which stores and visualizes them. Depending on the manufacturer, it also enables remote monitoring, remote control, and firmware updating of the system. Finally, the **mobile or web app** is the user interface for the operator and in turn accesses the cloud. In addition, further connected consumers and storage, such as **battery storage**, **charging stations for electric vehicles, or heat pumps,** are often integrated. Such additional components further enlarge the attack surface and the possible impact. At the grid connection point, there is also the meter of the distribution system operator. It measures the energy drawn and the energy fed in and is being replaced step by step in Switzerland by an intelligent metering system (**smart meter**) that makes the readings remotely readable. The meter does not belong to the operator but to the grid operator, and thus forms its own connection to the outside, independent of the manufacturer.

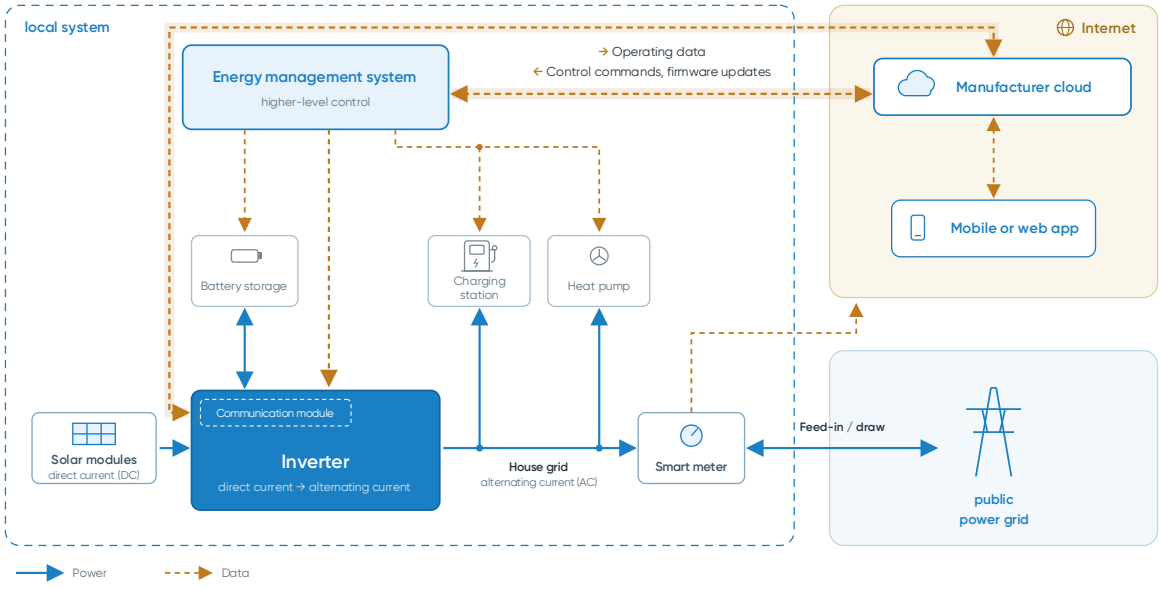


Figure 1: Schematic overview of a typical photovoltaic system

3.2 Inverter and Energy Management System

Understanding controllability hinges on the distinction between inverter and energy management system (EMS), because the two terms are often conflated in everyday use.

The **inverter** converts electricity and feeds it into the grid. Through its grid-serving functions such as active- and reactive-power setpoints or characteristic curves, it is the element that directly influences feed-in.

The **energy management system** is a higher-level controller. It coordinates several devices in a system - typically inverter, battery storage, charging station, and heat pump - and optimizes their operation, for example according to self-consumption.

This dual character is what makes the EMS especially significant for cybersecurity. As part of the solution, an EMS can reduce dependence on individual manufacturer clouds: not every device necessarily has to be connected to its manufacturer's cloud and an EMS placed sensibly between the local network and the inverter can limit the direct reachability of the individual devices. But it also aggravates the problem: whoever controls the EMS controls every device connected to it and can therefore cause at least as much damage as through a single inverter, potentially more, because the EMS also controls further components such as battery storage and a charging station. Cross-manufacturer EMS providers additionally aggregate this control across different device brands. The EMS is thus a local component at its core, but at the same time a single point of control whose compromise extends further than that of a single inverter.

3.3 Communication Paths and Known Vulnerabilities

Two questions are security-relevant: which components communicate with one another, and how well these connections are protected. The communication module reports the operating data to the manufacturer cloud and receives commands from it. The app in turn typically accesses the cloud, not the installation directly. If the communication module is integrated into the inverter, this connection takes place internally within the device. It is different as soon as an external device is to address the inverter directly, such as an energy management system. Then the connection runs locally in the building or home network.

For this local connection, industrial protocols are common, most notably Modbus: formerly over a serial cable connection (RS485), increasingly over the network (Modbus TCP). Alongside these, proprietary protocols occur. Modbus was designed for isolated installations and by itself offers neither encryption nor authentication. Some manufacturers add proprietary authorization mechanisms. A TLS-based security extension added in 2018 is barely used in practice. This interface is therefore significant for the findings that follow.

According to this architecture, the inverter is not directly reachable from the internet. The path from outside instead leads via the manufacturer cloud. The manufacturer cloud, in turn, can by design monitor, control, and update very many installations at once.

This picture matches the existing research. An evaluation[12] of 93 vulnerabilities with CVE numbers disclosed since 2012 across 34 manufacturers attributes the largest part to the monitoring and cloud layer - around 38 percent to solar monitoring and around 25 percent to the cloud - while the inverter with communication module was affected in just under 30 percent. Around 80 percent of all cases are rated high or critical. These figures should be read with caution, because they count occurrences and not risk, and the connected layer is far easier to examine remotely. They do not, however, remain theoretical: six of the cataloged vulnerabilities have been regularly exploited by botnets since 2022. In the end, what matters is less the number of vulnerabilities than the fact that a single cloud reaches many installations at once.

[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 Central and Local Control

The building blocks can be ordered by how many installations a compromised component can influence. A central entity such as the manufacturer cloud acts on many installations simultaneously. Whoever controls it can send commands to all connected devices. A local entity such as the inverter itself, the mobile app, or a local control device, by contrast, influences only its own installation. This distinction separates scalable attacks, which strike many installations remotely, from non-scalable attacks, which remain confined to the individual installation. It is the reason why individual small installations are insignificant on their own but become relevant in the connected mass. For grid-effective manipulation, the central level is the worthwhile point of attack. This central controllability can, however, also be deliberately limited technically. This report therefore recommends designing devices so that the cloud can only monitor the installation and supply it with signed updates, but can no longer control it (see chapter *8.4.2*).

Alongside the manufacturer cloud, a second central control level is increasingly emerging: aggregators and virtual power plants. Here, a provider pools many distributed installations via internet interfaces and markets their aggregated output, for example as balancing energy. One example is the pilot project "PV4Balancing"[13] of the national grid company Swissgrid, in which aggregated photovoltaic systems reduce their feed-in on demand as negative tertiary control reserve. Even closer to the mass of small installations is a second example: Helion received approval from Swissgrid to pool private small-scale photovoltaic systems, home storage, and charging stations via its own platform and to offer the aggregated output on the balancing energy market[14]. This places precisely those installations under central remote control that individually are subject to no cybersecurity requirements. The aggregator itself, by contrast, is covered as soon as it can access at least 100 MW via a single system (see chapter *7.4).* The "Flexpool"[15] of CKW, for example, already combines over 1,000 MW from around 1,700 customer installations at a single control point, albeit technologically mixed and not solely from photovoltaics. This development is double-edged: used in a grid-serving way, controllable, pooled installations are a stabilization instrument. At the same time, the aggregator creates a further central control point that, if compromised, opens up already-coordinated remote control over many installations. This pooling is not a by-product but part of the target architecture. Swissgrid states that the participation of decentralized units in the balancing energy markets should be made as easy and accessible as possible via aggregators, and names a central flexibility platform with a coordination mechanism as the most suitable option. This is being tested in a further pilot project, the "TSO-DSO coordination."[16] The number of installations reachable via a single control point is likely to continue growing. That makes it all the more important to clarify the security requirements for this level while it is under construction. The NTC has not assessed these platforms; the classification concerns the structure, not the security of individual providers.

3.5 Installation Types and Operators

The network connection and the level of protection depend strongly on the type of installation. Following the federal funding categories, installations up to 100 kW count as **small-scale installations**: they comprise single-family homes, multi-family homes, and smaller commercial buildings. Small-scale installations are usually on the normal building or home network and are operated by private individuals or smaller companies, who generally have no particular cyber expertise. **Large installations** above 100 kW are more often professionally managed and segmented behind a firewall. The largest installations are connected to their own substation and to the distribution system operator and more often forgo a connection to the manufacturer cloud. Conversely, while cloud connection is the rule for small-scale installations, it is not mandatory there either.

[13] Swissgrid, pilot project "PV4Balancing": https://www.swissgrid.ch/de/home/newsroom/blog/2025/die-sonne-als-ressource-fuer-einen-stabilen-netzbetrieb.html
[14] Helion Energy AG, virtual power plant for private customers based on the "Helion ONE" platform: https://www.gebaeudetechnik.ch/de/news/virtuelles-kraftwerk-fuer-die-schweiz--252
[15] CKW (Axpo Group), "Flexpool": https://www.ckw.ch/ueber-ckw/medienstelle/medienmitteilungen/2025/1000-megawatt-virtuelles-grosskraftwerk-von-ckw-erreicht-meilenstein
[16] Swissgrid AG, white paper "System-Compatible Integration of Photovoltaics" March 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html

2025	Anz. Anlagen	Leistung in MW	Ø Leistung in kW
bis 4 kW	1'132	3.0	2.7
über 4 kW bis 10 kW	9'073	68.9	7.6
über 10 kW bis 20 kW	14'864	211.9	14.3
über 20 kW bis 30 kW	4'831	117.8	24.4
über 30 kW bis 50 kW	3'134	119.8	38.2
über 50 kW bis 100 kW	1'977	138.9	70.3
über 100 kW bis 1000 kW	2'175	536.2	246.6
über 1000 kW	72	136.4	1'882.5
Total Netzverbundanlagen	**37'257**	**1'332.9**	**35.8**

Figure 2: Grid-connected installations by size. Source: Solar Energy Statistics 2025[17], SFOE

The size distribution clearly shows the imbalance. Of the 37,257 grid-connected installations newly installed in 2025, 35,011 - that is, 94 percent - were at most 100 kW. They accounted for roughly half of the newly installed capacity. The average installation has a capacity of around 25 kW, the median around 11 kW. At the same time, around 40 percent of Swiss photovoltaic production comes from installations under 30 kW. The installed base, for which no operational cybersecurity requirements apply, thus contributes a considerable share of generation.

3.6 Market Concentration

What matters for security is not only how many installations are installed, but how many different manufacturers they come from: the manufacturer determines firmware, maintenance access, and the update chain, which is why a single finding can apply to its entire device base, including installations without a cloud connection. In Switzerland, this field has shifted several times. The PV Barometer 2026[18] evaluates project designs for this: in 2017, Fronius stood at 45.7 percent market share; in 2020 the market was split among three similarly sized providers (FIMER 23.5 percent, Fronius 22.9, SolarEdge 22.8); in 2025, Huawei accounted for 52.3 percent, Fronius 13.3, Sungrow 9.2, and SolarEdge 8.2 percent. The share of the largest provider is thus higher today than ever before in the observation period. The number of providers has not fallen; what has changed is the distribution.

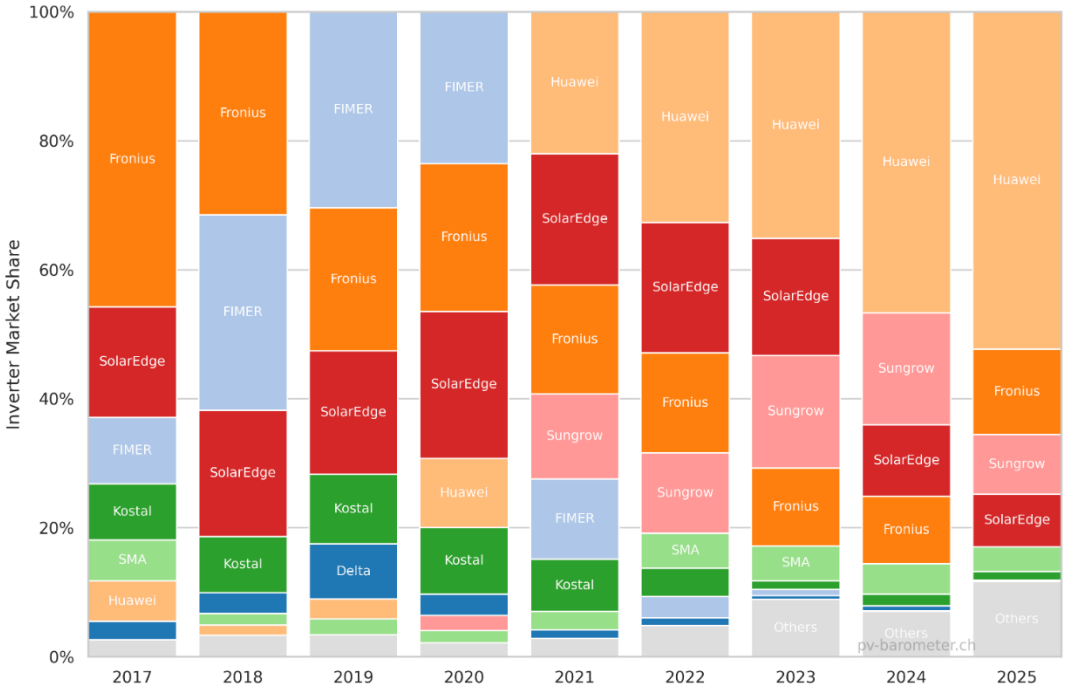


Figure 3: Market shares of inverter manufacturers in Switzerland. Source: PV Barometer 2026

[17] Swiss Federal Office of Energy (SFOE), "Solar Energy Statistics 2025": https://pubdb.bfe.admin.ch/de/sammlungen/statistik-sonnenenergie
[18] Bern University of Applied Sciences & Eturnity AG, "PV Barometer 2026": https://www.pv-barometer.ch/

4 Methodology

The NTC subjected inverters and energy management systems to a comprehensive technical security analysis. The assessment was guided by three principles:

- **Market relevance:** a selection of devices based on their prevalence in the Swiss market.
- **Independence:** no involvement of manufacturers in selection, execution, and funding; contact exclusively within the scope of vulnerability reporting.
- **Scalability:** a focus on vulnerabilities that can be used to manipulate many installations at once.

Over a period of about one year, the NTC devoted a total of around 1,300 working hours to the investigation. It was supported by numerous organizations from the energy sector, which provided test devices and contributed to the costs. The manufacturers of the assessed products were not involved. The following sections describe the subject of the investigation and its scope, the selection and procurement of the devices, the test setup, the analytical focus, and the handling of the vulnerabilities found.

4.1 Subject of the Investigation and Scope

The focus of the assessment lay deliberately on inverters and energy management systems, as well as on installations in residential and smaller commercial buildings. Both follow from the architecture described in chapter *3 The Ecosystem of a Photovoltaic System*: inverters and energy management systems are the central, grid- and cloud-connected components of a photovoltaic system and can actively control feed-in. Such small-scale installations, in turn, are subject to no operational cybersecurity requirements. On the product side, since August 2025 the cybersecurity requirements of the EU Radio Equipment Directive apply to newly placed devices, provided they have a radio interface (see chapter *7.3.2*). These set a basic level but say nothing about the configuration, operation, and maintenance of the installed system, and rely on the manufacturer's self-declaration. The installations are usually operated by private individuals or smaller companies without particular cyber expertise, and have so far rarely been independently assessed.

The solar modules were deliberately not examined. Some modules do contain active electronics such as module optimizers. However, these are, if networked at all, connected only to the inverter and thus lie outside the scalable attack picture. Also not part of the investigation were components such as smart meters, battery storage, and charging stations for electric mobility. These components are security-relevant too and are gaining in importance: battery storage, for example, is grid- and cloud-connected, similar to inverters, and coordinated charging or discharging of many storage units would have a comparable effect on the grid.

Also outside the scope of the investigation were very small plug-in solar devices ("balcony power plants"). They are considerably less common in the Swiss market than in Germany and are already the subject of independent investigations. That serious vulnerabilities exist in this category too is shown, for example, by the radio vulnerabilities disclosed by the Chaos Computer Club (CCC)[19] in Hoymiles microinverters (2026) (see chapter *5.3.4*).

The legal framework also shaped the depth of testing. The NTC procured the devices itself and could examine them without restriction. The manufacturer clouds, by contrast, are third-party production systems: access to them without the operator's consent can be punishable under Art. 143bis of the Swiss Criminal Code (StGB). A legal opinion commissioned by the NTC in 2023[20] delimits which testing activities are permissible without such consent.

Consent could only have been obtained through the manufacturers. That would have meant

[19] Chaos Computer Club (B. Heinz "Hunz"), "Wireless Interface Vulnerabilities of Hoymiles Microinverters" 2026: https://www.ccc.de/updates/2026/blinkenlights-hoymiles
[20] Walder Wyss AG, "Expert opinion on the criminal liability of "ethical hacking": https://www.walderwyss.com/en/news/2023-06-26_rechtsgutachten-zur-strafbarkeit-von-fuer-das-nationale-testinstitut-fuer-cybersicherheit-ntc

involving them in the investigation and would conflict with the principle of independence. The NTC therefore deliberately confined itself to the scope permissible without consent and refrained from an in-depth examination of the cloud layer.

This report assesses technical feasibility, not the intent of possible actors and not the course of crisis management.

4.2 Device Selection

A complete set of statistics on the inverters installed in Switzerland does not exist. Official data are available on the number of installations and the distribution of capacity (Pronovo statistics[21], Solar Energy Statistics[22] of the SFOE). For manufacturers' market shares, by contrast, only the PV Barometer survey exists, which is produced by a market participant but has reported the shares annually since 2017, thus making the development over time visible. Exact figures cannot be derived from it, but orders of magnitude can, and these are clear. In 2025, a good half of the newly installed inverters came from a single manufacturer, around two-thirds from two, and around 80 percent from four. Seven inverters from six manufacturers were therefore examined, including the market-leading providers.

For energy management systems, the data situation is even thinner. No comparable statistics exist. Decisive here were conversations with experts from the industry. Four systems were assessed.

The selection thus covers both time horizons. Looking back, the multi-year view helps: because most of the Swiss installed base was built only in recent years, the market shares of those years approximately reflect the installed base. Looking ahead, what is installed today shapes the risk for more than a decade.

4.3 Procurement

The devices were procured through partner organizations and by the same route a regular customer would use. This approach ensures that real as-delivered states and configurations were assessed, and not specially prepared test samples. Contact with the manufacturers took place exclusively within the scope of vulnerability reporting.

The assessment was carried out on the NTC's initiative. Design, execution, and evaluation lay entirely with the NTC and took place in its own laboratory. It was funded to a substantial extent from the NTC's own resources, supplemented by several partner organizations from the energy sector, which contributed to the costs and supplied test devices. Manufacturers were not involved, and the partner organizations had no influence on the scope of testing or the results.

4.4 Test Setup

Operating the inverters requires a DC supply on the input side. Because operating real solar modules in the laboratory is not practical, the modules were replaced by a controllable DC source. This allowed the devices to be tested under reproducible conditions. The focus was on analyzing firmware, interfaces, cloud connection, and configuration. One fundamental caveat remains: a device could change its behavior as soon as it detects that it is being tested. Such a test-bench mode would not necessarily be detectable with a laboratory-based approach. The NTC is aware of this possibility and has counteracted it as far as feasible: the devices were obtained through regular sales channels and operated in their as-delivered state, and the test setup was designed to differ as little as possible from a real installation.

[21] Pronovo AG, statistics: https://pronovo.ch/de/services/berichte/
[22] Swiss Federal Office of Energy (SFOE), "Solar Energy Statistics 2025": https://pubdb.bfe.admin.ch/de/sammlungen/statistik-sonnenenergie

4.5 Focus on Scalable Vulnerabilities

At the center of the analysis were vulnerabilities that can be used to manipulate a large number of installations at once. Vulnerabilities affecting only the individual installation - such as those requiring physical access to the device - were not the focus. This distinction between scalable and non-scalable vulnerabilities runs through the entire report and determines how the individual findings are weighted.

4.6 Vulnerability Disclosure Process

All identified vulnerabilities were reported confidentially to the affected manufacturers within the scope of a coordinated disclosure process (responsible disclosure) to enable their remediation before publication. This approach follows the NTC's responsible-disclosure policy[23] and common practice in the industry. This public report therefore deliberately refrains from technical details and from naming affected products, and instead presents the underlying risk patterns.

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

5 Findings and Risks

5.1 Overview

The NTC examined eleven products: seven inverters from six manufacturers and four energy management systems. Two of the energy management systems come from manufacturers that also make one of the assessed inverters, so the eleven products are distributed across eight manufacturers. In total, more than 50 vulnerabilities were identified, seven of them with a criticality of "critical" and six with "high." Five of the eleven products had at least one high or critical finding.

For four products, the NTC gained complete control over the device, that is, the highest privilege level (root access). For one product, three vulnerabilities allowed the execution of arbitrary program code on the device (remote code execution); all three are classified as critical. For three products, an inadequately protected manufacturer maintenance access sufficed. This privilege level is significant because it allows not only controlling the installation but also altering the firmware and thus the device's behavior as a whole.

Six of the more than 50 findings act through a central entity on many installations at once and thus scale. The rest remain confined to the individual installation. These six findings are the ones most relevant to grid stability, because a vulnerability becomes grid-relevant not through its technical severity but through the fact that it can be applied to an entire device fleet. In its notice[24] of June 2026, the BSI likewise explicitly cites the "exploitation of scaling effects" as the path from the individual installation to grid stability. Two of the six findings are classified as "critical," one as "high," and three as "medium." This classification assesses the impact on the assessed product and not the consequences for the power grid. A finding classified as "medium" in a cloud that controls a device fleet can weigh more heavily on the grid side than a critical finding on the individual device. Five of the six findings come from the layer with the greatest leverage, the manufacturer cloud, specifically from externally reachable interfaces. An in-depth examination of the cloud itself was not possible for legal reasons (see chapter *4.1*). Even the external view was sufficient, however, to find vulnerabilities with grid-wide reach.

For some of the findings, including several of the critical ones, the coordinated disclosure process is not yet complete at the time of publication. This reflects the nature of the task itself, not a lack of cooperation: in some cases several model ranges worldwide are affected and require new firmware.

The security level of the individual products is generally no worse than that of other widely used "Internet of Things" (IoT) devices, and in some aspects even better. This assessment is based on the NTC's testing experience with comparable device classes, namely from its assessments of peripheral devices[25] and of products within the scope of the RED Directive[26]. What must be taken seriously, however, are the recurring patterns and above all the structural risks that dominate the overall picture and are the focus of this chapter. That is precisely the crux: what remains a nuisance with connected household appliances here affects a class of devices that is systemically important in aggregate.

German security authorities confirm that these weaknesses do not exist only in the laboratory: they observe photovoltaic systems where access is in part possible without credentials and whose software versions are severely outdated (see chapter *2.5*).

[24] Federal Office for the Protection of the Constitution (BfV) and Federal Office for Information Security (BSI)"Joint Security Advisory (BfV and BSI): Reconnaissance of Poorly Protected PV Installations by State Cyber Actors", 3 June 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html
[25] NTC, Summary Report on the Cybersecurity of Peripheral Devices: https://www.ntc.swiss/aktuelles/2026-bericht-peripheriegeraete
[26] NTC, Report on the Cybersecurity of Connected Devices With Regard to the RED Directive: https://www.ntc.swiss/aktuelles/2025-bericht-red

5.2 Two Perspectives on the Threat

The findings should be read against the backdrop of two fundamentally different threat perspectives:

- **Vulnerability to third parties**: technical vulnerabilities that an external attacker exploits. This type of vulnerability occurs with all manufacturers and can be reduced through better product quality and independent testing.
- **The manufacturer or its supply chain as attacker:** Here it is not a matter of technical vulnerabilities but of dependencies. The legitimate means of remote maintenance and firmware distribution can be misused by the manufacturer itself, by an attacker who compromises the manufacturer, by malicious employees, or on the basis of a state order directed at the manufacturer. This risk is manufacturer-specific and cannot be addressed through technical security measures. It can be reduced only by making the dependency itself smaller: through verifiable assurances instead of mere trust, through diversification, and through technical limitation of what is possible remotely at all (see chapter *7.6*).

Both perspectives run through the findings that follow. This distinction is not unusual. In its position paper[27] on cybersecurity in the energy sector, the German BSI explicitly cites "the manipulation of energy infrastructure by manufacturers or third parties" among the new attack vectors, naming inverters as an example.

5.3 Results of the Technical Assessment

5.3.1 Manufacturer Clouds

For scalable attacks, the cloud layer is the most significant. A cloud manages an entire device fleet, which is why a single vulnerability there potentially affects a large number of installations, unlike a flaw on an individual device.

This very layer, however, could be examined only to a limited extent. Tests on a manufacturer cloud access a third-party production system and, without the operator's consent, are permissible only with restrictions under Art. 143bis StGB[28]. Obtaining such consent would have meant involving the manufacturers in the investigation, which would have conflicted with the principle of independence. The examination therefore confined itself to the scope permissible without consent. All the more remarkable is the result: even within this narrow scope, vulnerabilities were found in several manufacturer clouds, including those of the SQL injection and cross-site scripting categories. The manufacturers remediated them after they were reported.

This also reveals a structural problem: the layer with the greatest leverage is precisely the one that independent testing bodies cannot fully examine without the manufacturer's participation.

A finding from this examination is instructive in several respects. A vulnerability classified as critical affected the energy management system of the Swiss manufacturer Solar Manager. It would have allowed a remote attacker to access individual systems - not just one, but successively further systems. The manufacturer responded in exemplary fashion and closed the gap within a few hours. In addition, it gave the NTC consent to examine its cloud as well. This removed the legal barrier described above, which otherwise makes examining the cloud layer difficult. The case shows that this barrier can be removed when a manufacturer understands transparency as an opportunity. Unlike elsewhere, the NTC names the manufacturer here, with its consent and as a positive example of how the vulnerability disclosure was handled.

The case is instructive for a second reason as well. Solar Manager is common above all in the DACH region, with an estimated 50,000 installations. Products with such regional prevalence

[27] Federal Office for Information Security (BSI), "Position Paper: Cybersecurity in Germany's Energy Sector": https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Positionspapier_Cybersicherheit_Energiesektor.html
[28] Walder Wyss AG, "Expert opinion on the criminal liability of "ethical hacking": https://www.walderwyss.com/de/news/2023-06-26_rechtsgutachten-zur-strafbarkeit-von-fuer-das-nationale-testinstitut-fuer-cybersicherheit-ntc

generally do not appear in international studies, which mostly originate in the US or from globally active security firms. They fall through the net, even though they control tens of thousands of installations in Switzerland. This gap can be closed only through assessments that start from the actual Swiss market.

An internationally documented case shows how great the leverage of a single cloud can be, and how difficult remediation can prove[29]. The Dutch Institute for Vulnerability Disclosure (DIVD), which searches for and reports vulnerabilities similarly to the NTC, came across credentials for an administration account on the monitoring platform Solarman that were publicly exposed in a software repository (GitHub) and were not protected by a second security level (multi-factor authentication). Through this one account, almost a million installations worldwide, with a combined output of over 10 GW, could be viewed and controlled - down to reading and overwriting the firmware. The handling of it was telling: the operator did not respond for months, the exposed password was even reset to the disclosed value after being corrected once, and a solution was achieved only through diplomatic channels and the involvement of the Chinese CERT. The case thus stands for two patterns at once: the enormous reach of a central cloud, and the sometimes difficult cooperation with manufacturers on remediation in practice. In the Netherlands, it subsequently led to parliamentary inquiries and increased official attention to the cybersecurity of inverters. A later, considerably larger disclosure shows that this was not a one-off outlier[30]: in 2024, the security firm Bitdefender found new vulnerabilities in the same Solarman and Deye platforms that, according to media reports, would theoretically have affected an even larger fleet (around 195 GW of output across more than two million installations).

5.3.2 Local Interfaces and Manufacturer Access

The remaining findings are distributed across recurring classes. Most frequently, and across many of the assessed devices, deficiencies in authentication and access control occurred (such as missing session expiry and missing or unchanged default passwords), along with missing or weak encryption of communication over local interfaces. Further findings concerned interfaces that could not be disabled (such as a Wi-Fi hotspot that could not be switched off) and insecure manufacturer maintenance access via remote access (SSH, in some cases with fleet-wide identical credentials).

Independent studies confirm that these are not isolated cases. In the study SUN:DOWN, Forescout documented[31] comparable weaknesses at several market leaders (among them insecure cloud interfaces, hardcoded and unchangeable credentials, and firmware updates without a cryptographic signature). The researcher specializing in cybersecurity in the energy sector, Ruben Santamarta, describes[32] insecure remote maintenance access at European manufacturers.

One finding shows particularly clearly how poorly such maintenance access is sometimes protected. On one device, the password of the installer account could be reset and reassigned via the device's own Wi-Fi access point without any login at all. With the administrative rights thus obtained, remote access (SSH) and root access could then be activated. In the as-delivered state, this is protected by a default password that must be changed at first login. In normal operation, however, the access remains unused, and thus the default password remains in effect. Whoever logs in first assigns the new password themselves. For complete compromise, access to the device's own Wi-Fi was sufficient.

The chaining is instructive: three protective mechanisms are present: an account login, a deactivatable remote access, and a password change at first login. None takes effect, because the first can be bypassed without authentication and the third only takes effect once someone

[29] Dutch Institute for Vulnerability Disclosure (DIVD), case “Solarman” (DIVD-2022-00009): https://csirt.divd.nl/cases/DIVD-2022-00009/
[30] Bitdefender, investigation into vulnerabilities in the Solarman and Deye platforms, August 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” May 2026: https://www.reversemode.com/2026/05/a-practical-analysis-of-cyber-physical.html

logs in, which cannot be assumed.

Other vulnerabilities came to light only through analysis of the device firmware. On one product, services were found that run with the highest privileges and process inputs before any login has occurred. In one case, a debug service was still active in the shipped firmware that copies a parameter from a network request into a fixed-size memory area without checking its length (buffer overflow). Because this service runs with the highest privileges, such an overflow can be used to inject and execute one's own program code. Without credentials and with mere access to the local network, complete control over the device (root access) was attainable this way. Notably, the service is not needed in operation, yet was still reachable in the shipped firmware. This is precisely the aim of the principle set out by the guidelines cited in chapter *8.4.2 Factory-Set Control Lock for Grid-Relevant Functions*: what is not needed in every deployment scenario should be disabled at the factory.

The local control interface is especially consequential. Through it, on nearly all inverters assessed, not only can readings be retrieved, but the device's grid-relevant settings can also be changed, often without authentication. Technically, this happens via the industrial protocol Modbus. Whether the manufacturer uses the standardized SunSpec register models or its own scheme makes no difference: SunSpec[33] only describes the meaning of the registers and is not a security layer. This interface is deactivated at the factory by several manufacturers. For operation with an energy management system, however, it must be activated. When it is active, access takes place without any login, which means every device on the same network can send commands. Between energy management system and inverter, there is thus very often no security.

Common to all findings described in this section is that they require access to the local network. They allow complete control over a single device, not over many.

5.3.3 From a Local to a Scalable Attack

Local vulnerabilities, taken on their own, affect only the individual installation and do not scale. One consideration qualifies this reassurance: an attacker already on the local network can control inverters via the unprotected Modbus TCP. There, the effect is attainable by design, even without a vulnerability. An attacker reaches the local network, for example, via infected IoT devices. Both classic botnets of infected computers and IoT devices (such as the Mirai type) and the rapid rise of so-called residential proxy networks show that home devices are compromised on a large scale, in which hijacked home connections are re-let as access nodes.[34] The FIS, too, describes anonymization networks made up of poorly protected, internet-exposed home devices such as routers, in part via infrastructure rented in Switzerland.[35] If many home networks are compromised in this way, a local vector becomes a broadly effective one.

5.3.4 What Was Not Examined: Permanent Damage to Devices

The possibility of permanently damaging devices by operating them in certain states was not the subject of the NTC's own investigation. That this is not a purely hypothetical danger is shown by the Hoymiles case. In 2026, researchers at the Chaos Computer Club demonstrated that microinverters can be permanently rendered unusable via the unprotected radio protocol by loading manipulated firmware.[36] For four devices, the NTC gained complete control over the device (root access, the highest privilege level), but did not test permanent damage. In addition, further protective mechanisms may take effect, for example at the electronics level. Such an attack would, unlike a temporary grid disturbance, have long-term consequences.

[33] SunSpec Alliance, "Modbus" specification: https://sunspec.org/modbus/
[34] BSI, report on residential proxy abuse, Profiles of Current Botnets: Mirai, 2026: https://www.bsi.bund.de/dok/12820010
[35] Federal Intelligence Service (FIS), "Security Switzerland 2026": https://www.vbs.admin.ch/de/newnsb/jyRmuld1hBVy
[36] Chaos Computer Club (B. Heinz "Hunz"), "Wireless Interface Vulnerabilities of Hoymiles Microinverters", 2026: https://www.ccc.de/updates/2026/blinkenlights-hoymiles

5.3.5 What Was Not Found

What was not found is just as significant as the vulnerabilities that were. There was no evidence of deliberately built-in backdoors or hidden, undocumented communication components of the kind discussed in international reporting.[37] In one device, a microphone was initially discovered, which gave cause for investigation. The analysis, however, revealed a documented operating function (interaction via knock signals) and no indication of a covert function. That does not, however, close the case: the component can capture more than operation requires and could potentially be misused after a firmware update. Since the same function would be possible without a microphone, this choice must be judged a vulnerability - entirely without malicious intent. That is precisely the pattern of this report: the risks identified are structural in nature and do not require the assumption of malicious intent in order to be serious.

5.4 Structural Risks

The actual message of this report lies not in the individual findings but in five structural risks that exist independently of the quality of individual products.

5.4.1 Dependence on the Manufacturer Cloud

The central controllability described in the chapter "The Ecosystem of a Photovoltaic System" is functionally intended, but shifts control over a large number of installations to a single point. This gives rise to a risk in the event of malfunction or compromise of the manufacturer, and in the extreme case also the possible use as a geopolitical means of pressure. The dependence is reinforced by the fact that many devices are permanently connected to the cloud, in part encouraged by incentives such as extended warranties. The firmware update channel belongs to the same layer: it is necessary, but likewise acts on the entire fleet at once, and what is distributed through it changes the device profoundly.

The attack on the KA-SAT satellite network in February 2022 showed that this channel is exploited in reality. The attackers gained access to the server through which software updates are distributed to the modems and used it to deploy malware that overwrote the devices' memory. Among those affected was the remote monitoring of 5,800 wind turbines from the manufacturer Enercon, with a combined 11 gigawatts. The installations continued to feed in but could no longer be remotely monitored or reset. The attack was aimed at Ukraine; the German installations were collateral damage, precisely the scenario that the FIS also considers possible for Switzerland (see chapter *2.5*).[38]

5.4.2 Privileged Remote Maintenance Access

Independently of the cloud, most manufacturers retain privileged access to their device fleet, for example via maintenance accounts or remote access. This is not an isolated flaw but a design principle: a single compromised or reconstructible access method potentially affects the entire fleet, and such access cannot be remedied like an ordinary vulnerability. Also affected are large installations that are not connected to a manufacturer cloud but have their own remotely reachable control and maintenance interfaces. The case of the Deye inverters showed in November 2024 how real this possibility is: in the course of a distribution dispute, the manufacturer deliberately switched off numerous of its own devices that had been sold without authorization in several countries, entirely without a vulnerability.[39]

The same pattern extends beyond the manufacturer: installation companies, service providers,

[37] Reuters, reporting on undocumented communication modules, May 2025: https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/
[38] SentinelOne, "AcidRain – A Modem Wiper Rains Down on Europe," 31 March 2022: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
[39] heise online, Reporting on remotely deactivatable Deye inverters, 2024: https://www.heise.de/news/Photovoltaik-Deaktivierte-Deye-und-Sol-Ark-Wechselrichter-in-den-USA-10183706.html

and aggregators, too, often have remote access to all the installations they look after, without any cybersecurity requirements applying to them. A targeted attack in April 2022 on the Bremen-based maintenance service provider Deutsche Windtechnik, which looks after more than 7,600 wind turbines, showed how far this reaches: the company responded by switching off all remote data-monitoring connections, so that remote monitoring was unavailable for one to two days. The installations themselves were not affected.[40] Neither a manufacturer nor an operator was attacked, but the service provider in between.

5.4.3 Insecure Local Control Protocols as a Design Feature

The local control of many inverters relies on widely used industrial protocols that provide no authentication. This is not a flaw of individual devices but the standard of an entire device category. It is exacerbated by the shift of this control from physically access-restricted connections (RS485) to networked interfaces (Ethernet, Wi-Fi), because this makes every device on the same network a possible sender of control commands.

5.4.4 Market Concentration as a Concentration Risk

The concentration described in the chapter "The Ecosystem of a Photovoltaic System" acts in security terms as a "single point of failure": the larger a manufacturer's share, the more devices a single finding reaches. An assessment from the Dutch cybersecurity firm Secura shows how concrete this risk is: in the Netherlands, two manufacturers (Huawei and Sungrow) each individually have such a large market share that an attack on the systems of a single one of them would suffice to reach the order of magnitude needed for a grid effect. Across Europe, according to Secura, several manufacturers would exceed this threshold.[41]

5.4.5 A False Sense of Security Based on Location and Origin

Various manufacturers advertise that their cloud is operated in European data centers and managed by European organizations. The hosting location alone, however, says little about actual control over the device, among other reasons because firmware and software come from the manufacturer and are not developed at the hosting location. The NTC's own tests did confirm that the observed data traffic went to EU endpoints. Exclusively European control or data storage cannot be inferred from this. Nor does the origin of the device solve the problem: devices from European providers, too, often contain chips or software components from third countries or are manufactured there.

[40] heise online, Cyberattack: Remote monitoring of wind turbines paralyzed, 27 April 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

6 Impact on Grid Stability

6.1 Basic Principle: The Balance of Generation and Consumption

An alternating-current grid must be operated continuously close to its nominal frequency (50 Hz in Europe). This presupposes a real-time balance between generation and consumption. If the frequency deviates, tiered reserves take effect in the European interconnected grid: a primary reserve that kicks in within seconds (around 3,000 MW), and a secondary and a tertiary reserve with longer lead times.[42] A sudden power jump beyond the so-called reference incident of 3,000 MW can no longer be absorbed by the primary reserve alone. At 49 Hz, a regulatorily prescribed load shedding takes place.[43]

An aggravating structural factor is the decline in grid inertia. Conventional power plants stabilize the frequency via the rotating masses of their generators, whereas inverter-based generation does not provide this inertia on its own.[44] Modern inverters are increasingly expected to compensate for this via grid-forming functions. This aspect is taken up further below under the mitigating factors.

6.2 Real-World Evidence: The Grid Can Destabilize Even Without a Cyberattack

The Iberian blackout of 28 April 2025 showed how fragile a system can be under high inverter-based generation, and that without any malicious involvement. At times, a very high share of the electricity came from renewable sources. A chain of problems with voltage and reactive power (a grid-supporting quantity that helps determine the voltage in the grid, explained in more detail below under impact type B) led to rapidly rising voltage, cascading disconnections of generation, and finally the complete system collapse in Spain and Portugal. The causal assessment by ENTSO-E, the association of European transmission system operators, matters here for proportionality: what was decisive was not "too much renewable generation", but gaps in voltage and reactive-power control. [45]

The simultaneous reaction of many identically configured installations is not a thought experiment. In Germany, a 2005 guideline prescribed that photovoltaic systems disconnect from the grid immediately at a grid frequency of 50.2 Hz. With the expansion, this became a system risk: on reaching this frequency, installations with several gigawatts of output would have disconnected all at once. The 2012 System Stability Ordinance therefore obliged grid operators to retrofit around 300,000 existing installations with about one million inverters, so that disconnection occurs in a staggered rather than simultaneous manner.[46]

6.3 Three Attack Types of a Compromised Inverter

The widespread notion that an attack consists of mass "switching on and off" falls short. The security researcher Ruben Santamarta distinguishes three types of cyber-physical attacks of increasing complexity.[47]

---

[42] Goerke et al., Karlsruhe Institute of Technology, "Who Controls Your Power Grid? On the Impact of Misdirected Distributed Energy Resources on Grid Stability", 2024: https://publikationen.bibliothek.kit.edu/1000173186
[43] Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration, Article 15 (automatic under-frequency load shedding) and Annex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R2196
[44] ENTSO-E, "Frequency stability in long-term scenarios", study on the decline of system inertia in the Continental Europe synchronous area, December 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, 50.2 Hz problem, https://www.bdew.de/energie/systemstabilitaetsverordnung/502-hertz-problem/
[47] Santamarta, "Cyber-Physical Attacks on Solar Inverters", May 2026: https://www.reversemode.com/2026/05/a-practical-analysis-of-cyber-physical.html

6.3.1 Type A: Active Power and Frequency (Switching On and Off)

By coordinated disconnection or connection of many installations, the balance between generation and consumption is disturbed and the frequency shifted. This can be achieved via direct disconnection commands, via manipulation of the protective function that automatically disconnects an installation from the grid in the event of a grid outage (anti-islanding), or via altered specifications for the voltage at which an installation should stay connected or disconnect (the so-called ride-through curves HVRT and LVRT, "High/Low Voltage Ride-Through"). An attack that repeats the manipulation in time with the grid's own regulation, building up the oscillation, much like pushing a swing at the right rhythm, is particularly effective.

A phenomenon from market operation shows that simultaneity is grid-effective even without an attack. When many installations adjust their feed-in abruptly at the change of the market interval, frequency deviations arise at each hourly or quarter-hourly change, known as "deterministic frequency deviations." Swissgrid therefore intends to prescribe that photovoltaic systems, too, make such planned changes via a ramp. An attacker who switches many installations simultaneously uses the same effect - only deliberately and without a ramp.[48]

6.3.2 Type B: Reactive Power and Voltage

This is, in Santamarta's assessment, the most effective route to local outages. Inverters support the grid not only with active power but also with reactive power, which co-determines the voltage in the grid. Characteristic curves such as the volt-var curve define how an inverter should react: if the voltage rises, the inverter absorbs reactive power and lowers the voltage again. This stabilizes the grid. An attack reverses this reaction. A manipulated characteristic curve forces the inverter to feed in additional reactive power when the voltage is already high, thereby driving the voltage up further. Even a few installations can then push the local voltage beyond the permissible limits, whereupon protective devices of neighboring installations and substations switch off and can trigger a cascade. As for realism: via altered control logic, for example after a compromise of the firmware, such a reversal is plausible. The attack requires neither complex malware nor large scale. Grid simulations reach the same conclusion, carried out by DNV on behalf of SolarPower Europe using the grid models of ENTSO-E:[49] if large capacities are switched simultaneously between inductive and capacitive reactive power, rapid voltage jumps arise that trigger protective devices of neighboring generation installations and substations and can set off a cascade. At the same time, the study notes that it remains unclear how quickly and how far the existing voltage-maintenance mechanisms would counteract this.

6.3.3 Type C: Converter-Driven Instability (Oscillations)

The targeted excitation of the grid's own oscillations, up to forced oscillations, is the most complex vector. It is considered - also by Santamarta's own assessment - currently unrealistic, particularly as a coordinated attack via a multitude of small, heterogeneous home inverters. As a phenomenon, it is nonetheless real. During the Iberian blackout, a forced oscillation from a single large photovoltaic power plant (according to Santamarta's analysis, the Núñez de Balboa installation), not from distributed small installations, excited a supraregional oscillation.[50]

6.3.4 Assessment: The Most Dangerous Vector Is Not the Most Complex

What is surprising here is that the most dangerous vector is not the most complex. Against pure generation losses, the grid is comparatively robust. The voltage-driven attack via reactive power, by contrast, requires only small scale and low complexity, which makes the threat more plausible

[48] Swissgrid AG, white paper "System-Compatible Integration of Photovoltaics", March 2026: https://www.swissgrid.ch/de/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
[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/

- as the Iberian blackout shows at precisely this level (see chapter *6.2*).

6.4 The Cyber Scenario: Coordinated Load and Generation Manipulation

The idea that compromised, internet-connected devices could be combined into a grid-effective network has been established in research for around a decade (under the terms "load-altering" and MaDIoT, "Manipulation of Demand via IoT"). The work ranges from early models via Dabrowski et al.[51] (2017) and Soltan et al.[52] (2018) to Goerke et al.[53] (2024), which quantify in detail how many installations of each type would be needed for a grid effect in the European interconnected grid. The first photovoltaics-specific formulation of this basic idea comes from the "Horus scenario"[54] by Willem Westerhof, published in August 2017 and based on a disclosure to the manufacturer in December 2016.

Inverters are especially suited to such attacks because, as real-time systems, they track the grid frequency precisely and can therefore execute an attack very accurately.

Beyond pure grid destabilization, a second damage path should be mentioned. Attackers with far-reaching access can permanently disable devices via malicious firmware, so that they have to be replaced or reflashed on site. Extortion is also conceivable ("ransomware on inverters"). Such destructive effects would have considerably longer-term consequences than a temporary grid disturbance.

6.5 Order of Magnitude (Illustrative Rough Calculation)

For context - expressly not as a standalone blackout forecast - the order of magnitude can be derived from the literature. According to Dabrowski et al., under conditions favorable to an attacker, control over around 4,500 MW suffices to push the frequency in the European interconnected grid below the load-shedding threshold of 49 Hz - one and a half times the reference incident. The value applies to an attack that modulates the power in time with grid regulation and thereby builds up the deviation; a one-off power jump would have to amount to around 6,000 MW under the same grid conditions. The threshold denotes a power imbalance that can be reached from the consumption side as well as the generation side: Dabrowski derives it from the load side; Goerke et al. and dos Santos et al. transfer it to photovoltaics. For photovoltaics, this specifically means a sunny day with low load, such as on a summer weekend or public holiday.

For context: 4,500 MW corresponds to just under half of the 9.5 GW installed in Switzerland. The threshold is thus a European one, not a Swiss one. On a European scale, conversely, a small share suffices: measured against the roughly 406 GW installed in the EU at the end of 2025, 4,500 MW is a good one percent, and even the conservative variant of 6,000 MW remains below two percent; this share decreases with each additional year of expansion.[55] An independent simulation arrives at a similar order of magnitude: for the European grid, DNV cites a targeted compromise of 3 GW as the threshold above which significant impacts are possible.[56]

For Switzerland, this brings no reassurance but a different question: how strongly the Swiss installed base is concentrated at individual control points. Because a good half of the market share falls to a single manufacturer (see chapter *3.6*), a single manufacturer cloud already reaches a considerable and growing part of the Swiss installed base. A similar concentration

[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., Karlsruhe Institute of Technology, "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/
[55] SolarPower Europe, "EU Solar Market Outlook 2025-2030", December 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

arises through aggregators and virtual power plants (see chapter 3.4). For a Europe-wide coordinated attack, it is not the national total that is decisive, but the number of platforms through which it is reachable.

A robust, standalone calculation for the Swiss grid lies outside the scope of the investigation. What remains robust is the core statement: even a share of under two percent of the European inverter base is arithmetically sufficient to trigger relevant grid effects, though the concrete figure depends strongly on device distribution and grid state. The reactive-power vector (type B), according to Santamarta, requires considerably less controlled power, but acts locally rather than supraregionally.

6.6 Real-World Precedent: Poland, 29 December 2025

A coordinated cyberattack struck more than 30 wind and solar farms, as well as a combined heat and power plant and an industrial company. At the renewable installations, communication with the distribution system operators was lost. Electricity generation itself was not impaired, and the transmission system operator saw the stability of the Polish system as not endangered at any point. Generation continued, but was decoupled from the grid's requirements. The Polish transmission system operator noted that irregularities in the operation of smaller generators had been observed and remedied, but that the system had been able to be balanced with the available means. The malware used was destructive (a wiper). The report by the responsible authority compares the attacks to deliberate arson.

The significance of the incident lies not in a narrowly averted blackout, but in the fact that a capable actor demonstrably gained access to the control level (operational technology, OT) of numerous renewable-energy parks and showed intent to destroy. With this, the scenario loses its purely theoretical character. On 13 July 2026, the United Kingdom and the EU officially attributed the attack to the Russian intelligence service FSB (Center 16) and imposed a joint sanctions package. According to British assessment, the attack could have cut around 500,000 people off from the electricity supply in winter.[57] The technical documentation is provided by CERT Polska.[58]

6.7 Assessment by Independent Experts

Outside state bodies, too, the danger is taken seriously. The Dutch DIVD (see chapter 5) examines inverters, charging stations, smart meters, and increasingly energy management systems in its own program. In July 2026, following the attack in Poland, experts publicly warned that in the worst-case scenario a successful attack could lead to widespread power outages lasting for days.[59]

6.8 Mitigating Factors

The grid is not defenseless. Tiered reserves, protection systems, and the still-present inertia absorb many disturbances, and not every manipulation cascades. The heterogeneity of the fleet, with its many manufacturers, firmware versions, and configurations, additionally makes a single, cross-manufacturer exploit difficult. Within a dominant manufacturer cloud, however, the concentration remains real, and in Switzerland it is pronounced (see chapter 3).

At the same time, grid inertia declines as conventional power plants are phased out. Grid-forming inverters are meant to compensate for this. If, however, precisely these inverters are the target of an attack, then along with generation the stabilizing component is lost as well. Overall, the basic level of protection is likely to rise through ongoing updates by manufacturers and current and

[57] OFSI/GOV.UK, sanctions notice of 13 July 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/
[59] Dutch Institute for Vulnerability Disclosure (DIVD), public warning on the vulnerability of the power grid (Chris van 't Hof), July 2026: https://www.nu.nl/klimaat/6403086/stroomnet-kwetsbaar-voor-cyberaanval-geen-kwestie-van-of-maar-wanneer.html

forthcoming EU product regulation (RED, CRA). The structural and geopolitical risks, however, are not eliminated by this.

7 International Comparison and Regulation

The cybersecurity of photovoltaic systems has moved onto the regulatory agenda internationally over the past roughly two years. This chapter provides an overview of the measures taken by other states and the EU and situates Switzerland within them. The assessments presented come from the respective authorities and governments. They are explained here, not evaluated.

7.1 A Common Pattern

Strikingly, the initiatives of various countries target the same two points: the possibility of remote control via manufacturer clouds, and the strong concentration of the market on a few, predominantly Chinese manufacturers. Nine of the ten largest inverter manufacturers worldwide were from China in 2024; Huawei and Sungrow alone accounted for around 55 percent of global shipments.[60] This situation is classified as a strategic risk by several national security authorities.

The opposing view is also part of the picture. In May 2026, the Chinese Ministry of Commerce said that classifying China as a high-risk state was made without concrete evidence and a stigmatization of Chinese products.[61] The Chinese Chamber of Commerce to the EU, for its part, rejected the accusation that China could use energy as a means of pressure, and pointed to the contribution of Chinese companies to the European energy transition.[62]

7.2 Overview of the Instruments Used

The initiatives can be ordered by their depth of intervention, from mere informing to the denial of grid connection.

- **Warning:** Estonia and the Czech Republic rely on official warnings. The Estonian foreign intelligence service warned[63] explicitly against Chinese inverters in February 2024 and noted that the more Estonia relies on solar energy, the greater the effect of a possible manipulation would be. The intelligence chief spoke of a risk of extortion.[64] The Czech cyber authority NUKIB warned on 3 September 2025 against data transfer to, and remote administration from, China for critical infrastructure, and named photovoltaic inverters as one of several examples. This is a warning, not a ban: regulated entities must take it into account in their risk analysis.[65] In June 2026, in a joint advisory from the Office for the Protection of the Constitution and the BSI, Germany warned against the reconnaissance of unprotected, internet-connected photovoltaic systems by Russian actors.[66]
- **Recommending:** Australia addressed the topic early. In August 2023, the Cyber Security Cooperative Research Centre published the report "Power Out? Solar Inverters and the Silent Cyber Threat" and recommended three measures: cyber risk assessments for all inverters sold, mandatory cybersecurity ratings, and the recall or remediation of devices with serious vulnerabilities.[67] Independently of this, a general product requirement for connected consumer devices has applied in Australia since 4 March 2026: the Cyber Security Act 2024

[60] EUISS, Caspar Hobhouse, "The dragon in the grid: Limiting China's influence in Europe's energy system," January 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," May 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 May 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," February 2024: https://raport.valisluureamet.ee/2024/en/6-china/6-3-the-advance-of-chinese-technology/
[64] Reuters, reporting on undocumented communication modules, May 2025: https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/
[65] Czech cyber authority NÚKIB, September 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] Federal Office for the Protection of the Constitution (BfV) and Federal Office for Information Security (BSI), "Joint Security Advisory: Reconnaissance of Poorly Protected PV Installations by State Cyber Actors", 3 June 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html
[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/

and the Security Standards for Smart Devices Rules based on it require, among other things, unique passwords, a point of contact for vulnerabilities, and a statement of the support period.[68]

- **Testing and disclosing:** The Netherlands came to oversight via research. Between 2021 and 2023, the Rijksinspectie Digitale Infrastructuur tested nine commercially available inverters from eight brands against the ETSI EN 303 645 standard, a European baseline standard that sets only minimum requirements for connected consumer devices and is expressly intended to protect only against elementary attacks on basic design weaknesses, such as manufacturer-wide identical default passwords. Not a single device met all the requirements. The authority warned that devices could be switched off remotely or misused for attacks.[69] Independently of this, the disclosures described in the chapter "Findings and Risks" triggered parliamentary inquiries in the Netherlands.
- **Commenting on one's own legislative project:** Germany shows the conflict of objectives between grid-serving control and cybersecurity particularly clearly (see chapter *7.3.1*).
- **Tying funding:** The European Union excludes inverters from high-risk suppliers from EU funding and, in parallel, raises the basic level of protection of connected products via RED and CRA (see chapter *7.3.2*).
- **Tying market access to testing:** Taiwan makes the cybersecurity certificate part of type approval (see chapter *7.3.3*).
- **Tying grid connection to security:** Lithuania prohibits manufacturers from threat states from remotely accessing installations over 100 kW and allows grid operators to disconnect non-compliant installations (see chapter *7.3.4*).
- **Self-regulation:** In 2025, the European industry association SolarPower Europe presented an analysis of photovoltaics' cyber risks to grid stability, prepared by the testing company DNV. It contains a risk assessment, grid simulations, and a catalog of minimum requirements for manufacturers, operators, and policymakers. The industry has thus taken up the topic itself.[70]

7.3 Four Approaches in Detail

The four approaches last mentioned are presented in more detail below, because they are directly applicable to the Swiss discussion.

7.3.1 Germany: The Conflict of Objectives Between Grid Control and Cybersecurity

Germany shows the conflict of objectives between grid-serving control and cybersecurity particularly clearly. Under Section 14a of the Energy Industry Act (EnWG), since 1 January 2024 grid operators may, in the event of an impending local grid overload, temporarily throttle the power drawn from the grid by controllable consumption devices such as heat pumps, wallboxes, and battery storage generally to no less than 4.2 kW. In return, the grid fee is reduced.[71]

When the so-called Solar Peak Act (Solarspitzengesetz) also provided for the curtailment of photovoltaic systems via the existing inverters, the Federal Office for Information Security (BSI) expressed considerable concerns. It viewed realizing grid-serving remote control of inverters via the manufacturers very critically. That manufacturers - possibly via a cloud operated abroad - would have direct access to such a large number of devices in the European interconnected grid carried a considerable potential for harm. In addition to the manufacturer itself, security vulnerabilities could also open up unauthorized access to third parties. As an alternative, the BSI proposed operating such installations as locally as possible and realizing grid-serving control via

[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," May 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
[71] Federal Network Agency (Bundesnetzagentur), "Integration of Controllable Consumption Devices (Section 14a EnWG)": https://www.bundesnetzagentur.de/DE/Vportal/Energie/SteuerbareVBE/artikel.html

smart metering systems rather than via manufacturer clouds.[72] Expert commentators countered that remotely controllable inverters can be switched off via their manufacturer backend anyway, and that the access feared by the BSI has therefore long existed even without the law, given the market dominance of Chinese manufacturers. [73]

It is also notable for Switzerland that Germany has the same regulatory gap. The BSI critical-infrastructure ordinance (BSI-KritisV)[74] applies only at or above 104 MW of installation output; smaller photovoltaic systems do not fall under the rules for critical infrastructure.

7.3.2 European Union

The clearest step so far is the "Economic Security Doctrine" published on 3 December 2025, which explicitly names dependence on solar inverters as a high-risk dependency and justifies this with supplier concentration, cyber-manipulation risks, and access to grid-relevant operating data. Among its instruments, it cites coordinated cyber risk assessments and certification under the Cyber Resilience Act. The manufacturers' association ESMC additionally demands that member states be able to exclude high-risk hardware from grid connection.[75]

In spring 2026, a concrete measure followed: the Commission is restricting EU funding - including from the European Investment Bank - for solar, wind, and storage projects that use inverters from high-risk suppliers from China, Russia, Iran, or North Korea. Providers from trustworthy partner countries remain eligible for funding.[76] Important for context: this is a funding restriction, not a market ban. A further step toward permanent market restrictions is laid out in the proposed revision of the Cybersecurity Act (CSA2). A structural gap remains: the NIS2 Directive, fundamental to many of these measures, applies primarily to medium-sized and larger organizations and generally does not cover smaller generation installations such as private rooftop photovoltaics.

Independently of this, the EU is raising the basic level of protection of connected products. The cybersecurity requirements of the Radio Equipment Directive (RED) have applied since 1 August 2025 and require network protection, protection of personal data, and fraud prevention for internet-capable radio devices. From 11 December 2027, the Cyber Resilience Act will replace them; reporting obligations for actively exploited vulnerabilities and serious incidents already apply from 11 September 2026. The CRA is technology-neutral and lifecycle-oriented and requires, among other things, secure update mechanisms and a structured approach to vulnerabilities over the entire product lifetime. Because these rules apply to market access and the products concerned are largely the same as in Switzerland, they are likely to raise the security level here as well.

7.3.3 Taiwan: Product-Related Testing With Considerable Depth

Taiwan has one of the few product-related testing regimes for solar inverters, and the most detailed one publicly documented. In October 2025, the testing authority BSMI published a technical test specification and, with a revision of type approval in May 2026, made the cybersecurity certificates binding. For solar inverters - alongside charging infrastructure, power converters, and stationary lithium storage - they will become a mandatory part of type approval from 1 January 2028, and the simplified route of the declaration of conformity will then no longer

[72] pv magazine Germany, Petra Hannen, "Solar Peak Act: BSI warns of Chinese manufacturers' access to German photovoltaic systems," January 2025: https://www.pv-magazine.de/2025/01/20/solarspitzen-gesetz-bsi-warnt-vor-zugriff-chinesischer-hersteller-auf-deutsche-Photovoltaikanlagen/
[73] zfk, Julian Korb, "Uproar over surveillance in Chinese inverters": https://www.zfk.de/energie/strom/wirbel-um-ueberwachung-in-chinesischen-wechselrichtern
[74] BSI-KritisV, Annex 1, Part 3 No. 1.1.1: https://www.gesetze-im-internet.de/bsi-kritisv/anhang_1.html
[75] pv magazine, EU security doctrine highlights high-risk dependency on Chinese solar inverters, 16 December 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 April 2026: https://www.pv-magazine.com/2026/04/23/eu-moves-to-restrict-funding-for-projects-using-inverters-from-high-risk-suppliers/

be available.[77]

Two units are tested separately, the inverter itself and the monitoring unit. Four security dimensions apply to the monitoring unit - namely physical, system, communication, and authentication security - and three to the inverter, based on international standards such as IEC 62443-4-2. The testing depth is considerable. Submission of the source code for a static analysis is required, whereby vulnerabilities with a severity score (CVSS) of 7 or higher lead to non-conformity absent a justified countermeasure. Added to this is an integrity check of the firmware update, in which the inverter must reject deliberately manipulated firmware or fall back into a safe state. For the monitoring unit, a traffic analysis over at least 24 hours is also provided for, in which the actual destination addresses are compared with the servers declared by the manufacturer.

Two limits are analytically instructive. First, this is a type test at the time of certification: the specification does require the device to detect manipulated firmware, but does not prescribe a specific cryptographic method for this, and it does not provide for a specific re-check upon later firmware changes. Second, it expressly excludes the information security of the management system, that is, the cloud layer, from the testing scope; the only thing included is whether it can manage user accounts and update firmware remotely. This testing regime thus omits precisely the layer that, according to the findings of this analysis, has the greatest leverage. The lesson for Switzerland and the EU is correspondingly twofold: a product-related testing regime is possible and sensible, but it remains incomplete as long as it captures neither a lifecycle component nor the central control layer.

7.3.4 Lithuania: Security as a Condition for Grid Connection

Lithuania has gone furthest. With Article 73[3], adopted on 12 November 2024, manufacturers from states that are considered a threat under the national security strategy - among them China - are prohibited from remotely accessing the control systems of solar, wind, and storage installations over 100 kW, specifically from remotely changing power parameters and switching them on and off. Required are, among other things, multi-factor authentication, secure communication, supply-chain controls, and an audit. For new installations, the rule has applied since 1 May 2025; existing installations had to comply by 1 June 2026. Conformity is a precondition for grid connection, and since the end of the transition period grid operators may also disconnect non-compliant installations from the grid. [78] The European Association of Solar Manufacturers supported the rule.[79]

What the law does not require is worth noting. Chinese devices are not banned, and already-installed systems do not have to be replaced. Their operators must, however, implement additional protective measures.

The Lithuanian experience also shows where the implementation burden lies. For new installations, conformity is comparatively cheap to achieve, because it can be factored in from the outset during procurement and connection. Costly and time-consuming is the retrofitting of the installed base, where implementation backlogs formed. For Switzerland, it follows that such an approach is most effective for new installations, and that the installed base remains the larger open flank for years.

7.4 Regulation in Switzerland

In Switzerland, the ICT minimum standard for the electricity sector has been binding since 1 July 2024. The revised Electricity Supply Ordinance (StromVV, Annex 1a) prescribes protection levels

[77] Taiwan, Bureau of Standards, Metrology and Inspection (BSMI), revision of the type-approval rules of May 2026: https://www.bsmi.gov.tw/wSite/public/Attachment/f1761016956224.pdf; summary: 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, June 2026: https://www.pv-magazine.com/2026/06/05/lithuanias-grid-operators-can-now-disconnect-solar-plants-without-cybersecurity-measures/
[79] pv magazine, Lithuania bans remote Chinese access to solar, wind, storage devices, 18 November 2024: https://www.pv-magazine.com/2024/11/18/lithuania-bans-remote-chinese-access-to-solar-wind-storage-devices/

and maturity levels, whose fulfillment the Federal Electricity Commission (ElCom) can review. The classification is based on capability: protection level A applies, for example, to grid operators from 450 GWh per year, protection level B to grid operators from 112 GWh per year, as well as to generators, storage operators, and service providers, provided they operate installations with a total output of at least 100 MW and can control them via a single system.[80] In addition, a reporting obligation has applied since 1 April 2025: cyberattacks on critical infrastructure must be reported within 24 hours to the National Cyber Security Centre (NCSC).

The decisive gap concerns small-scale installations and thus practically all Swiss photovoltaic systems. Generators are subject to the standard only from 100 MW of controllable total output via a single system. The installed base of small installations, distributed across hundreds of thousands of operators, is not covered by any single obligated entity. Current and forthcoming EU product regulation is likely to raise the device level. It does not, however, address the structural and geopolitical questions - market concentration and remote controllability.

That this gap is recognized is shown by a paper from the national grid company. In its white paper "System-Compatible Integration of Photovoltaics"[81] of March 2026, Swissgrid states that Switzerland's electricity supply is already today distributed across hundreds of thousands of decentralized installations. This, it argues, requires a defined level of protection against cyberattacks for these installations and their control as well. Binding minimum requirements are called for, for photovoltaic systems, which would moreover have to be effectively implemented and monitored for existing installations too. The recommendation is addressed to legislators and the Federal Inspectorate for Heavy Current Installations (ESTI). The need for action described in this report is thus shared by the very body responsible for the stability of the overall system.

It is worth noting what the ICT minimum standard achieves and what it does not. It is aimed at organizations and requires them to identify risks, implement protective measures, detect incidents, and respond to them. It cannot sensibly be applied to a private installation operated by a private individual with no dedicated IT function. The gap for small-scale installations therefore cannot be closed by lowering the output threshold. Other instruments are effective here: requirements on the product, conditions for grid connection, or coverage of the entity that concentrates access to many installations.

7.5 Assessment for Switzerland

The international trend is clear: several states increasingly treat distributed photovoltaics as a matter of critical infrastructure and not merely of climate policy. The instruments used range from warnings (Czech Republic, Estonia, Germany) and official comments on legislative projects (Germany), through supervisory market testing (Netherlands) and product-related testing regimes (Taiwan), to funding and procurement criteria (EU) and binding grid connection conditions (Lithuania).

On the enforcement side, a further instrument is added. With the attribution of the attack on the Polish power grid to the Russian intelligence service FSB and the joint sanctions package of 13 July 2026 (see chapter *6.6*), the EU and the United Kingdom show that such attribution and sanctions are used to complement technical and regulatory safeguards.[82]

Swiss regulation covers grid operators, large generators and storage operators, and service providers with comparable control reach. Binding cybersecurity requirements for the operation of the individual small-scale installation are lacking. The industry recommendation NA/EEA-NE7 has, since 2025, contained a chapter on remote access and firmware updates, but there confines itself to password protection and updates. Which of these approaches may be suitable for Switzerland is taken up in chapter *8 Recommendations* .

[80] National Cyber Security Centre (NCSC), ICT minimum standards: https://www.bacs.admin.ch/en/ict-minimum-standard
[81] Swissgrid AG, white paper "System-Compatible Integration of Photovoltaics", March 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html
[82] OFSI/GOV.UK, sanctions notice of 13 July 2026: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions

7.6 Regulatory Outlook

The basic level of protection of connected products is rising, but the structural questions remain untouched by this.

On the product side, the cybersecurity requirements of the Radio Equipment Directive (RED) have applied since August 2025; in Switzerland they are implemented via the Ordinance on Telecommunications Installations, with the Federal Office of Communications (OFCOM) as the market surveillance authority. They become testable through the EN 18031 series of standards, which makes access control, secure update mechanisms, and the handling of credentials concrete. From December 2027, the Cyber Resilience Act replaces the RED requirements and extends them to all products with digital elements, that is, also to devices without a radio interface. In parallel, testing regimes are emerging specifically for this device class: the Taiwanese type approval, UL 2941, and the certification of the SunSpec Alliance (see chapter *7.3.3* and *8.5.3*).

What these frameworks achieve is a higher baseline; they make unauthorized access by third parties more difficult. They address, however, neither the market concentration nor the remote controllability by the manufacturer itself. Manufacturers and operators should therefore implement the recommendations in the next chapter not only when future obligations take effect, but already now.

8 Recommendations

The following recommendations arise from the central finding of this report: the decisive risk is structural in nature, that is, a question of cloud dependence, market concentration, and control protocols left unprotected by design, and less a question of deficient individual devices. They are organized by addressee and deliberately kept at a high level. This report does not argue against photovoltaics. The recommendations are intended to enable its secure further expansion. It should be said at the outset that there is no single, simple, and complete solution: all approaches have drawbacks, and residual risks remain.

8.1 For Operators of Small-Scale Installations

Installation is not a one-off task: installations must be configured correctly and updated regularly, and someone must be responsible in the event of an incident. Those who cannot perform these tasks themselves should assign them contractually to the installation company or a third party. An offer to operate the installation is not in itself proof of competence. A provider's suitability is shown by whether it addresses the following points on its own initiative and guarantees them in writing.

Concrete points for the individual installation:

- Change default passwords immediately and activate automatic firmware updates, or install updates promptly.
- Do not make any component of the installation reachable from the internet, and in particular do not set up port forwarding.
- Deliberately decide whether the installation should be permanently connected to the manufacturer cloud. This connection is not technically mandatory, but is the default in practice, and is rarely questioned. On many devices, production can also be read locally without the cloud. Such operation without a cloud connection reduces the attack surface but comes at the cost of convenience, such as easy monitoring via the app. It should also be considered that without a connection, no automatic firmware updates are received, and known vulnerabilities may remain unpatched. Where the device allows it, a control lock is therefore often the better compromise: it still permits updates but no active remote control (see chapter *8.4.2*). Unneeded remote access should be deactivated.
- Choose an energy management system by verifiable characteristics rather than by the range of features: local operability without a permanent cloud connection, a guaranteed update and support period, and, where possible, an independent assessment. An EMS concentrates control over all connected devices in a single component, which means a single vulnerability can affect the entire installation.
- At handover, have it confirmed that individual passwords are set and that the installation is not reachable from the internet.
- Specify contractually who ensures that firmware updates are installed and who is responsible in the event of an incident.

8.2 For Operators of Larger Installations

For grid operators and operators of large commercial and industrial installations, the proven principles from OT and IoT environments apply:

- **Inventory the installed base:** record and keep up to date the inverters, energy management systems, and their interfaces, including all remote accesses (manufacturer, installer, service provider, aggregator). What is not known cannot be secured.
- **Not reachable from the internet:** inverters and energy management systems, along with their management interfaces, do not belong on the internet. If remote access is necessary, it should take place via secured channels, such as a virtual private network (VPN).
- **Network segmentation:** separate photovoltaics, energy management, and charging infrastructure individually from the rest of the network, because combined access to electricity feed-in and consumption is especially effective (see chapter *2.6*).

- **Separation of local control from the internet-facing network:** if Modbus TCP is used, the inverter is often connected to the same network segment as an internet-connected energy management system. An ordinary network firewall typically only protects against access from outside, but not against an attacker already on the local network, for example via a compromised IoT device (see chapter *5.3.3).* A more robust option is therefore an energy management system with two physically separate network ports, one for the local part (inverter, without internet) and one for the internet-facing network. Deliberately using a different physical medium (such as RS485 instead of end-to-end Ethernet) reduces the risk that a device inadvertently becomes reachable from the internet.
- **Treat the energy management system as a single point of control**: it controls all connected devices, and its reach thus extends beyond that of a single inverter. If it becomes the enforcement point of the control lock, the requirements from chapter 8.4.2 apply to this system.
- **Specify manufacturer access contractually:** set out in writing the scope, purpose, and duration of privileged remote access, and provide for a right of revocation (see chapter *5.4.2*).
- **Configure central controllability deliberately:** where the installation does not need manufacturer-side remote control, this should be restricted, and control of grid-relevant functions reserved for the regulated entity (see chapter *3.4* and *8.4.2*).
- **Monitoring and logging**: continuously monitor inverters, energy management systems, and their remote accesses, and centrally collect and evaluate the device-side logs.
- **Operate an update process:** for one's own fleet, check systematically whether new, particularly security-relevant, firmware is available, and install it promptly after a risk assessment.
- **Prepare for the event of an incident:** determine in advance who is responsible in the event of a security incident, including contacts at the manufacturer or aggregator and the cybersecurity authorities. Installations should also be able to disconnect in an orderly manner from the affected control channel, without simultaneously shutting down in an uncontrolled way (see chapter *8.4.2*).
- **Security in procurement:** include security requirements in tenders and make cybersecurity a procurement criterion.
- **Apply the ICT minimum standard voluntarily:** also apply it to systems that do not fall within its mandatory scope (see chapter *7.4).*

8.3 For Installation Companies

In practice, installation companies determine the security level of the individual installation. What can later be attacked is determined at commissioning: whoever sets the credentials, configures the interfaces, and connects the installation to the grid determines whether a default password remains in effect, whether the inverter is reachable from the internet, and whether the local control interface is left unprotected. As a rule, these decisions are made not by the operator but by the installation company. The BSI considers it likely that installation and setup are frequently carried out by specialist solar firms with little expertise in IT security.[83] It is therefore all the more important that a few principles be followed during commissioning:

- Set individual credentials for each installation and do not use passwords that are uniform across the customer base. A fleet-wide installer code shifts the same risk this report describes at manufacturers down to the level of the installation company (see chapter *5.4.2*).
- Do not make any component of the installation reachable from the internet, and in particular do not set up port forwarding.
- Deactivate interfaces that are not needed, such as an unused Wi-Fi hotspot or an open local control interface (see chapter *5.3.2*).
- Separate the installation from the rest of the home or company network, so that a compromised device on the same network cannot readily reach the inverter (see chapter

[83] Federal Office for the Protection of the Constitution (BfV) and Federal Office for Information Security (BSI), "Joint Security Advisory: Reconnaissance of Poorly Protected PV Installations by State Cyber Actors", 3 June 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

5.3.3).

- Handover includes documentation of the chosen configuration and a clear agreement on who will ensure that firmware updates are installed in the future and who is responsible for incident response.
- In procurement, favor products that also function without a cloud connection, offer protected local interfaces, and come with a guaranteed update period.

Putting these points into practice requires the necessary expertise within the installation company. Cybersecurity fundamentals should therefore be an integral part of initial and continuing training.

8.4 For Manufacturers

8.4.1 Basic Requirements

Responsibility for the basic security level lies with the manufacturers. The most important requirements are:

- **Security as a design principle: build security in from the start rather than adding it afterward** ("Security by Design").
- **Secure firmware updates:** cryptographically signed, with protection against rolling back to older, vulnerable versions.
- **Secure maintenance and service access:** the credentials must be device-specific and non-reconstructible, so that a single compromised access method does not affect the entire fleet. Privileged remote access should also be time-limited and revocable by the responsible entity.
- **Logging of security-relevant events:** logins, changes to grid-relevant parameters, firmware changes, and access via maintenance accounts must be logged on the device and retrievable.
- **Secured cloud interfaces:** end-to-end authentication and authorization in all APIs.
- **Handling of reported vulnerabilities:** a structured responsible disclosure process with a reachable point of contact and remediation within a reasonable period.
- **Safe state at end of support:** the device must remain fully functional in local operation even after manufacturer support ends (e.g., due to business closure, market withdrawal, sanctions, or a distribution dispute). Remote deactivation or lockout must not be possible.
- **Backup and restoration:** it must be possible to back up and restore the configuration and grid-relevant settings, and the manufacturer should provide a tested baseline of the firmware in such a way that an installation can be put back into operation even without the manufacturer's involvement.
- **Limit the reach of one's own remote access:** even legitimate access should not be able to control or update the entire device fleet simultaneously. This must be technically enforced through separate networks, control servers, and cloud applications (see chapter *8.5.2*).
- **Offer a secured local interface:** for local control there is no widely used secure standard, and enforcing encrypted communication would break compatibility with common energy management systems. Manufacturers should therefore offer an additional authenticated and encrypted channel, as some already do (see chapter *3.3*), and deactivate the interface at the factory as long as it is not needed.

Part of these requirements is not a recommendation but product law: for devices with a radio interface, the cybersecurity requirements of the Radio Equipment Directive (RED) have applied since August 2025 and, for these products, will be replaced by the CRA in December 2027, which then applies to all products with digital elements (see chapter *7.3.2*). The findings of this analysis show that these requirements are not consistently met in practice. Manufacturers are therefore advised not to aim for the minimum needed for the declaration of conformity, but to implement the underlying principles: secure defaults and security as a design principle.

8.4.2 Factory-Set Control Lock for Grid-Relevant Functions

Beyond basic security hygiene, it is recommended that the device itself restrict which settings can be modified remotely. This principle is not new: the US NIST guidelines for inverters (NIST IR 8498)[84] recommend that capabilities not required in every deployment scenario be disabled at the factory and enabled only deliberately.

Such a restriction must be enforced at a point that can distinguish read from control commands by their content, and the enforcement point itself must not be bypassable. An ordinary network firewall does not meet the first condition, because operating data and control commands run over the same connection to the same endpoint. The restriction can be enforced in the inverter itself or in an upstream energy management system (see chapter *8.2*). The latter option, however, works only if the inverter has no path of its own open to the manufacturer cloud and refuses unauthenticated local write access. The recommendation distinguishes three classes of capabilities, each subject to a different regime: remote access in the as-delivered state, the grid-relevant parameters, and the feed-in setpoints.

As-delivered state: the only capabilities permitted remotely are reading operating data and cryptographically signed firmware updates. The installation must continue to run fully without the update channel, with unchanged behavior towards the grid.

The Swiss industry recommendation NA/EEA-NE7[85] recommends, by contrast, deactivating the function for remote firmware updates where possible and performing updates only on site. The reasoning is understandable, because the update channel is indeed the most powerful remote access. With an installed base of hundreds of thousands of small installations, however, this leads, in the NTC's view, to the greater risk: without a functioning update channel, known vulnerabilities remain open for years. The German BSI urgently advises checking regularly whether new software versions are available and installing at least those that fix security vulnerabilities as quickly as possible after a risk assessment.[86] The report follows this line but combines it with requirements for the update chain itself: cryptographic signature, protection against installing older versions, and a determinable version whose changes to grid behavior are documented.

Grid-relevant parameters: grid-relevant parameters are set at commissioning and are locked thereafter. These are the values that determine the installation's behavior toward the grid: e.g., the country setting as a whole, the protection settings for voltage and frequency, the connection and reconnection conditions, the reactive- and active-power behavior as a function of voltage and frequency, and the behavior in the event of grid faults. Their scope is prescribed by Annex E of the industry recommendation NA/EEA-NE7. At the same time, they are a particularly effective attack vector (see chapter *6.3*, type B). Swissgrid demands the same protection without reference to an attack: the installations' behavior in the event of a grid disconnection and their conditions for reconnection should be defined directly in the installation, in order to reduce a large uncertainty component in the demanding phase of grid restoration. These values are therefore to be protected not only because they can be manipulated, but also because grid operation relies on them.

The special protection of these values is also recommended internationally:

- The NIST recommendations for inverters call for unused interfaces to be disabled at the factory, for software to be accepted only from verified sources, and for control functions to be separated from communication interfaces. Notably, a password alone is no longer considered adequate for access that affects critical infrastructure.
- The Secura study recommends keeping critical parameters unchangeable and permitting

[84] National Institute of Standards and Technology (NIST), Cybersecurity for Smart Inverters – Guidelines for Residential and Light Commercial Solar Energy Systems, NIST IR 8498, December 2024: https://doi.org/10.6028/NIST.IR.8498
[85] VSE, industry recommendation "Grid Connection for Energy Generation Installations to the Low-Voltage Grid NA/EEA-NE7 – CH 2025": https://www.strom.ch/de/dokument/netzanschluss-fuer-energieerzeugungsanlagen-das-niederspannungsnetz-naeea-ne7-ch-2025-0
[86] Federal Office for the Protection of the Constitution (BfV) and Federal Office for Information Security (BSI), "Joint Security Advisory: Reconnaissance of Poorly Protected PV Installations by State Cyber Actors", 3 June 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

remote configuration only with local consent.[87]

For Switzerland, there is no uniform requirement for this. What would be decisive is that such a lock does not rest on authentication alone. A credential that is centrally available can be used across many installations simultaneously, and it is precisely this simultaneity that this report describes as systemically relevant. It therefore makes sense to tie the release of the lock to a local authorization on the device- for example, through a physical action on site, so that it cannot be triggered across many installations at once via a centrally available access. The lock applies to all write paths to these values, that is, the user interface, the local communication interfaces, the cloud connection, and the maintenance access. The physical tamper-evident sealing of meters and protective devices has long followed the same principle. This means the protection against unauthorized change, not immutability as such. If the connection conditions change, an adjustment in the installed base must remain possible.

Feed-in setpoints: locked, but releasable on site as soon as the installation participates in a grid service. A mere limitation of the setpoint range is not enough, because curtailment to zero is precisely the intended grid service and at the same time corresponds to the type A attack pattern. This is subject to two conditions:

- If the capability is enabled, it should not run via the manufacturer cloud but via the grid operator or the contractually bound aggregator (see chapter *8.5.1).*
- If the control connection fails or is never established, the device falls back after a holding time to a state defined at commissioning. The holding time prevents a communication disturbance from triggering a power jump across many installations simultaneously. Swissgrid sets the same requirement even without an attack scenario as well. Swissgrid recommends building new installations “fail-safe”: they should be able to continue operating safely even without external control and without functioning communication, for which the grid operators are to develop specifications for a predefined state. The trigger there is the ordinary communication interruption, that is, the same case that the holding time described above addresses. The recommendation thus does not presuppose the assumption of an attacker.
[88]

With this, the secured state is the default, and every additional remote controllability becomes a deliberate, visible, and locally made decision. This does not protect a device against manipulated firmware, because code on the device can bypass any device-side lock. Against the manufacturer itself and against a compromised update chain, therefore, only the integrity of this chain, a re-check upon significant firmware changes (see chapter *8.5.3*), diversification, and independent testability are effective.

Finally, on the relationship of this recommendation to the energy-policy thrust: the industry is moving toward more controllability. In its white paper on the integration of photovoltaics, Swissgrid states that flexibility will in the future be a precondition for photovoltaic systems, not an option. The factory-set control lock proposed here does not conflict with this. It does not require forgoing flexibility, but only that its release takes place on site and that grid-relevant control then runs via the regulated entity.

8.5 For Policy and Regulation

8.5.1 Responsibility

Close the responsibility gap for small-scale installations: requirements exist, but they fall short. The cybersecurity requirements of the Radio Equipment Directive cover only devices with a radio interface and rest on the manufacturer's declaration, and the industry recommendation on grid connection confines itself to password protection and updates. Effective instruments are those

[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 AG, white paper “System-Compatible Integration of Photovoltaics” March 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html

that do not start with the individual operator. Regulatory intervention is probably necessary here, because this safeguarding does not arise on its own. As approaches, possible models include approaches already used by other states: grid connection conditions for the controllability of installations (as in Lithuania) or procurement and funding criteria (as at the EU level). None of these paths is perfect (see chapter *7*). This need for action does not arise from the technical findings alone. The FIS explicitly points out that Switzerland gains in attractiveness as a target if neighboring states protect their critical infrastructure more strongly and Switzerland does not follow suit (see chapter *2.5*).

Secure sovereignty over grid-relevant functions: the goal is not a ban on the cloud, but a clear answer to the question of who may issue grid-relevant commands to an installation. This authority should lie with an entity that is itself regulated and is accountable for grid stability: the distribution system operator or a contractually bound aggregator subject to the ICT minimum standard. The European industry association recommends the same model, distinguishing between critical and non-critical functions: starting, stopping, and changing active and reactive power only via the regulated entity; monitoring and software updates also via other channels, provided these can be interrupted in the event of suspicion.[89] For Switzerland, this principle is already reflected in general terms: the distribution system operator may use an installation's flexibility only in a grid-serving way.[90] Swissgrid at the same time points out the practical gaps:[91] what is lacking is a standardized communication between the installation or energy management system and the distribution system operator, a standardized cascading between the grid operators, and the technical implementation of the legal rule whereby the guaranteed grid-serving flexibility overrides all other control signals. Whoever wants to regulate control sovereignty in a binding way must therefore also create the interface for it. Without it, the path via the manufacturer cloud remains the only one that works in practice. It remains to be clarified whether a permanent connection to a manufacturer cloud is required at all on the grid side and, if so, what requirements this infrastructure must meet. The mere hosting location is not sufficient for this (see chapter *5.4.5*). On the device side, the requirement that inverters have a control lock for grid-relevant functions active at the factory would be implementable (see chapter *8.4.2*). This direction aligns with the position of the German BSI (see chapter *7.3.1*).

Designate a body responsible for the aggregate risk: while no single small-scale installation warrants individual oversight, the risk arising from the aggregation of many such installations currently has no designated owner. What needs to be clarified is which entity observes this aggregated risk, coordinates in the event of an incident, and monitors the effectiveness of the product- and connection-side measures.

Prepare for the event of an incident: besides prevention, the ability is needed to detect an ongoing misuse and end it in an orderly manner. There is no central emergency off switch, and a defensive mass shutdown would itself endanger the stability of the grid. A compromised control channel can be disconnected safely only if the installations then fall into a safe, grid-compliant state (see chapter *8.4.2*) and a named entity maintains the situational picture and coordinates those involved. The capability serves above all to fend off persistent compromise and to manage the aftermath of an incident, not to prevent the first attack, which unfolds in seconds.

8.5.2 Reach of a Single Point of Access

Limit the reach of a single point of access: what is grid-relevant is not the severity of a vulnerability but its reach. This leads to a measure that works independently of market shares and product quality: no single point should be able to change an entire device fleet simultaneously. In classic generation, this limit arose on its own, because a power plant rarely comprises more than around 1.5 gigawatts and its control system reaches only this one plant. With manufacturer clouds and aggregators, it disappears. The European industry association therefore proposes to

[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 Electricity Supply Act (StromVG, SR 734.7) and Art. 19a Electricity Supply Ordinance (StromVV, SR 734.71). For context: Association of Swiss Electricity Companies (VSE), "Potential and Limits of the New Flexibility Regulation," December 2025: https://www.strom.ch/de/perspective/potenzial-und-limiten-der-neuen-flexibilitaetsregulierung
[91] Swissgrid AG, white paper "System-Compatible Integration of Photovoltaics" March 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html

prescribe it explicitly and back it up technically:[92]

- an upper limit for the generation capacity that can be addressed via a single control system: whoever operates more must use separate systems with no common cause of failure
- a segmentation of the manufacturer's own remote access, so that the entire fleet cannot be controlled at once
- technical precautions against the simultaneous updating of all devices, so that time remains for intervention if an update is faulty or manipulated
- device-individual random delays for selected control commands. Which commands are affected and how long the delay is are to be defined via standards and in coordination with grid operation

These measures require no forgoing of remote control and no change in market shares. They limit only how much a single command can do. Three caveats apply: the threshold has not yet been defined. The implementation lies in the manufacturer's architecture and is barely verifiable from outside, so without a duty of proof it remains a self-declaration. And it limits reach, not dependence itself: a segmented remote access provides time to intervene in the event of an incident, but still lets the manufacturer retain control over each individual segment.

Promote diversification in good time: the inverter market is consolidating strongly. For cybersecurity this is directly relevant, because a heterogeneous manufacturer field is itself a protective factor: different manufacturers, platforms, and firmware versions make it harder to reach many installations with a single attack. Conversely, with each further market consolidation a larger "single point of failure" arises. The goal should therefore be to have manufacturers in several world regions to choose from on a lasting basis, and not the preference for a particular origin. Instruments are, for example, procurement criteria that reward multi-vendor strategies. The point touches on procurement and trade law and can be implemented unilaterally only to a limited extent. The window could narrow, because several providers still have capacity but are losing market share. How this develops is open. Diversification lowers the risk of a single, cross-manufacturer exploit, but does not solve the structural core problem: at a threshold of under two percent of the European installed base (see chapter *6.5)*, practically every market-relevant manufacturer remains systemically important on its own. According to Secura, in the Netherlands an attack on a single manufacturer suffices; two meet this threshold based on their market share (see chapter *5.4*). Diversification is therefore a sensible complement, but not a substitute for the other measures named here.

8.5.3 Inspection and Retrofitting of the Installed Base

Product testing with a lifecycle component: a product-related cybersecurity testing regime for inverters and energy management systems is possible and sensible. Taiwan shows, with source-code analysis, traffic analysis, and firmware integrity checking, how deep such testing can go. What is decisive, however, is that such a regime does not stop at a one-time type test: needed are a prescribed cryptographic update procedure and a re-check upon significant firmware changes. The limit of every product test must be kept in mind: it addresses vulnerability to third parties but does not make one independent of the manufacturer itself. Against the scenario of the insider or state actor who controls the legitimate update chain, only diversification and a technical limitation of what the cloud may control remotely are effective (see chapter *5.2*).

Not all of this presupposes new law. For inverters with a radio interface, conformity with the cybersecurity requirements of the Radio Equipment Directive and the associated EN 18031 standard could already be checked today within market surveillance (see chapter 7.4 Regulation in Switzerland). Product-related testing regimes for this device class are also emerging internationally: alongside the Taiwanese type approval, there are programs such as UL 2941[93] and the certification of the SunSpec Alliance[94], on which a Swiss or European requirement could draw.

[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
[93] UL Solutions, UL 2941, Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources, 2023; certification program since February 2026: https://www.ul.com/services/cybersecurity-distributed-energy-and-inverter-based-resources
[94] SunSpec Alliance, DER Device Cybersecurity Certification: https://sunspec.org/certifications/

Use the existing installation inspection for cybersecurity: photovoltaic systems are subject to mandatory inspection under the Low-Voltage Installation Ordinance. An independent inspection body checks the installation after its construction, the safety certificate goes to the grid operator, and the inspection is repeated periodically. There is thus a mandatory procedure that captures the installation in its installed state and whose result ends up with a regulated entity. It starts where product requirements and requirements on the individual operator do not suffice. It is recommended to supplement the associated inspection protocol with a few unambiguously determinable points: e.g., changed default passwords, no reachability from the internet, deactivated unneeded interfaces, and the state of the control lock (see chapter *8.4.2*). Swissgrid proposes the same route for the operational settings and separately requires minimum requirements for cybersecurity that must also be inspected, without naming a procedure for this.[95] What is needed for this is adjusting the requirements within an established procedure rather than creating a new regime, and only what can be determined without room for interpretation remains verifiable.

Do not forget the installed base: all the preceding measures work above all via new installations. Only the periodic installation inspection also reaches the installed base, but slowly. The existing installation stock remains the larger open flank for years (see chapter *7.3.4*). One option for retrofitting existing installations would be an upstream communication unit that works with existing inverters and assigns control to the grid operator. It thereby transfers to the installed base what chapter *8.5.1 Responsibility* proposes.

Common to all these recommendations is one direction: photovoltaics should continue to grow, but control over hundreds of thousands of grid-relevant devices must not lie with a few entities whose interventions are technically unlimited and unverifiable from outside. The window for this is open. It closes with every installation that is built today and is still on the grid in twenty years.

[95] Swissgrid AG, white paper "System-Compatible Integration of Photovoltaics" March 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html