SOLAR INVESTOR'S GUIDE

SIG 6/2025

Minimising risks

Security of solar projects and power storage

photo: Tobias Langner Branding & Design

pv Europe
solar technology and applications

photo: Mildred Klaus

Identifying and mitigating risks in solar projects

Investing in solar parks, expansive rooftop systems and cutting-edge battery storage de-mands patience and a truly long-term perspective. Such projects are typically designed to operate for twenty years or more, making it crucial to safeguard them against a broad spectrum of risks over their entire lifespan – a priority that remains all too often underesti-mated.

This issue of our Solar Investors Guide centres on the topic of risk. Our aim is not to cause concern, but to raise awareness and offer practical, actionable guidance for managing these challenges with professionalism.

We pay particular attention to technical aspects and the exceptional quality of the compo-nents used. TÜV Rheinland's inspection engineers work worldwide, assessing and securing solar parks. Time and again, they find that durability and high quality are not given enough consideration when selecting solar modules, inverters and storage batteries. This oversight can have costly, long-term consequences. As the saying goes, buy cheap, buy twice.

We also share advice on protecting your investment from unauthorised access – whether from thieves targeting valuable metal components such as cables or inverters, or from criminals seeking to access operational data and plant controls via the internet. Robust cybersecurity is becoming ever more important and is now required by both grid operators and authorities. The surge in cyberattacks over the past three years underscores just how critical this issue has become.

Learn from the best how to avoid mistakes and actively minimise risks. I wish you an en-gaging and insightful read!

Yours,

Heiko Schwarzburger

Heiko Schwarzburger
editor-in-chief
PV Europe & photovoltaik

E-PAPER SOLAR INVESTORS GUIDE

Solarise parking and charging

Mobility is shifting to electric, bringing millions of private electric cars, company fleets and commercial vehicles that place new demands on the energy supply. Filling stations, parking garages and parking lots offer significant opportunities for supplying EVs with solar power. Download the new e-paper now – for free!

▶ *https://www.pveurope.eu/sig-2025-5-solarise-parking-lots*

photo: Heiko Schwarzburger

PREVIEW SIG 1/2026

C&I storage systems

photo: Heiko Schwarzburger

Our next SIG will provide insights into planning, installation and operation of C&I storage projects. These systems increase self-supply with solar energy, provide power for charging of EVs and help to manage peak loads to reduce energy costs in the industry.
It will be published on **2 February 2026**.

Speed matters – the easier it is for intruders to access the modules, the more they can take.

photo: Tobias Langner Branding & Design

Fight back against theft

Crime ▪ The number of thefts at solar installations has declined, but the risk remains. Because criminals are active and underway, and have their eye on the next generation of components. But the market offers suitable systems for protection.

by Sven Ullrich

photo: Tobias Langner Branding & Design

Perpetrators can be extremely aggressive. They show little concern for damage beyond what they actually steal.

Night-time is when they're most active. Most intruders prefer to avoid attention, but some are brazen enough to act as if they belong. The tactic is now well known: wearing a yellow vest, they blend in at solar parks, breaking in to steal entire rows of modules or inverters.

Falling prices, persistent risk

Module prices have steadily declined in recent years and inverters have also become less expensive, raising questions about whether such thefts are still worth the risk. Yet despite falling values, German police statistics show that solar component theft remains a persistent problem.

It's not just solar parks that are affected. Rooftop systems and even camper vans fitted with solar modules are targeted repeatedly. Rooftop installations are especially vulnerable when they are far from the nearest town or when buildings are out of sight, such as on agricultural properties.

In general, perpetrators choose locations that are not regularly visited by third parties or site managers, but are conveniently located for access. Ultimately, the true scale of theft at solar installations can only be guessed at.

Insurer data and financial impact

Insurers have recorded fewer thefts at solar installations since 2022, but whether this downward trend will continue or reverse in the coming months remains uncertain.

Every theft is disruptive and the financial impact on solar parks can be especially severe, with losses sometimes reaching several hundred thousand euros. Lost revenue from stolen modules and the costs of repair or replacement are also significant.

At present, solar modules and inverters are not the main targets for criminals. Often, only specific types of modules or inverters are stolen, or sometimes just their displays.

Construction and assembly risks

Solar park construction phases are especially at risk. During assembly, it's not uncommon for intruders to take as much material as can be fitted onto a van. Inverters, pallets of modules, mounting structure components and small metal parts are all vulnerable. These thefts are frequent enough that Allianz Insurance regularly settles claims for stolen inverters, particularly those rated between 30 and 50 kilowatts. And while theft at solar parks used to focus mainly on modules and mounting structures, insurers now report that such cases are increasingly rare.

Cables, machinery and opportunistic theft

Metals have now become the main target. Copper cables, installed in large quantities at solar parks, are valuable and easy to resell. They are also easier for thieves to steal.

photo: Tobias Langner Branding & Design

The easier the access to the solar field the easier is the getaway.

photo: Tobias Langner Branding & Design

Inverter theft is uncommon, but when it does occur, the consequences are especially costly.

photo: Tobias Langner Branding & Design

Sometimes criminals specifically seek out inverters in solar parks, operating for illicit deal-ers.

Other stolen items include construction machinery such as mini-excavators and site fences. Criminals have even siphoned fuel from diesel generators used to power surveillance equipment at solar parks, as well as batteries from switchgear.

Organised gangs and escalation

Inverters are stolen less frequently, but when perpetrators do target them, the losses are significant. Often, large numbers are taken at once. In one case, 52 inverters worth around €161,620 were stolen from a solar park near the border of Germany, the Czech Republic and Poland.

These crimes are mainly carried out by organised gangs acting with little regard for consequences. They are undeterred by collateral damage and have even attacked security staff or site personnel. Authorities strongly advise against confronting suspicious individuals directly. If in doubt, contact the police.

Advanced surveillance

That's why, monitoring construction sites at solar parks poses distinct challenges for project developers, not least the challenge of monitoring sites without external power infrastructure. German company LivEye operates all over Europa. It offers an autonomous surveillance system and a full-service package centred on security. An example: The tracks left by pallets of solar modules are still visible. With the last panels now installed on the module tables recently set up near Trier, a camera stands watch high above the site.

The permanent surveillance system that will eventually protect the new solar park from theft is not yet in place, so for now, LivEye's mobile monitoring system is securing the construction area.

Company background and technology

Based just a few kilometres east of Trier, near the Luxembourg border, LivEye has built up extensive experience monitoring solar parks, wind farms and construction sites. The company has developed a range of security solutions and operates its own emergency and service control centre.

Its latest innovation is a mobile, autonomous surveillance system powered by solar energy. "During transport, the solar modules are folded in and enclose the system," explains Carsten Simons, managing director of LivEye.

On site, the modules are unfolded and aligned with the sun. "We operate a summer mode when the sun is higher in the sky and a winter mode when the sun's angle is lower," Simons adds.

Night-time battery and fuel cell backup

The modules are wired in parallel, each with its own inverter to maximise yield, even if one module is shaded. "Every watt hour counts for us to keep the cameras running," Simons emphasises.

photo: Liveye

Systems are designed to be moved with a forklift or pallet truck.

photo: Liveye

The camera keeps a close watch over the construction site and, later, the facility itself.

Since most incidents occur after dark, LivEye equips the system with a large battery storage unit. This battery is sufficient to power the cameras on the mast for several days and, crucially, through the night.

For prolonged periods of low sunlight, the system includes a fuel cell. LivEye has fitted two 60-litre methanol tanks for this purpose – methanol being easier to handle than hydrogen.

The tanks are typically refilled once a year, but the solar modules remain the primary power source. "We run the system on the fuel cell for between 30 and 60 days a year," says Simons.

Mobile cameras and monitoring

Surveillance is handled by two PTZ (Pan Tilt Zoom) cameras, with both direction and zoom controlled remotely. These allow staff at the control centre to visually track intruders and capture detailed images of suspects and their vehicles, including licence plates.

In turn, these images can provide police with critical evidence for investigations or help guide officers through the park to potentially apprehend suspects. The images are high-resolution, ensuring details are clearly visible.

The cameras are mounted on a mast up to 6.5 metres high, covering a surveillance radius of up to 200 metres. LivEye primarily uses the system to monitor construction sites. The construction phase is the most vulnerable period for a solar park, with modules and other components stored on pallets awaiting installation.

Vulnerabilities during installation

Any materials not installed on the day of delivery remain overnight and become easy targets for theft. "It's not just the value of stolen components that matters," explains Andreas Schmitz, senior representative at LivEye. "If entire pallets of modules or inverters are stolen, it disrupts workflow. On a tightly scheduled site, this can cause delays that are very costly."

Camera surveillance can deter these incidents, but site procedures must be adapted to keep monitoring costs under control. "It's not efficient to secure the entire site during construction," says Simons. "All assets should be concentrated in the camera surveillance zones each evening to reduce the number of systems required."s

It also makes little sense to distribute modules throughout the park in advance. "They should be collected from storage only when installers are ready to mount them that day. It may also be worth increasing manual site security on days when large amounts of material are on site."

photo: Martini Media/Liveye

On-site, the solar modules are unfolded and supply power to the system.

photo: Liveye

Two remote-controlled, movable cameras trigger an alarm when they detect unusual movement.

Deployment and setup

LivEye quotes a monthly cost of €1,600 to €2,200 per system for complete construction site monitoring, including alarm evaluation at the emergency centre and data transmission costs.

The camera systems and supply container are delivered to site by lorry and can be moved by forklift or pallet truck. Once set up, the supports are extended and the solar modules unfolded. The mast with the cameras is then raised to a height of up to 6.5 metres.

This setup provides ample coverage. The system operates fully autonomously, with no external power connection required. For data protection, signage must be installed to indicate video surveillance is in operation.

Data security and alarm response

Once installed, the systems provide continuous monitoring of the construction site or solar park. “Typically, the systems monitor the site or facility overnight,” says Andreas Coböke, who heads LivEye’s emergency centre and service operations.

When the cameras detect unusual movement, they automatically trigger an alarm, which is sent via the mobile network. “If there’s no mobile coverage, we switch to very stable satellite connections,” says Simons.

Data transmission is secured via VPN to protect against attacks. Artificial intelligence helps distinguish between false alarms and real threats during alarm evaluation.

Alarm chain triggered

If unauthorised persons or vehicles enter the solar park, the alarm is relayed to a response chain, such as the police and the site operator. The systems are also equipped with loudspeakers, allowing staff at the emergency centre to address intruders directly. “This often causes thieves to flee immediately,” says Simons. At the same time, video recording is activated to secure evidence. Staff can also detect if a camera has failed or if someone attempts to tamper with the surveillance system.

The service centre also monitors the methanol tank levels for the fuel cell, allowing staff to dispatch maintenance personnel in good time for refilling.

▶ ***https://www.liveye.uk/***

photo: Velka Botička

The camera mast can be extended up to 6.5 metres, providing ample coverage.

The path to the loot is blocked - by lockend fences.

How to guard solar assets

Project business ■ As solar parks become the new playground for thieves, it’s time for operators to outsmart the light-fingered competition. Because criminal tactics evolve. Protection starts with planning and is part of asset operation, too.

by Sven Ullrich

photo: Velka Botička

photo: Velka Botička

These inverters are well protected against thieves.

photo: Velka Botička

High costs mean video surveillance is used sparingly in solar parks.

Solar module prices have fallen steeply in recent months. At first glance, this could suggest that panels are no longer attractive to thieves. In principle, as the price of new modules falls, so does the value of stolen goods on the black market.

But that's far from the reality. "Even with lower module prices, theft prevention remains a key issue," warns Jana Grathwohl from project developer Enviria. "Beyond the material losses, theft can lead to significant project delays. Our security concept not only protects the components, but also ensures reliable project delivery for our clients."

More recently, thieves have shifted their attention to cables. High metal prices have made cables more lucrative, and they are also easier to resell. The installation period is particularly vulnerable, as this is when solar parks and large-scale storage systems are being put in place.

Lasse Nieswitz, who oversees project execution at Goldbeck Solar, explains: "With almost 15 years of experience in solar plant construction, I can say that theft is definitely an issue, just as it is across the entire construction sector. For us as an EPC, it is particularly relevant during installation." During construction, the priority is to raise barriers to theft, especially overnight, and

photo: Secondsol

Visible security measures help deter opportunistic thieves.

to minimise losses if theft does occur. “That’s why we put up fencing around the site before we even start building the solar plant. Additional measures, such as installing a video surveillance system or deploying security personnel can also make sense.”

Off-grid power supply is crucial

Unlike in the operational phase, it’s essential during construction that security systems work independently, using solar modules, batteries, fuel cells or diesel generators. However, there have been cases where even the fuel for diesel generators was stolen from the site.

At Enviria, effective site security rests on three pillars: physical barriers with fences and lockable gates, electronic surveillance with cameras and motion detectors, as well as regular checks by security personnel. Project staff also need regular training.

Fences at least two metres high

Staff must play their part in preventing components from disappearing overnight. This includes making sure that materials are stored at the end of each workday in fenced-off areas monitored by cameras.

But protection doesn’t stop once the solar generator is built. Large solar parks are often found in remote areas, and insurers are increasingly unwilling to cover preventable theft. “For ground-mounted installations, at least a suitable enclosure is required,” recommends Barmenia Insurance. The fence should be at least 1.8 metres high and have extra extensions to deter climbing.

Observe regional requirements

Insurers also advise installing a steel fence or wall with features to prevent climbing and burrowing. Wooden pasture fences are not considered suitable. Lockable gates further help restrict unauthorised access. Regional regulations are a key consideration.

In some cases, environmental requirements make anti-burrow measures unworkable. In certain regions, fencing may not be allowed at all.

Technical safeguards

Experts at Allianz Insurance recommend regular patrols by security personnel. Materials and components at construction sites or in solar parks can also be safeguarded with technical solutions. Options include tamper-proof screw heads with embedded steel balls or plugs, or screw heads sealed with resin. Inverters are best protected with cages or enclosures.

In many cases, police advise installing and securing inverters and storage units within a concrete technical station, with special attention to the security of windows and doors.

Electronic systems

Theft prevention measures can be tailored to local conditions, using tools like fence sensors, dome cameras, video surveillance with motion detection and GPS transmitters in module junction boxes. Moreover, such solutions support the recovery of stolen components.

Investors and park operators are often hesitant to use cameras, so these systems are rarely installed. Cameras are costly to buy and operate, require ongoing maintenance and must be linked to an emergency response centre.

Thieves adapt quickly

Watchful thieves will quickly notice if cameras fail or alarms go unchecked. They approach the solar park and watch for any reaction. If no one responds, they know the surveillance isn’t working.

Some insurers make cameras a prerequisite for coverage. In these cases, operators have little choice. Best practice is to plan for camera surveillance from the start and, at minimum, install empty conduits in advance, taking advantage of open cable trenches during installation. Enviria deploys camera surveillance when the risk of theft is deemed high. “For projects on secured industrial sites, we can often leverage existing infrastructure, which is both cost-efficient and secure,” says Jana Grathwohl.

Other factors considered

Other factors such as project size, value and insurance costs are also considered, along with site-specific risks. “Overall, investment in solar project security typically accounts for only a small fraction of total costs,” notes Roman F. Kehrberger of Enviria. “This investment pays off by preventing damage and delays, and by securing better insurance terms.”

Design makes access harder

Theft prevention begins at the planning stage of a solar project. One strategy is to design construction roads to limit accessibility and reduce the number of access routes. This makes it harder for thieves to reach cables or inverters, slowing them down when time is not on their side.

The more effort it takes to reach valuable components, the greater the risk for the would-be thief. Ultimately, strong deterrence is the best defence against opportunistic theft. And deterrence starts with planning of the solar park and preparation of installation.

▶ *https://enviria.energy/en*
▶ *https://goldbecksolar.com/en/*

photo: Secondsol

Security labels or artificial DNA markings boost the chances of recovering stolen components.

INTERVIEW

“Deterrence is key”

Secondsol has introduced the German website PV-Diebstahl as a straightforward addition to existing solar plant security measures. Managing Director **Stefan Wippich** explains how the two-stage protection system works.

You have developed PV-Diebstahl to prevent components from disappearing from solar plants. How does the system work?

Stefan Wippich: *PV-Diebstahl is a two-stage protection system. The first stage involves securing components on site. We do this using special security labels and prominent signs on the perimeter fence, making it clear that all components are marked. This acts as a deterrent to thieves. The labels also make it more difficult to resell or reuse stolen components. The second stage focuses on tracking and tracing any stolen items.*

How does this second stage work?

Modules are registered in our database with both their serial numbers and the numbers from their security labels. If components are stolen, police can use the QR codes on the labels or the serial numbers of modules and inverters to check the database and confirm whether they belong to a registered plant. They can also identify which plant the components came from and whether they are being sold legally or were stolen. The database includes the contact details of the component owners, enabling police to reach out to them directly.

That’s a good idea, but couldn’t thieves simply peel off the security labels so no one notices?

If thieves try to peel off the labels, they tear into small pieces. There’s always a checker-board pattern left behind, which can only be removed with a lot of effort. This increases the risk of detection if thieves try to sell labelled components. The QR code makes it easy to identify the product, giving the police a starting point for investigation. At the same time, removing the label on site takes time, so thieves can’t steal as many components in the same period, which reduces the total loss.

Are modules with labels also harder to sell?

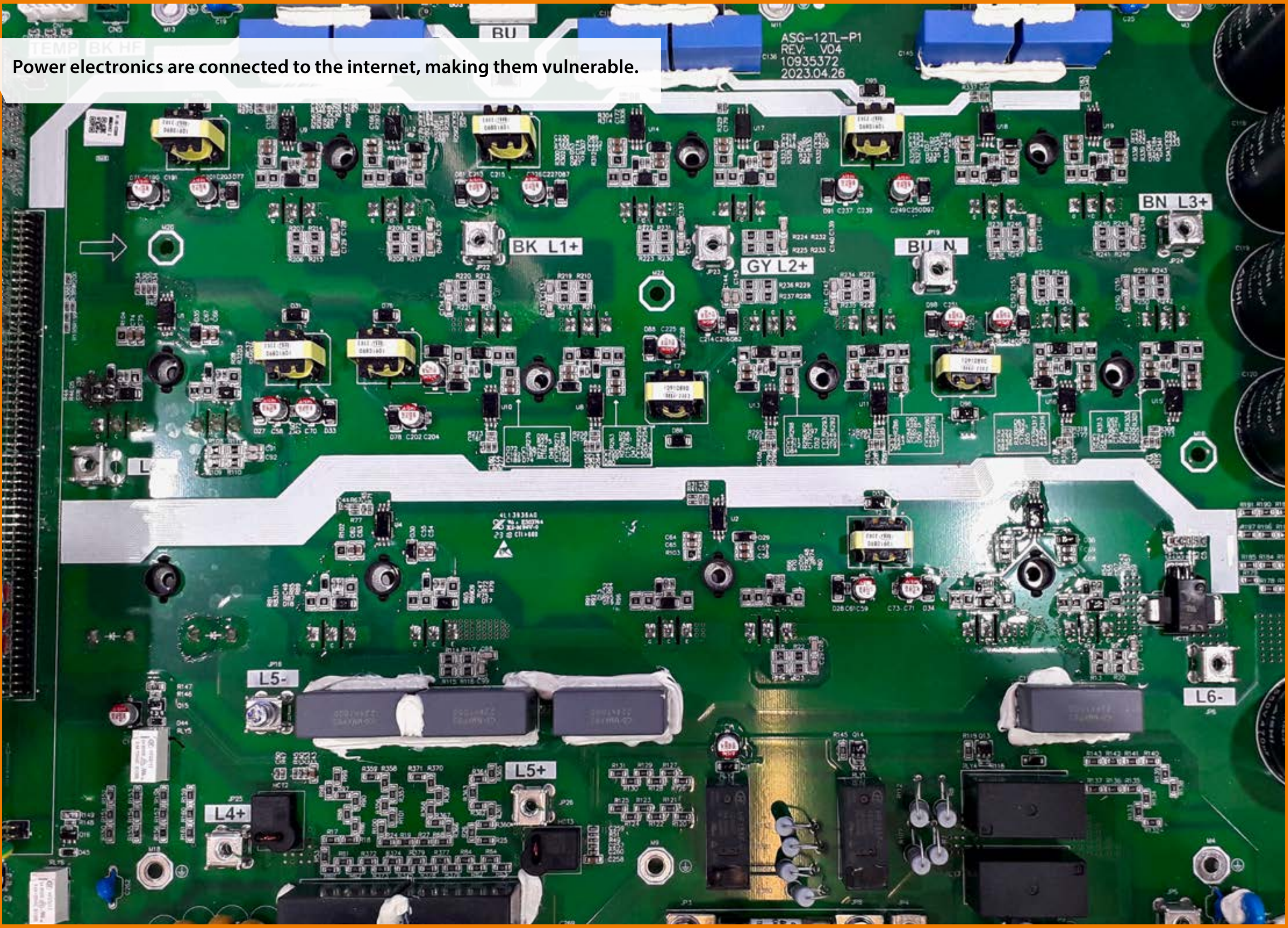
Exactly. Thieves would need to clean the modules and inverters thoroughly, which greatly reduces their value. Like anyone else, thieves consider the economics and want to sell components with minimal effort. Removing the labels adds to their workload and cuts into their profits. Even if the label is gone, there is still a risk of detection through the module or inverter serial number, which remains in the database. This provides a reliable way to trace the origin of components.

Are labelling and registration enough to prevent theft?

Indirectly, just like other systems. We rely on strong deterrence. Of course, this does not replace fencing, alarm systems or similar security measures – it complements them. Like bicycle coding, security labels and online registration make products harder to sell, which discourages thieves. As with bikes, coding is more effective as a deterrent than as direct theft protection. It shows ownership and helps police match recovered items. The goal is to prevent thieves from even considering breaking into a solar park or climbing onto a roof.

photo: Secondsol

Interview by Sven Ullrich.
▶ ***https://www.pv-diebstahl.de***



Power electronics are connected to the internet, making them vulnerable.

photo: Heiko Schwarzburger

Cybersecurity threats rise for PV systems

IT & OT ■ Security has long been a priority for the solar sector. Established standards, products and solutions exist to protect against lightning, surges, fire and theft. But now a new challenge has emerged, and it should not be underestimated.

Heiko Schwarzburger

There was a time when security meant a cast-iron lock on the door to your home or the factory gate. In this digital age, however, it no longer pays to think in such material terms. Connected systems introduce new vulnerabilities, enabling hackers to exploit data networks remotely, bypassing physical defences entirely.

Attacks are a reality

Cybersecurity threats are no longer hypothetical. Gaining unauthorised access through data cables, routers and IT systems has become routine, posing a persistent and concrete danger.

Incidents such as Russian hackers targeting of Ukraine's power infrastructure on Kremlin orders represent only a fraction of the growing risks. Cyberwarfare is ongoing globally, regardless of official statements.

Bomb labs and intercepted pagers

In the Iran-Israel conflict, hackers have repeatedly targeted Iran's nuclear programme. In 2010, Israeli specialists deployed the Stuxnet virus to disable centrifuges at Natanz, marking the first known cyberattack on an industrial facility. The virus, a joint US-Israeli development, was likely exposed unintentionally.

Another attack in April 2021 caused a blackout at the same facility, this time without public acknowledgment from Israel. More recently, in summer 2024, tens of thousands of Hamas pagers were remotely destroyed in a targeted cyber operation.

Varta hit by hackers

In February 2024, a cyberattack paralysed all five Varta plants, halting battery cell production for four weeks. The hackers accessed the company's IT systems, forcing Varta to shut down all internet-connected operations.

Facilities in Germany, Indonesia and Romania were all affected, with many employees placed on leave or reassigned to maintenance tasks. The subsequent recovery of the storage units and data centre took months to complete.

Rheinmetall under attack

In spring 2025, German arms company Rheinmetall suffered a breach exposing 750 gigabytes of confidential data on weapons systems and production processes. Hackers published links to 1,400 internal documents, targeting the company for sabotage and espionage. Darknet monitoring revealed the breach, prompting Rheinmetall to alert authorities.

Two sides of AI

A survey by DXC Technology found that the maturity of AI systems has significantly increased cybersecurity risks. Advanced tools like deepfakes and sophisticated phishing techniques enhance the credibility of attacks, enabling criminal hackers and terrorist groups to exploit these emerging technologies more effectively.

"Companies must take AI-driven threats seriously and adapt their security strategies," says Bruno Messmer, AI expert at DXC Technology. He advocates using AI for attack detection, staff training and recruitment.

Despite its risks, AI also offers powerful tools for combating cybercrime. Yet, over a third of German companies and an even higher share in Austria and Switzerland do not yet use AI in their cybersecurity measures.

Entry points multiply

The widespread use of smartphones, tablets and laptops by installers blurs the line between professional and personal activities, creating new vulnerabilities. Apps, SMS and social media platforms can easily expose sensitive data.

Adopting a zero-trust approach in which users authenticate at every network entry point can help limit the impact of compromised devices. Staff awareness is also critical, though only about half of German companies conduct regular cyberattack drills, with slightly higher rates in Austria and Switzerland.

Emergency planning

Cyberattacks on critical infrastructure are expected to rise, targeting factories, power plants and hospitals. While progress is being made, it remains gradual.

photo: Heiko Schwarzburger

Many decentralized storage systems help to make power grids more secure.

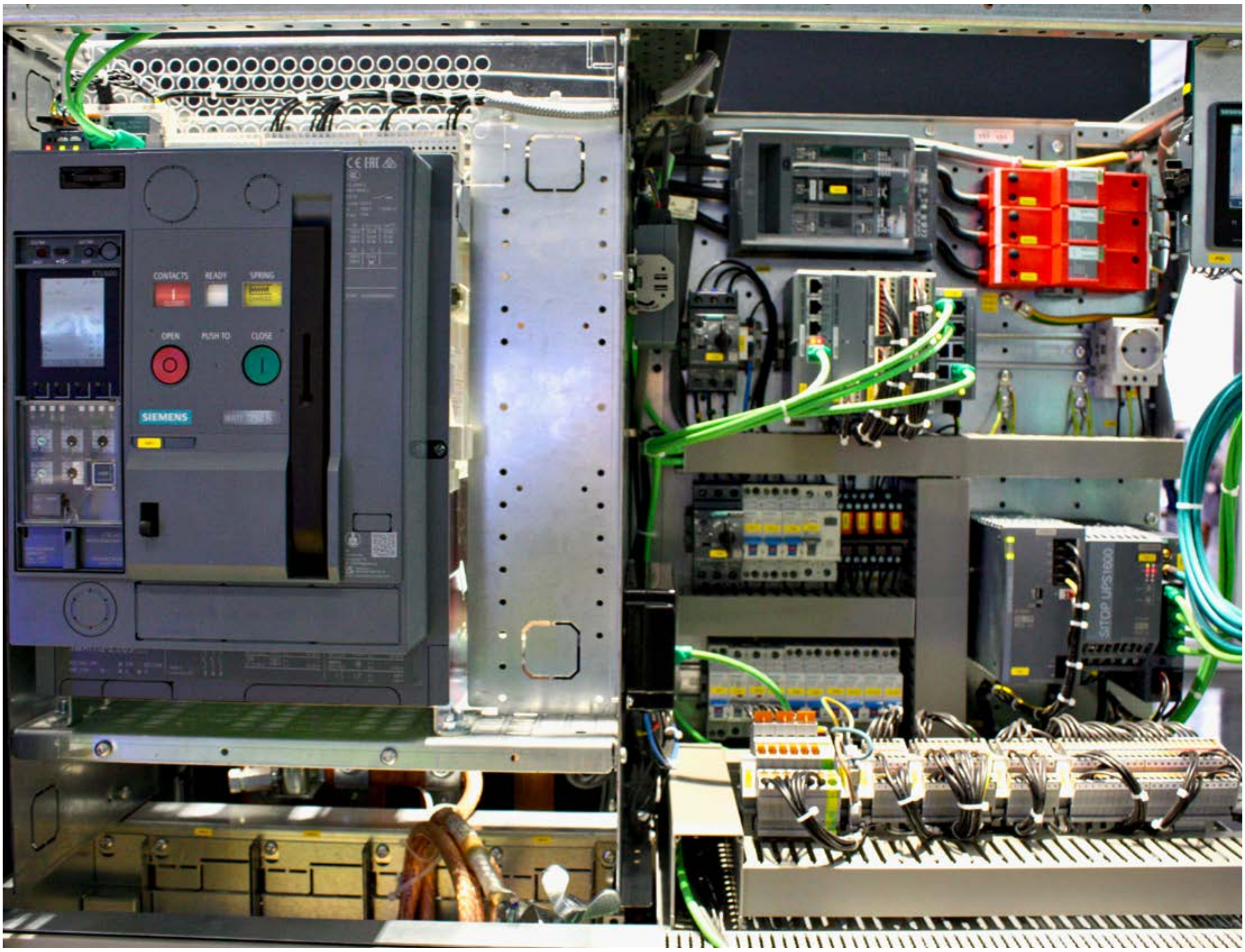


photo: Heiko Schwarzburger

Charging stations for electric vehicles are also considered critical infrastructure.

Currently, 76 percent of German companies have emergency plans for cyberattacks, up from 52 percent two years ago. In Austria and Switzerland, nearly 70 percent of firms are similarly prepared.

Supply chains under scrutiny

Cybercriminals increasingly target supply chains, exploiting networks of companies, suppliers and customers to access credentials, internal data and client information. Comprehensive risk management, including regular supplier assessments, is essential for digitally connected supply chains.

This focus aligns with Germany's upcoming Kritis umbrella law, which implements the EU's NIS-2 directive. Currently, 76 percent of German companies assess their suppliers for cyber risks, though the rates are lower in Austria and Switzerland.

Solar power ensures grid stability

The energy transition is improving grid stability. As more solar and wind power feed into the network, voltage and frequency fluctuations decrease, reducing blackouts. Renewables have made significant strides with grid-supporting features such as curtailment and fault ride-through.

Cybersecurity for the solar sector

Again, however, the digital management of solar installations introduces new vulnerabilities. Solar systems are classified as critical infrastructure, prompting stricter regulations in Germany, Austria and Switzerland to align with European guidelines.

European manufacturers are seen as leading the way. "We take this issue very seriously," says Dr Harald Scherleitner of Fronius International. "Our products meet the highest security standards, with full-time experts ensuring protection against unauthorised access and safeguarding operational data."

Fronius stores data exclusively on European servers and clouds and achieved ISO 27001 certification in 2022. The company has proposed an Inverter Security Toolbox, modelled on the 5G Security Toolbox, to regulate access to the European grid.

Expertise at SMA

At SMA, cybersecurity specialist Marek Seeger works to address security vulnerabilities. The Kassel-based, ISO 27001-certified company highlights how decentralised, interconnected generators now replace isolated large power plants in today's grid.

Speaking at the PV Symposium, Seeger highlighted a targeted attack that disabled solar systems in Beirut shortly after the destruction of Hezbollah's pagers. He also cited incidents in Japan where hackers threatened to destroy installations by compromising monitoring systems.

Long-term, targeted attacks

Seeger warns that state-backed actors pose the greatest threat, with their expertise and resources enabling highly coordinated, long-term attacks.

SMA employs a layered cybersecurity approach, including encrypted connections, anomaly detection and firmware updates. These updates are critical for security but require action from installers and maintenance teams. “IT security is a shared responsibility,” Seeger emphasises.

Customer awareness

Seeger advises customers to prioritise security when choosing inverters. European-developed devices with secure, regularly updated software offer greater reliability. He also recommends hosting monitoring platforms and data entirely within the EU to benefit from stringent data protection laws.

ISO 27001 certification

For large-scale projects, TÜV-certified ISO 27001 compliance is essential, ensuring systematic vulnerability management. Michael Silvan, IT security expert at TÜV Rheinland, highlights the importance of this certification as the EU’s NIS-2 directive is implemented by 2025.

Mandatory from November 2027

The EU Cyber Resilience Act, adopted in 2024, sets cybersecurity requirements for products with digital controls, including inverters and smart meters. From November 2027, all providers must demonstrate compliance.

POLAND

Measures set out to boost grid resilience

The Polish Energy Ministry and transmission operator PSE have put forward a package of legislative changes to strengthen grid resilience and protect against disruptions, including outages and cyberattacks.

The proposals, which are scheduled for cabinet review, include amendments to the Energy Law, the Cybersecurity Law, and the Public Procurement Law. These measures are intended to ensure that households and businesses maintain reliable electricity access during unexpected disruptions. The initiative follows a major outage on the Iberian Peninsula on 28 April 2025, which brought into focus the vulnerability of modern power systems to large-scale disruptions.

▶ ***https://www.pveurope.eu/markets/poland-sets-out-measures-boost-grid-resilience***

ALBANIA

Lorenc Malka talks about advancing electricity market liberalisation

In his interview on **PV Europe**, Lorenc Malka discusses Albania’s energy-market liberalisation, exploring solar investment, new incentives and the pressing shift from hydropower to solar as climate pressures intensify. The Professor of the Energy Department at the Polytechnic University of Tirana explores how solar energy and storage could reshape the nation’s energy future.

Albania’s geographical location in Southeast Europe offers strong potential for photovoltaic deployment. Professor Lorenc Malka outlines the current landscape, future scenarios, opportunities and challenges for developing photovoltaic power plants and battery energy storage systems in the country. Read the full interview:

▶ ***https://www.pveurope.eu/markets/lorenc-malka-solar-key-albanias-hydropower-challenge***

SOLAR INVESTORS GUIDE PODCAST

Cybersecurity – Villains come via the Internet

photo: SPE/private

Cybersecurity is a burning issue for inverters and solar storage systems. Uri Sadot is Cybersecurity Expert from SolarPower Europe. In this talk, he explains risks and incidents and analyzes gaps in the security of systems and installations. He says: Those who take precautions avoid criminal access. Those who wait risk significant damage – from economic losses to system failure and grid disruptions.

New EU directives are tightening the requirements for devices, their integration, and the operation of systems. Data storage is also part of the critical infrastructure. To be prepared, what should be done? Duration of the podcast: 1:09 hours

▶ ***https://www.pveurope.eu/podcast***

SOLARPOWER EUROPE

Unlock the full potenzial of renewables

SolarPower Europe submitted the paper in response to the European Commission’s Call for Evidence on the “Revision of the EU Energy Security Framework”. The paper highlights key vulnerabilities in Europe’s current energy system, such as fossil fuel dependency, cybersecurity risks and supply chain concentration, and proposes practical pathways to address them. The European Commission is preparing a revision of the EU Energy Security Framework, expected in early 2026.

“Europe’s energy security strategy must evolve with its energy system. Energy security policies can no longer incentivise fossil fuel storage or imports. It must be built on renewables, flexibility and electrification,” said Dries Acke, Deputy CEO of SolarPower Europe.

Solar power and battery energy storage systems (BESS) already play a decisive role in safeguarding Europe’s power supply, saving around €29 billion in fossil fuel imports in the summer of 2022 alone. Accelerating solar, storage and flexibility solutions will enable Europe to permanently reduce its reliance on imported fossil fuels and protect consumers from price volatility. SolarPower Europe proposes the following measures:

- Unlock the full potential of renewables for grid stability by enabling solar, batteries and inverters to provide flexible power, balancing and grid stability services, replacing fossil fuels in these roles.
- Establish a robust EU cybersecurity framework to safeguard distributed energy systems and inverters, with strong harmonised standards, strict remote-control limitations and EU data storage requirements.
- Build resilience against economic and climate shocks by investing in a flexible, decarbonised, renewables-based system that protects citizens from volatile energy prices and supports agriculture and biodiversity with solutions such as agrisolar and floating PV.

▶ ***https://www.solarpowereurope.org/advocacy/position-papers/securing-europe-s-energy-future***

photo: Secida AG

Sonna Barry

holds a business degree and has worked with complex business software since 2007. Her passion is translating technical knowledge for non-specialist decision makers. Since 2018, she has focused on cyber security. She is Vice President of Business Development & Strategy at Secida AG, which provides analysis, design, implementation and managed services for IT infrastructure and cyber security. Its clients include companies in the energy, finance and industrial sectors.

▶ ***https://secida.com***

“Cybersecurity must be a top priority”

Kritis ■ Statistically, solar power systems offer more effective blackout protection for the grid than large power plants. But the risk of cyberattacks should not be underestimated. Expert **Sonna Barry** of Secida AG explains how solar companies can respond to escalating threats.

an interview

Solar parks and large battery systems are now part of critical infrastructure. How important is it to protect them from unauthorised access?

Sonna Barry: Critical infrastructure today includes not just energy networks but many other essential services such as large public companies, hospitals and supermarket chains. The number of attacks has risen sharply over the past five years. Criminals often try to extort ransom money, and an entire criminal economy has emerged.

What kind of criminal actors are we talking about?

It started with the clichéd “hoodie hackers” or cyberkids who were seeing how far they could get. You might still find a few of them out there. But today we see state-sponsored groups and highly organised cybercrime outfits whose services can be bought on the darknet. These teams systematically scan for vulnerabilities to access data or systems, and the rise in attacks reflects how sophisticated this business has become.

Is this a growing wave?

It’s already here. Attacks have become routine occurrences for mid-sized companies. The statistics show thousands of attempted breaches every day. The question isn’t if they happen, it’s whether they succeed. You could say cyberattacks are as frequent now as pickpocketing at a train station.

Have there been known attacks on energy systems?

Cyberattacks now seem to be part of modern warfare. The Baltic states disconnected from the Russian grid to reduce their risk. In 2016, Ukraine suffered a

photo: Heiko Schwarzburger

Wind power, solar generators, power storage – decentralized energy supply is becoming increasingly complex and thus more vulnerable to criminals.

partial blackout caused by hackers, reportedly with links to the Russian state. Incidents like this have become increasingly common.

Are there any known cases in the solar sector?
Studies show that if attackers gain control over even a few gigawatts of PV capacity, they could destabilise the grid by shifting the frequency. Fortunately, that scale has not yet been reached. But as more PV systems and batteries connect to the grid, protection becomes more urgent. It's the price of progress.

What requirements come from EU and German law?
We usually split it into compliance and operational security. Let me start with compliance, which covers legal obligations. The EU's new NIS2 directive will greatly tighten documentation and reporting requirements. The original 2016 directive has been expanded because threats have grown. The energy sector was already covered, but now it applies to many more and smaller providers.

What qualifies a company or facility for NIS2 obligations?
Either it has a turnover of more than ten million euros annually or has at least 50 employees. There's a useful self-assessment form on the German Federal Office for Information Security (BSI) website. The BSI also offers extensive guidance and support. That form helps companies determine if NIS2 applies. The directive hasn't yet been transposed into German law.

In our field we deal with inverters and storage systems, usually linked to the grid via power electronics and control. What do manufacturers need to consider?
The EU has adopted the Cyber Resilience Act to cover these products. It applies to all internet-connected devices, including inverters, batteries, energy managers and building automation tech. From 2027, such devices may no longer be sold if known vulnerabilities exist. Manufacturers must constantly test for weaknesses and reduce risks, for example through regular firmware updates or targeted fixes for critical flaws.

What do you mean by vulnerabilities?
Primarily, we mean gaps that weren't known when the product was sold but which could allow external access. Detecting such flaws, whether in products or internal IT systems, is the first step towards better cybersecurity. Devices also need to fit seamlessly into a broader security architecture.

photo: Heiko Schwarzburger

Storage systems play a crucial role in energy supply – also in terms of security.

Can you give an example?

Sure. An inverter sends its operating data to a cloud or operations centre. Those servers are also part of critical infrastructure. So if you're analysing risk, you can't stop at the inverter. You need to consider the entire digital chain.

You mentioned the German Kritis law?

Yes, the Kritis umbrella law currently applies. This originally transposed the first NIS directive into national law. The IT security catalogue from Germany's Energy Industry Act (EnWG) also applies. It requires energy providers to be certified by the Federal Network Agency, and energy traders by the BSI. I hope the new rules will simplify things. We need better protection, ideally with reduced bureaucracy.

How should a solar company proceed, for example if it runs a portfolio of solar parks?

First, ask yourself: do we have anyone in the company with cybersecurity expertise? If not, bring in qualified partners. Otherwise, it's easy to get overwhelmed, especially with limited internal capacity.

What are the key elements of protection?

Compliance is one. Hardening IT systems and operations against attacks is another. You may need partners to meet compliance standards. Among other things, they can help you work through ISO 27001 certification. Even if certification isn't mandatory, going through its checklists helps identify and fix weak points.

What's the right process for identifying vulnerabilities in systems and operations?

Start by analysing your IT landscape and also your operational technology (OT). The key questions: what weaknesses are present, how serious are the associated risks, and what worst-case scenarios could emerge? This kind of baseline analysis requires coordination between management, IT and all departments. It's about finding critical systems and determining how long they can go down before mission-critical systems are threatened.

What comes next?

Then you address the risks. Cybersecurity must be part of overall risk management. We already do this in fire protection, if needed we bring in outside expertise. Many companies now need to extend this kind of thinking to the area of cyber.

Can you give a practical example?

Most firms have fire plans or emergency procedures for technical failures. But what if all your inverters are hacked and your technicians can't access the systems? You need backup processes ready to go. That's part of what's generally referred to as Business Continuity Management, or BCM.

This gets serious when storage systems providing balancing power go offline …

Exactly. Even during an attack, fallback mechanisms must kick in to protect the grid. That includes alerting grid operators, the Federal Network Agency and the BSI. Countermeasures must take effect quickly, or at least a secure backup must take over. All this needs rigorous preplanning.

How do you recover from a cyberattack?

The goal is to restore operations as quickly as possible. You may have to rebuild systems or restore backups. That can take time and money. If hardware is damaged, it must be replaced.

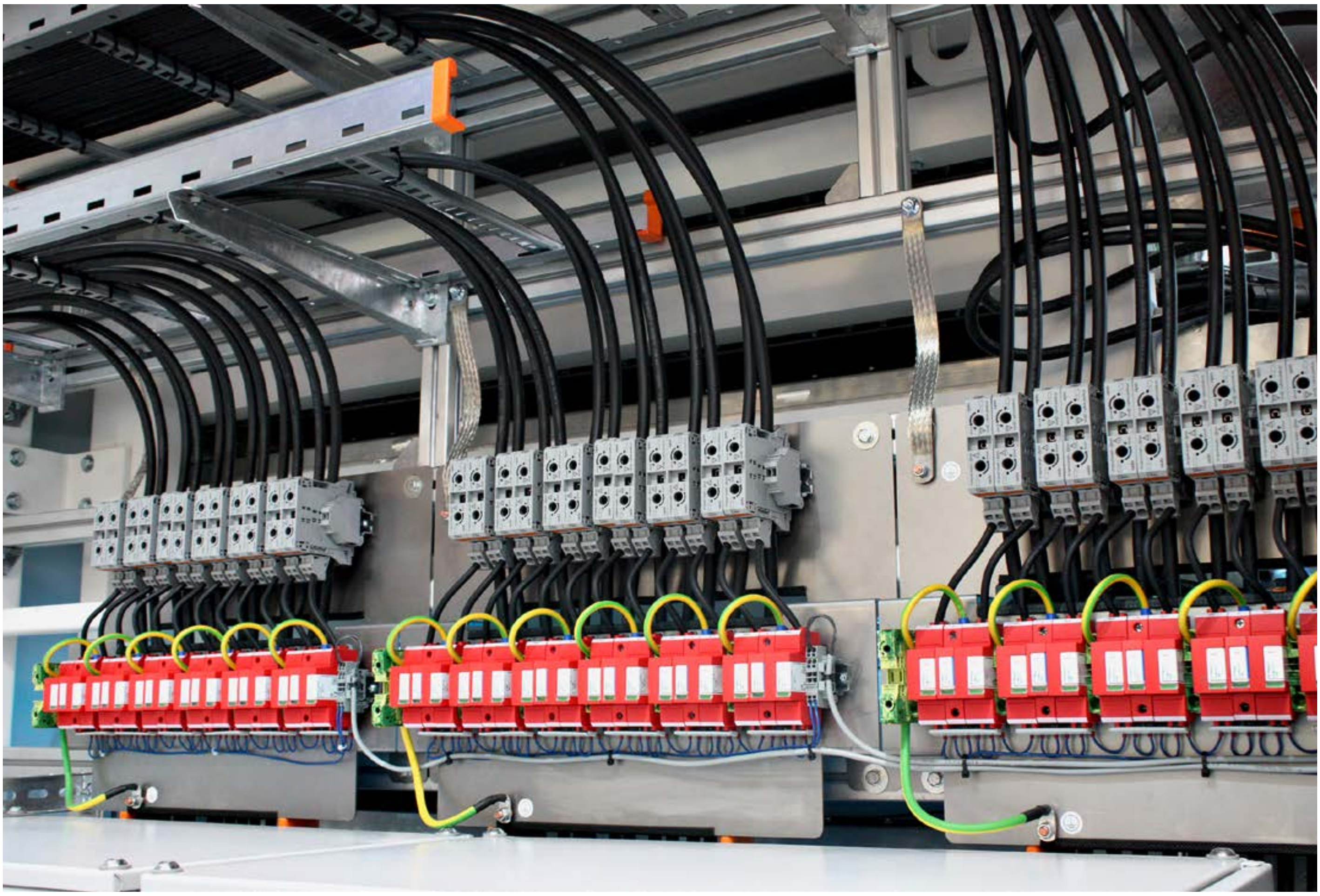


photo: Heiko Schwarzburger

The control of storage systems on the grid is a loophole for criminal elements.

photo: Heiko Schwarzburger

In Europe, renewable energies are considered critical infrastructure that requires special protection.

How can damage be limited?
It helps to stock critical components for quick replacement. You also need to decide what data should be stored offline versus in the cloud. Cloud-stored data should have an offline backup that's inaccessible to hackers. These decisions depend on your risk profile and risk appetite.

How reliable are firmware updates and patches?
Updates must be applied promptly and in their latest version. You need an inventory of all devices and the software running on them. This ensures updates reach every relevant system. You also need to test whether the patches actually work in your infrastructure. Ultimately, responsibility for security lies with the operator. It can't be outsourced.

So cyber security is never "done"?
Exactly. You can harden systems, but the job isn't over after installation. Ongoing monitoring is crucial. Monitoring systems will flag suspicious activity, although some alerts turn out to be false positives.

How do you filter the real threats?
AI can help identify typical patterns and distinguish real threats from noise. Attacks leave traces. Good monitoring systems speed up detection and help prevent escalating damage.

What happens after a confirmed attack?
Then it's the job of IT forensics. They determine when and how the attack happened, what was compromised and what actions were triggered. Speed matters: the longer attackers remain undetected, the greater the risk.

This really does sound like fire protection.
Exactly. And just like fire drills, cyberattack response must be practised at all levels. Don't wait to learn the hard way as that will undoubtedly be expensive.

Which risks are most often underestimated?
Access credentials. Companies need strong authentication systems and clearly defined access rights. Regular employee training is essential. Otherwise, it's easy to fall for phishing. Some risks can't be eliminated entirely, but cyber insurance can help cover potential losses.

How useful is ISO 27001 certification?
It's part of the Kritis framework and aims to expose and reduce vulnerabilities. At Secida, we're ISO 27001 certified. It takes time and effort, but it offers an excellent starting framework. Still, I wouldn't recommend it unless it's legally required, because it's resource-intensive.

Is it relevant for the solar industry?
Personally, I would only use inverter suppliers certified to ISO 27001, otherwise you have to assess the risk of non-certified vendors. The standard applies EU-wide, and certification lasts two years.

How much does it cost?
We spent a five-figure sum for certification at Secida. The documentation alone takes considerable effort. But preparing for certification is valuable in itself as it helps identify risks and design responses. The BSI provides free resources, guides and templates on its site.

What's the certification process like?
Once you've gathered the documentation, an audit firm steps in. They check whether your documented processes are actually followed in practice. Then you usually get a list of corrections. Recertification after two years is much easier.

What's your assessment of cyber risk in the energy sector?
Operational technology is often fairly secure thanks to BNetzA regulations. But back-office IT is frequently a weak point, especially in municipal utilities. Hackers can use that entry point to reach operating systems. That's what happened in Ukraine: they hijacked control servers and took down substations.

So even small gaps can have major effects?
Precisely. IT systems are often less protected by regulation and more vulnerable. That makes it easier for attackers to reach the core systems. The resulting damage can be immense. That's why cyber security must be a leadership issue, not just an IT problem.

Interview by Heiko Schwarzburger

Hamza Maaroufi is one of TÜV's experts for solar modules and solar parks.

photo: Oliver Tjaden/TÜV Rheinland

Increasing requirements for solar modules

Certifications ■ The enormous price pressure has consequences. Sloppiness and errors in manufacturing are becoming more common. Therefore, it is essential to inspect the product before installation.

by Heiko Schwarzburger

photo: Oliver Tjaden/TÜV Rheinland

Tausende Module werden jedes Jahr beim TÜV in Köln auf Herz und Nieren geprüft.

The certification procedures for modules and components are becoming more demanding all the time. This comes against the backdrop of larger and heavier modules making their way onto the market. Price pressure sometimes leads to savings being made in the wrong areas, namely glass panes, frames, screws, or clamps.

At this year's Solar Energy Conference in February, TÜV Rheinland hosted around 160 experts, who also visited the TÜV headquarters in Cologne. One takeaway from their stay on the Rhine: quality issues in the industry have not declined over the years. While some problems seem to have been resolved, new issues have taken their place.

As the sector matures, much of the testing has been expanded and tightened. "Some modules pass the new tests immediately," says Eckart Janknecht, module testing expert at TÜV. "But the number of failed inspections of freshly produced modules is definitely a concern."

Modules arrive defective from the factory

This suggests that modules are not undergoing sufficiently rigorous stress testing. "We often find that the rated power is not met," says Roman Alexander Brück, who heads TÜV's testing department for PV components. "Performance is between half and one percent lower. For a 650-watt module, that's a full 6.5 watts."

The reason for this is the constant price pressure that forces manufacturers to push materials and machinery to their limits. It's not uncommon for deliveries to include completely non-functioning or undersized modules. "One example is aluminium frames," says Hamza Maaroufi, who regularly inspects solar parks on TÜV Rheinland's behalf. "Modern modules are slimmed down so much that very large and heavy ones can bend under their own weight."

Inadequate screws and clamps

Along with thin frames, long-time PV specialist Wilhelm Vaaßen criticises the use of overly thin glass. "What's more, the screws and clamps being used are far too small," he says. "These components should be able to carry twice the load."

He advises investors to test the modules with the actual clamps and screws beforehand. "It's not a big expense, given the risk it eliminates," he says. "Damage down the line tends to cost far more."

Even in tracking systems, critical materials are often underdimensioned. The latest modules for solar parks measure 2.50 by 1.30 metres and deliver up

photo: Oliver Tjaden/TÜV Rheinland

Stress test for solar modules in the Cologne laboratory.

photo: Oliver Tjaden/TÜV Rheinland

Delivery of the new climate chamber to the laboratory.

to 700 watts. "If the support profile is only 40 centimetres wide, that simply won't do," warns Vaaßen.

Thin panes break quickly

Another issue is the trend toward extremely thin glass panes. Some manufacturers have reduced thickness to 1.6 millimetres. "Two panes of two-millimetre glass is standard for larger modules," reports Maaroufi. "Even at that thickness, we see breakages in the field due to bending under heavy loads."

At the end of the day, two layers of 1.6 mm glass (front and back) are not enough for large-scale installations.

With every new facility, the industry learns

The last major liability case involved brittle backsheets from modules manufactured between 2010 and 2012. At the time, high-quality films were in short supply, and some manufacturers switched to polyamide. A decade later, the backsheets had become brittle and chalked, by which point many gigawatts of solar power had been lost. Cracks formed, rendering the modules unusable.

Foils require their own certification

Certifiers have since learned from the "film epidemic." The new IEC 62788-2-1:2023 standard has been in effect since September 2023. "Many film manufacturers still aren't aware of the standard, even though it's mandatory," says Roman Alexander Brück. "If the film isn't certified, we won't certify the module either."

Test expert Eckart Janknecht advises manufacturers to contact TÜV early in the process. New films that undergo certification may require production adjustments, including pretests during development.

photo: Oliver Tjaden/TÜV Rheinland

A crane hoists the new container onto the TÜV premises in Cologne.

In the solar business for 40 years

TÜV Rheinland has contributed its expertise to the solar sector for four decades. Globally, around 1,000 experts are working to minimise technical risks in large-scale solar systems.

Europe's largest testing lab for solar modules, components, inverters – and now battery storage – is located in Cologne. Additional labs are in Bangalore (India), Shanghai (China), Taichung (Taiwan), and Pleasanton (USA).

New climate chambers

To improve testing facilities, TÜV Rheinland's solar laboratory in Cologne is expanding with two new climate chambers. They are designed to push solar modules to their limits under extreme environmental conditions.

The simulation capabilities now range from minus 70°C to plus 150°C, and from 10 to 98 percent humidity, allowing for realistic recreations of alpine snowstorms, tropical monsoons and desert heat, among others.

Extreme weather events

As extreme weather events become more frequent due to climate change, stress testing solar modules under these conditions is increasingly crucial, says Lukas Jakisch, Head of TÜV Rheinland's Solar Laboratory.

"With the new climate chambers, we can meet growing demands for comprehensive solar module testing," adds Jakisch. The chambers feature cutting-edge equipment, including the use of environmentally friendly refrigerants.

With an investment of around one million euros, TÜV Rheinland is reaffirming its long-term commitment to pioneering testing methods and sustainable progress in the solar industry.

▶ ***https://www.tuv.com/landingpage/en/pv-solar-energy/***

photo: Oliver Tjaden/TÜV Rheinland

The TÜV Rheinland solar laboratory recently received a new climate chamber.

BAYWA R.E. SOLAR TRADE

Supply chains increasingly going green

The solar retailer has a clear vision: "Renewable energy and sustainability go hand in hand," says Frank Jessel, CEO of BayWa r.e. Solar Trade in Tübingen. "As a sustainable company, we see it as our responsibility to cut CO_2 emissions across the board , whether in our internal processes or through how we manage our logistics and supply chains."

A prime example of sector coupling and sustainability is BayWa r.e.'s new, self-sufficient buildings in Tübingen, completed in 2023. These CO_2-neutral structures use eco-friendly materials and generate solar power from both the roof and façade. The energy is stored in high-performance systems, with the halls featuring UPS and concrete core activation for energy storage.

Installed with 1.3 megawatts of solar modules on the roof and facade, the warehouse generates around 1.3 million kilowatt-hours annually – almost double what's needed. The power runs industrial trucks, 54 charging stations for electric cars, and e-bikes for employees. It also provides electricity, heat, and air conditioning through innovative ceiling heating and cooling systems. The concept is further supported by six large heat pumps and a solar storage system with a one-megawatt-hour capacity.

In collaboration with long-term logistics partner Emons Logistik, BayWa r.e. Solar Trade is testing the fully electric Mercedes-Benz E Actros 300 in real-world operations. The truck, which is powered entirely by green electricity from its own solar system, has already completed several regional delivery trips. Read the full report here:

▶ ***https://www.pveurope.eu/specialized-trade/supply-chains-increasingly-going-green***

PUBLISHER'S INFORMATION

pv Europe
solar technology and applications

photovoltaik
SOLARTECHNIK FÜR INSTALLATEURE | PLANER | ARCHITEKTEN

Date of publication
December 2025

Publisher and publishing house
Gentner Energy Media GmbH
Forststr. 131, 70193 Stuttgart

PO box address:
Postfach 10 17 42, 70015 Stuttgart

Editorial team
Dipl.-Ing. Heiko Schwarzburger MA
(Editor-in-chief)
Wörther Str. 1, 10435 Berlin
phone: +49 (0) 30 / 24 53 65 49
schwarzburger@photovoltaik.eu

Thomas Finnis
(Senior Editor)
finnis@pveurope.eu

Advertising management
Bettina Mayer
Head of Media Sales
phone: +49 (0) 7 11 / 6 36 72-836
fax: +49 (0) 7 11 / 6 36 72-760
mayer@gentner.de

Order management
Melanie Schweigler (direction)
Rudolf Beck
Forststr. 131, 70193 Stuttgart
phone: +49 (0) 7 11 / 6 36 72-861
fax: +49 (0) 7 11 / 6 36 72-760
beck@gentner.de

Layout and design
GreenTomato GmbH, Stuttgart

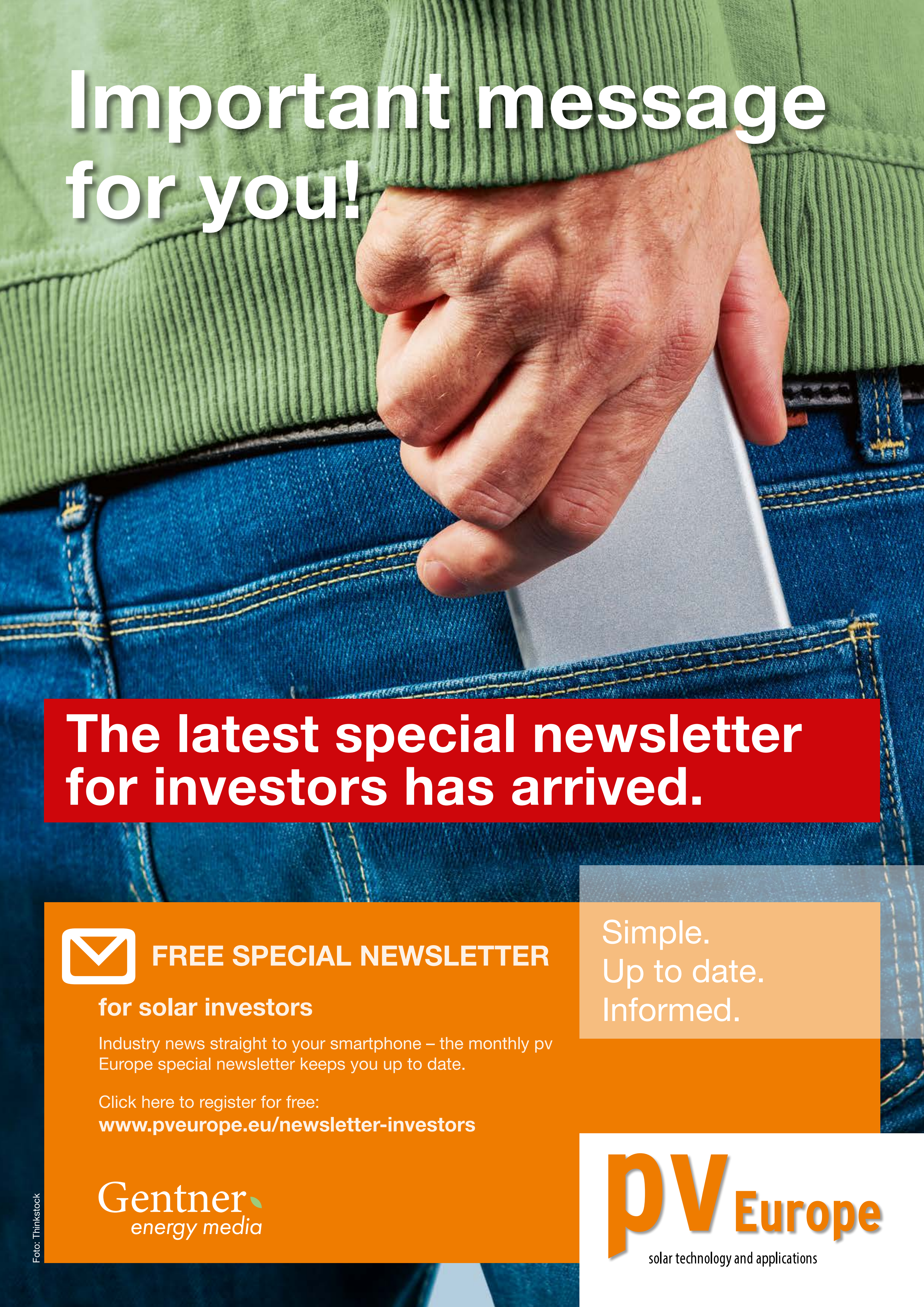


Foto: Thinkstock