

Cyber-proofing PV operation

EU cybersecurity framework and next steps



Two-thirds of the EU solar fleet is on rooftops

Segmentation of cumulative EU solar PV installations 2024

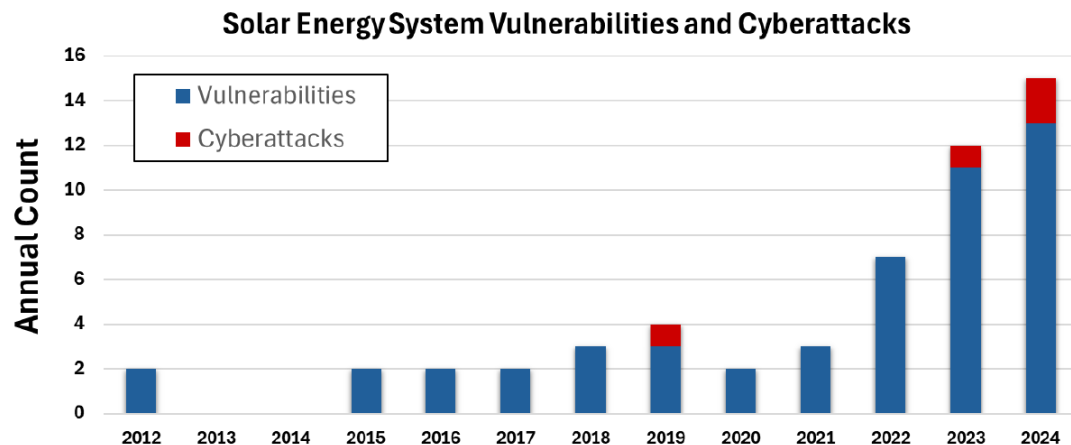
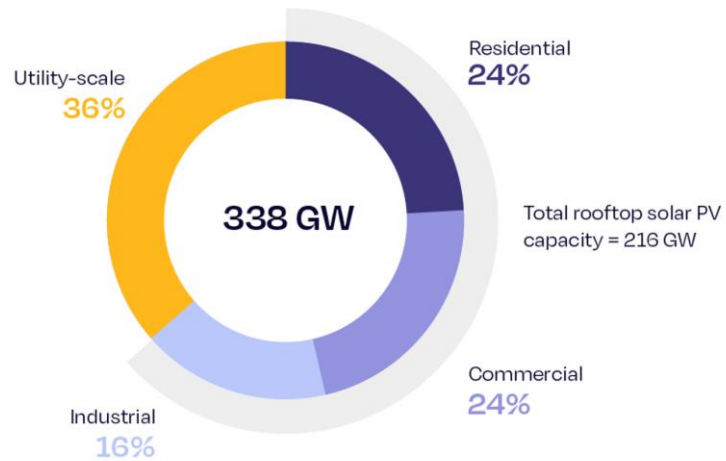


Figure 1: Solar cybersecurity reports binned by year.

DER Security. 2024. Public History of Solar Energy Cyberattacks and Vulnerabilities

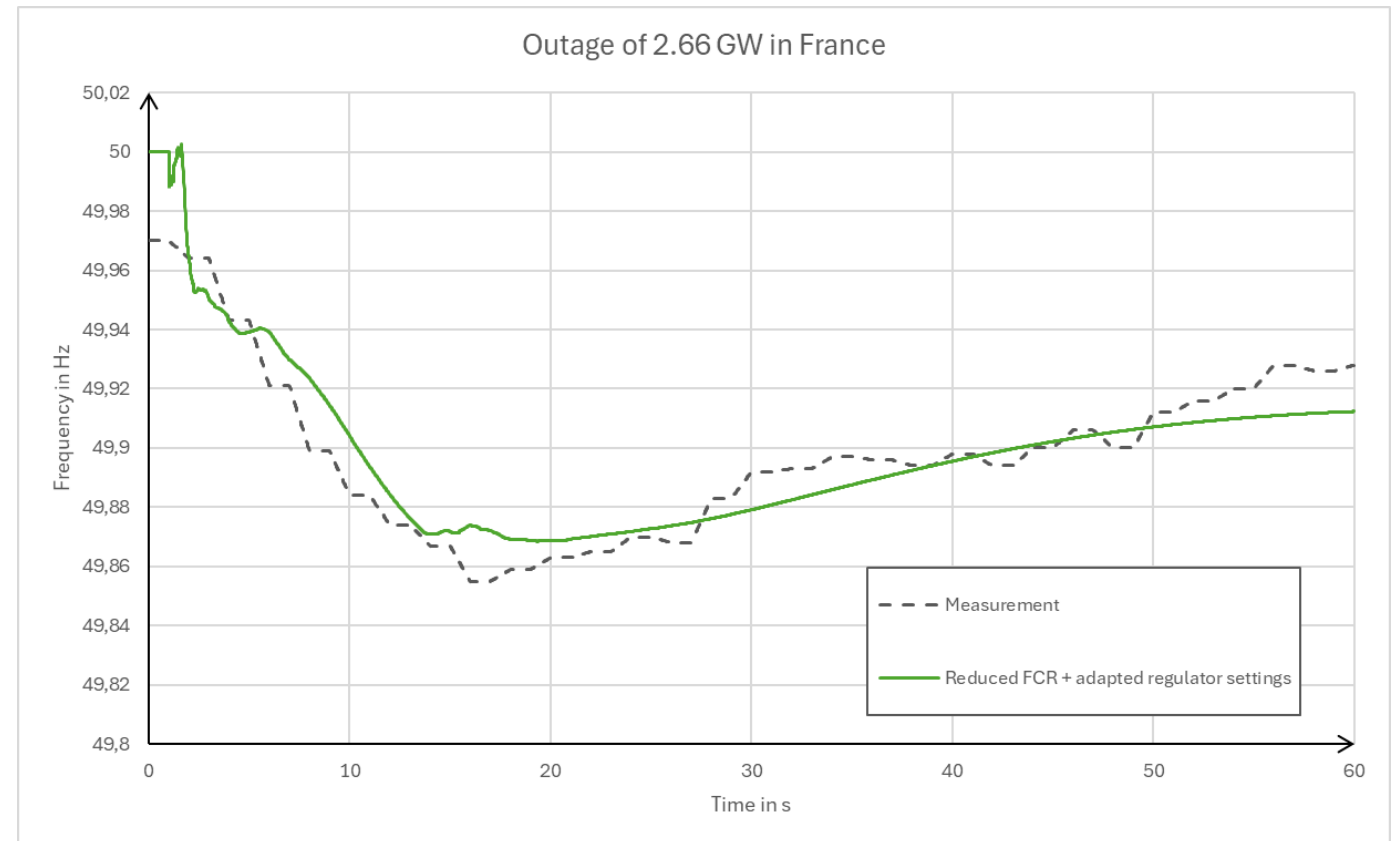
PV increases system security but cyberattacks are picking up

- **Distributed PV introduces resilience.**
Reaching critical thresholds requires controlling large numbers of assets.
- **Utility-scale assets**
 - Operate similar to traditional fossil generators.
 - Operators usually use SCADA systems to control traffic.
- **Rooftop and small utility-scale PV systems**
 - IoT-type devices without dedicated control.
 - Operate similarly to a robot cleaner or smartwatch.
 - OEM, installer, utility, etc. can access the device via IT infrastructure. Cybersecurity is in their hands.
- **Cyberattacks on PV assets have increased**
almost ten-fold in the past five years.

A cyberattack could have critical impact on the power grid

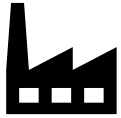


- Static and dynamic analysis on validated ENTSO-E grid models.
- Regional grid frequency stability is quite resilient.
- Simultaneous manipulation of reactive output power from large groups of inverters could lead to significant grid voltage transients.



Frequency response, example of 2 tripping NPP units in France with 2.66 GW – Measurement vs. simulation

Manufacturers
(inverters, HEMS,
etc.)



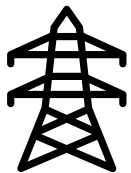
Project developer



**Asset owners,
aggregators**



Grid operators



Cyber Resilience Act (CRA)

- **Products with digital éléments, hardware and software**
- Security by design
- Lifecycle security
- Risk assessments
- Transparency and user information

Radio Equipment Directive (RED)

- **Product security for wifi-connected equipment**

NIS2

- **Applies at holding level**
- Risk management
- Reporting obligations
- Business continuity
- Corporate Accountability

Network Code on Cybersecurity [...] (NCCS)

- **Electricity-specific cybersecurity law**
- Risk assessments of high and critical-impact entities
- Minimum cybersecurity measures within “impact perimeters”

GDPR

- **Protection of personal data**
- Applies to all stakeholders

The EU framework leads world-wide, but gaps persist

- **The Cyber Resilience Act will introduce basic device cybersecurity** for smart energy devices like inverters.
- **The NIS2 Directive and the Network Code for Cybersecurity will addresses big electricity players.**
 - Like suppliers, grid operators and aggregators.
 - Basic requirements for manufacturers.
 - Exempted are service providers, installers, including for aggregated services

Many assets will need to comply with NIS2

Scope: Applies to suppliers, electricity producers (highly critical entities) and manufacturers (other critical sectors) depending on asset sizes (if spun out of the holding).

Assets outside of NIS2 scope

- No further requirements.
- From 2028, the Cyber Resilience Act will ensure basic end-point cybersecurity.
- → risk assessments, security by design, lifecycle security, transparency and user information.

Assets classified as important entities:

- >10m EUR turnover, >50 people employed.
- Also: Manufacturers (like inverter OEMs)

- **NIS2:** Risk management, reporting obligations, ensure business continuity, corporate accountability
- **Impact**
 - Increased operational costs.
 - Affects agreements with the asset operator.
 - Increased reliability and data quality.

Assets classified as essential entities: >50m EUR turnover, >250 people employed.

- Increased requirements on reporting and corporate accountability compared to important entities.
- Increased impact.

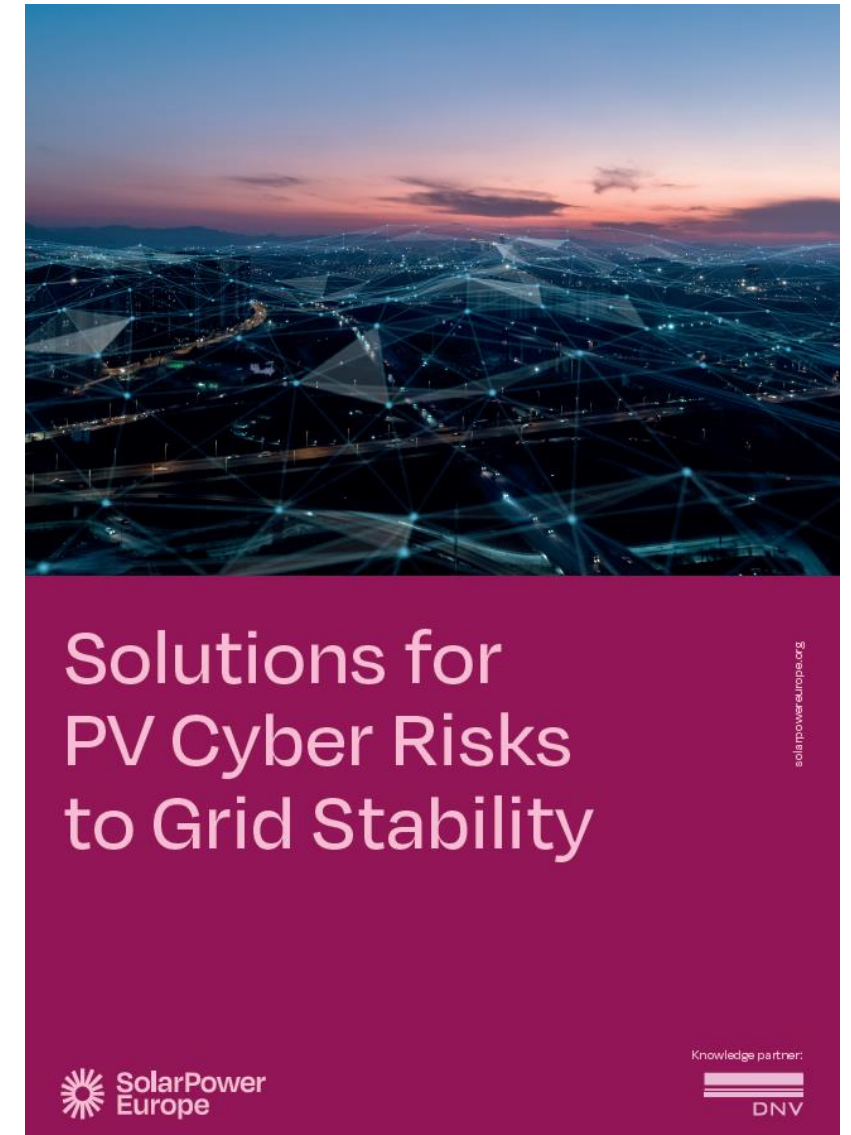
Gaps and SolarPower Europe and DNV solutions

1. Guideline defining the essential security requirements.

- Technical implementation guidance for “end-to-end” security.
- Industry-specific guidance aligned with the Cyber Resiliency Act.
- Recommendations for technical barrier solutions.

2. Limit remote access to secure jurisdictions.

- Remote access for system changes, such as inject / self-consume, grid-settings, etc.
- Delayed remote access through software updates.
- OEMs have to implement zero-trust solutions



The policy solution is at our fingertips...

Near-term solution: Network Code for Cybersecurity

1. Generation from DER is a critical process.
2. Through financial and interconnection contracts to monetize exports.

Final solution:

1. Dedicated legislation that accounts for DER, such as solar, EV charging, and large controllable loads.
2. Integration into other key legislation.

... waiting for implementation.

Q4 / 2025

- **Cyber Resilience Act** implementation
- Device classifications
- *Possibly*: Standardisation request to CEN CENELEC.

Q1 / 2026

- **EU Energy Security Strategy**
- Revision of the Security of Supply Directives

Q1 / 2027

- Identification of critical entities in the for the **Network Code for Cybersecurity**



SMA – ENERGY THAT CHANGES

Cyber Security at SMA

Dedicated to the future of energy transition

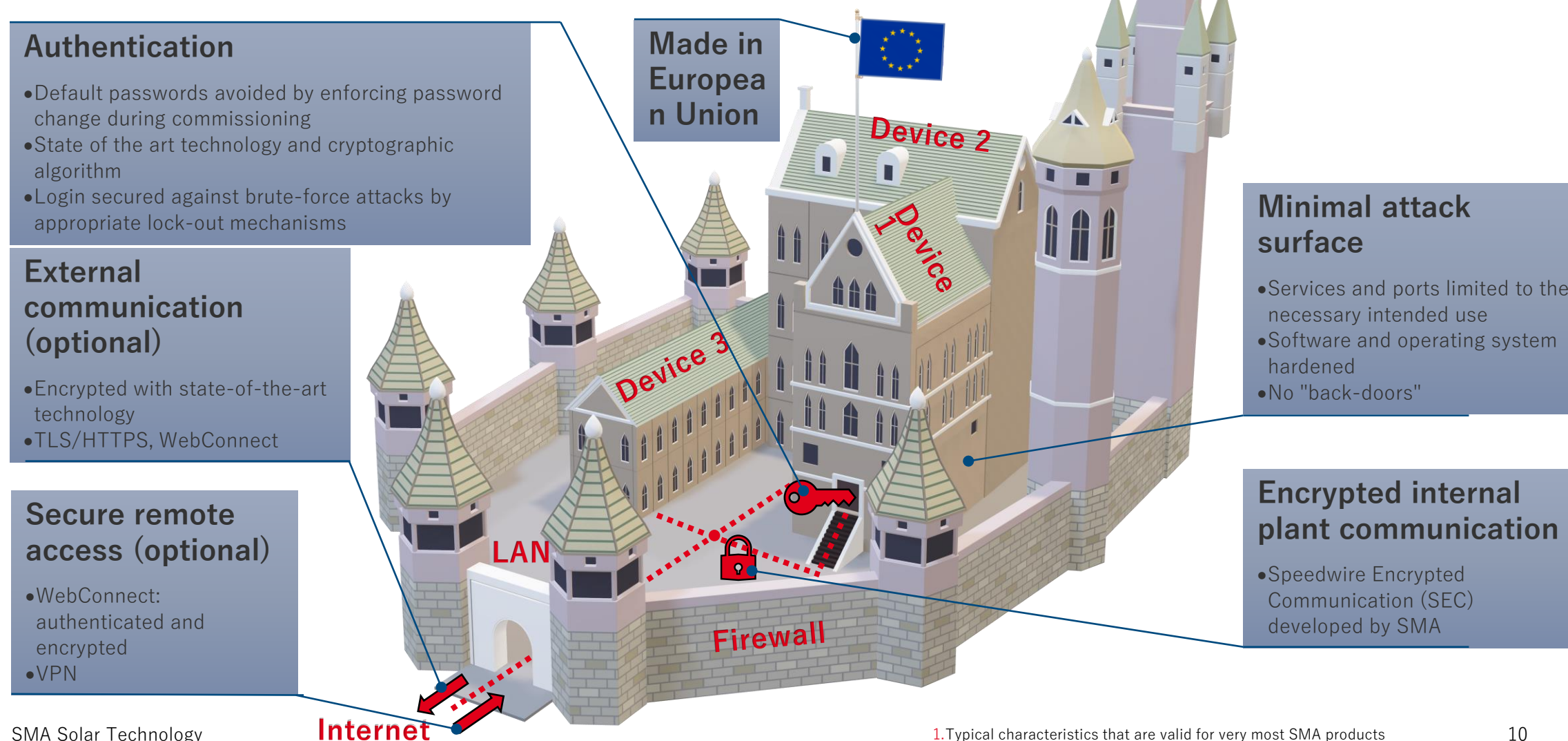


Provide a **comprehensive cyber security level**,
accomplish **constant improvement**
of our products and operations to

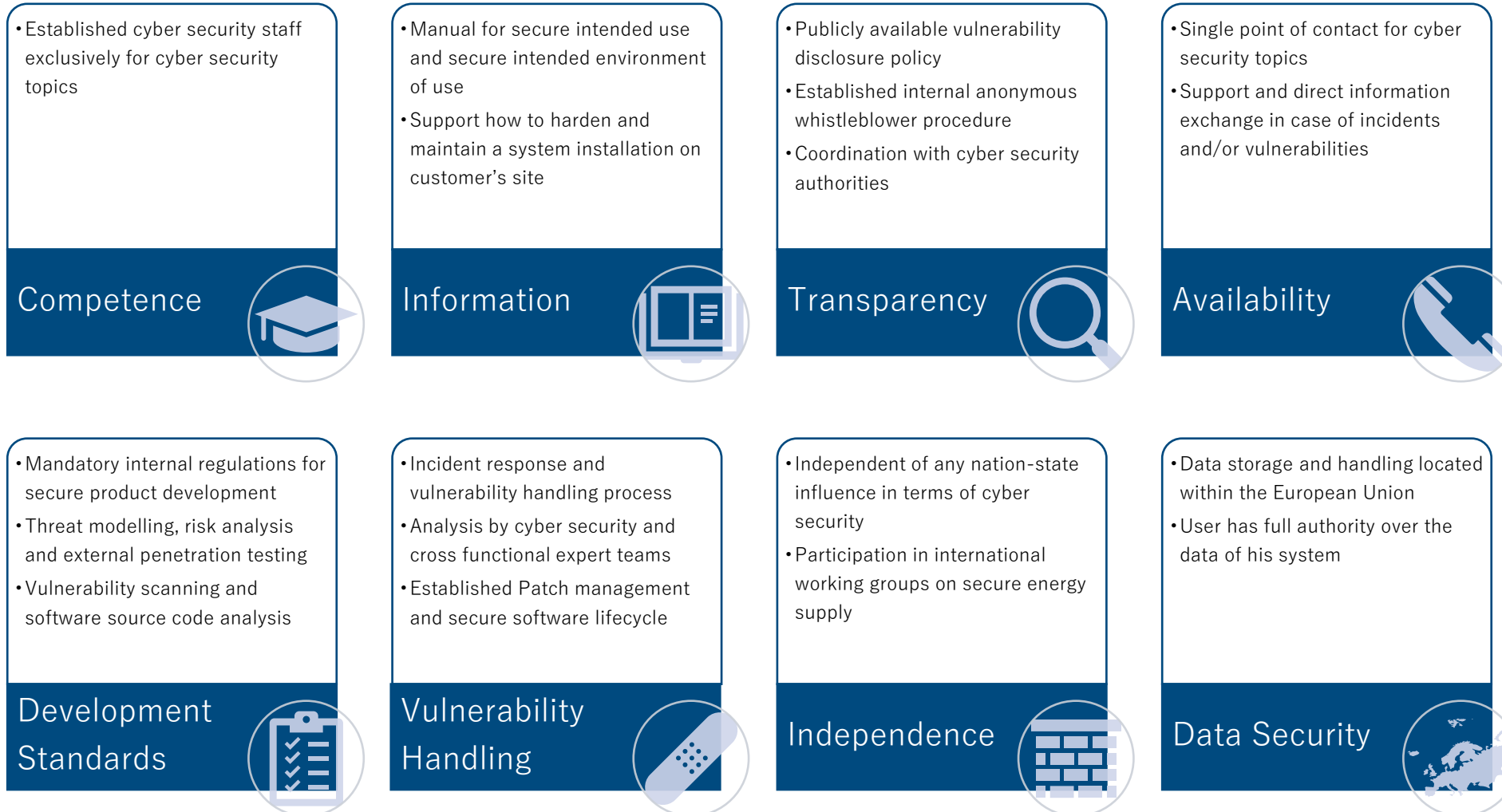
- ... protect **electricity supply**
- ... protect SMA **customers**
- ... protect **SMA** itself



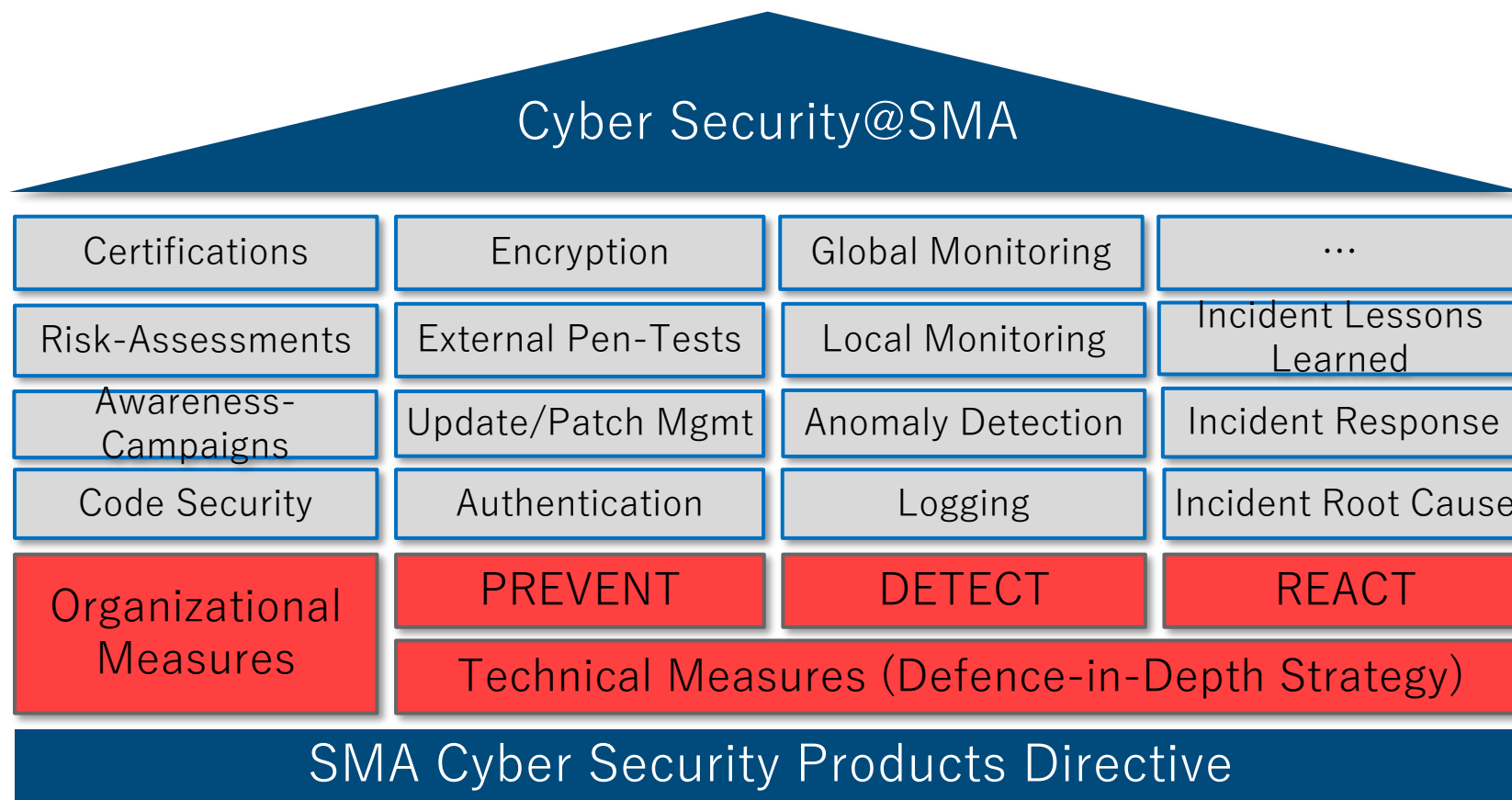
Cyber Security Characteristics of SMA Products



8 Cyber Security Characteristics of SMA



Cyber Security Measures: Holistic Defense Strategy





www.solarpowereurope.org