

## **Preventing the theft of Photovoltaic Installations**

**The components of photovoltaic installations are relatively simple to dismantle and to transport. It is not only the honest user that is attracted by the yields – PV installations are an attractive target for thieves. Owners of solar installations should follow a few simple rules, because only unsecured installations are easy prey.**

With their rising usage, valuable photovoltaic modules, fixings, and electrical components are increasingly becoming a target for organized criminal gangs. Generally, it makes little difference whether these are mounted in open spaces or on rooftops. Yet, for a comparatively low cost, installed systems can be protected against theft. It is generally recommended that power plant operators take the time to seek out individual consultation at an early stage, including from local police, in the form of a site inspection.

It should be kept in mind, that the security requirements for installations in urban estates differ from those outside of residential areas, such as those on isolated buildings, for example, on stables, or alternatively for field-based installations. With open space, ground-mounted installations, for example, insurance companies often demand that they be enclosed by way of a perimeter fence. This can then be fitted with further theft prevention measures – from acoustic signals, simple barbed wire, movement sensors, all the way up to sophisticated video surveillance. The investment costs will generally be offset through cheaper insurance policies. In this way the acquisition costs are amortized over the duration of the term.

Protection from theft should always be viewed holistically. It is important that all measures be comprehensively planned prior to construction, so that they can be effectively implemented as soon as the modules are put in place. The one hundred percent protection of PV installations can, however, never be guaranteed. However, by implementing such measures, owners significantly raise the barriers for those with an eye on their property. It makes theft more difficult, increasing the time required for dismantling the parts, and of course, the likelihood of being caught.

### **Find the right screw**

In recent years, numerous fixings have proven their merit: For example, screws can be mechanically encoded without problems or furnished with one-way drives. Also, ball bearings can be driven into the top of much-used socket-head screws as the modules are mounted. This basic approach means that the screws can no longer be loosened with a normal wrench. If, however, this should become necessary for maintenance, then you need to call an expert. This approach proves to be efficient as an anti-theft device, yet renders eventual maintenance and replacement work more difficult. Mind you, such comprehensive reconditioning works are, from my experience, a rarity. For this reason, the benefit of the approach almost always outweighs any additional expenditure.

This is also the case with specially made screws that allow the screw heads to be broken off. The screws are initially tightened with a torque wrench. If the anchoring is correct, then the

head will be broken off at a given torque value. A similar method can be similar accomplished through the 'over-tightening' of the socket head: In this case, the installer tightens the screw to such an extent, that the edges are rounded. Alternatively the screw-heads can be filled with casting resin.

Often, specially made cross-slot screws will be used: The turning of the screw is only possible using a special bit. The unscrewing, through the anti-clockwise movement is impossible because the wrench slips out of the cross-slot. The installation owner could still dismount the modules themselves, but the job is time-consuming, as each screw needs to be drilled-out individually.

### **Labeling prevents misuse**

Integrated RFID chips offer other suitable possibilities for theft protection: data chips within the solar module save the coordinates of its location. In the event of a location change, the reprogramming of coordinates is only possible by a specialist using a security code – this means that, in case of theft, the modules can no longer be used. This is a method that has been employed for smartphones and, more recently, automobiles.

Besides using fixings that normal trade tools can't unscrew, the police also recommend that modules be permanently labeled. Suitable for this task are specialized self-explanatory codes, such as the so-called Owner Identification Number, which comprise the city, street name and house number, municipality keys, and the initials of the owner – comparable to the automobile sector who use a similar process for the vehicle identification number.

Installation owners should attach such ID numbers to their modules, in such a way that they are clearly visible, and as permanent as possible. Once the installation components are labeled, it becomes very easy later on to identify the owner. All such labeling should be cleared with the manufacturer in advance to avoid any eventual problems with claiming on the warranty. It is imperative that the protection against the theft of solar modules and electrical components are not be taken lightly by plant operators. It is an unavoidable topic, and in borderline cases, serves as a guarantee that the insurance kicks in, in those cases thieves are able to overcome all of the protective measures.

Yours,  
Simone Amann