KELSEY MISBRENER
SENIOR EDITOR

CYBER ATTACKS

THREATEN SMART INVERTERS, BUT SCIENTISTS HAVE SOLUTIONS

Smart inverters expand opportunities for more distributed resources on the grid. But the internet-enabled communications that allow smart inverters to work with the grid also open the door for something sinister.

Cybersecurity issues increase as inverters get smarter, and the threat level will only rise as solar makes up more and more of the energy mix — which will accelerate even more rapidly with California's 2020 mandate of solar on all new homes.

Scientists at Lawrence Berkeley National Lab have been working on solutions to combat cybersecurity threats on smart inverters since 2016. They've found some promising solutions to inevitable hacks, but also some serious challenges that come with the growing proliferation of smart inverters.

The threats that come with smart inverters

Any device connected to the internet could be in danger of being hacked, even smart inverters. They communicate with the grid to perform voltage management functions autonomously, using internet-connected software. When used for good, this means smart inverters can regulate the voltage of power feeding into the grid in such a way that no damaging fluctuations occur. But if hackers gain control of smart inverters, they could potentially feed bad settings into the software and throw the voltage out of control, leading to brownouts or blackouts in extreme cases, according to Dan Arnold, research scientist at Berkeley Lab and one of the leads on the inverter cybersecurity project.

If only a few inverters had bad voltage settings programmed, the grid likely wouldn't feel much of an impact. But when bad software is controlling a large aggregation of smart inverters and moving their voltages simultaneously in the wrong direction, it could cause the grid to collapse.

Inverter manufacturers can take precautions to ensure cybersecurity on their end, but when the internet is involved and there aren't