CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

cybersecuritycrc.org.au

Cyber Security
Cooperative Research Centre

POWER OUT?

SOLAR INVERTERS AND THE SILENT CYBER THREAT

By Rachael Falk and Anne-Louise Brown

CONTENTS

With the support of

Australian Government
Department of Industry, Science and Resources

AusIndustry
Cooperative Research Centres Program

Disclaimer: This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

What's the problem?

As Australia accelerates adoption of renewable energy sources, new cyber security vulnerabilities are being introduced through Internet of Things (IoT) devices. Cyber security concerns about these devices, notably photovoltaic inverters (solar inverters), have recently come to the fore, and policy solutions are required to help mitigate against the cyber security threats they pose.

What's the solution?

As the number of IoT devices continues to rapidly proliferate, regulatory approaches to assessing and managing associated cyber security risks must be formulated. This is vitally important regarding IoT devices with the potential to impact critical infrastructure functions like power supply, namely solar inverters. Therefore, as a matter of priority, there is a need for the cyber security risks associated with solar inverters to be assessed.

Recommendations

- Cyber security impact assessments be completed for all solar inverters being sold in Australia, with vulnerabilities disclosed to manufacturers for remediation.
- Mandatory cyber security ratings be introduced for solar inverters and other IoT devices essential to the functioning of Australia's critical infrastructure, with a voluntary cyber security rating system applied to IoT devices more broadly.
- Solar inverters assessed as having serious cyber security vulnerabilities should be removed from sale and recalled from use, or appropriate security fixes applied if available.

INTRODUCTION

There are currently more than 15 billion operational IoT devices in the world – almost two for every person. And this number is expected to explode, with IoT proliferation set to hit 30 billion devices by 2030.[1]

These devices are central to our everyday lives – we hold them, we wear them, we watch them and, for those with home solar power systems, they are essential to keeping the lights on. But, for all the convenience these devices bring, they do not come without cyber security risks. As internet-connected devices they collect and distribute valuable data and are attractive targets for malicious cyber actors. In the case of photovoltaic inverters (solar inverters), which play an increasingly vital role in Australia's power supply, the potential ramifications could be catastrophic, presenting threats to national security, economic prosperity and even to life.

As the number of IoT devices in Australia continues to balloon, steps must be taken to ensure the cyber security and integrity of IoT devices upon which our nation's critical infrastructure relies. This policy report addresses this complex issue through the prism of solar inverter cyber security, exploring potential attack vectors and impacts of cyber incidents targeted at solar inverters. It also analyses action being taken globally in relation to IoT cyber security rating and assessment and presents several key policy approaches that would help bolster the cyber security of solar inverters sold in Australia.

What are solar inverters?

Solar inverters convert energy collected by a solar panel into the correct form of electricity for home consumption (AC/DC). They are connected to a solar energy system, which integrates smart communication and monitoring technologies to provide insights into energy production and usage.[2] Excess electricity can be fed into the grid or stored in a rechargeable battery, with batteries also providing power outage back-up.

According to the Federal Government, Australia has the highest global uptake of solar power, with about 30% of homes installed with solar systems. As of January 2022, more than three million rooftop solar PV systems had been installed across Australia,[3] with solar the fastest growing power generation type nationally, accounting for about 10% of total generation in 2020-21.[4] This trend is set to accelerate under the Federal Government's plan to reach 82% renewable energy by 2030.[5]

What are Distributed Energy Resources?

The US Government's National Renewable Energy Laboratory (NREL) defines 'distributed energy resources' (DER) as "any grid-connected energy storage and generation technologies and their associated flexible loads".[9] Common examples include solar inverters, rooftop solar units, battery storage, thermal energy storage, electric vehicles and chargers, smart meters, and home energy management technologies.[10] As noted by the Australian Renewable Energy Agency (ARENA), DER may contribute up to 45% of the nation's electricity generation capacity by 2050, meaning "organisations responsible for managing the electricity system have a massive challenge to ensure that it all works together and the electricity grid remains stable".[11]

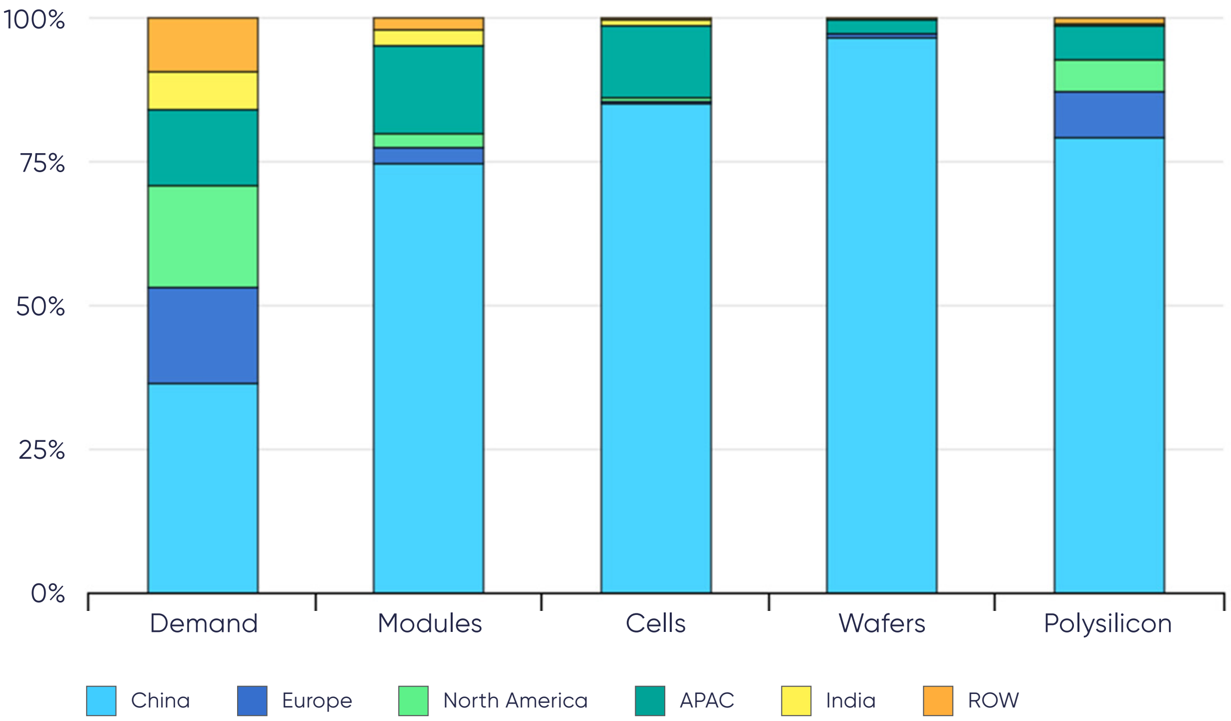
Where are inverters made?

Over the last decade the global solar energy manufacturing industry has changed significantly, with a shift from European, Japanese and US dominance to Chinese market monopolisation. This has been the result of massive investment by the Chinese Government in its domestic solar industry, equating to about US$ 50 billion. The International Energy Agency (IEA) has reported China's global share in all the manufacturing stages of solar panels exceeds 80%, and the country is home to the world's 10 top suppliers of solar power manufacturing equipment.[6]

In relation to inverters, it has been reported that China's share of the global market is about 76%, with Chinese-manufactured Huawei and Sungrow inverters producing more gigawatts of energy than European makers combined.[7] According to the IEA, "the world will almost completely rely on China for the supply of key building blocks for solar panel production through 2025 … This level of concentration in any global supply chain would represent a considerable vulnerability".[8]

Solar PV manufacturing capacity by country and region, 2021

Source: IEA



Why do solar inverters present a cyber security risk?

Traditionally, the cyber risk associated with solar inverters was low because they were not connected to the internet. However, as the popularity of smart home energy systems has boomed, this has changed, with most solar inverters now web connected for monitoring and control purposes. In turn, this has increased the cyber-attack surface of solar systems and, as internet-connected devices, solar inverters are vulnerable to a range of cyber intrusions including hacking, malware attacks, manipulation and disruption. Therefore, as the number of homes with solar systems continues to increase, the risk associated with solar inverters continues to grow.

The US Government's Office of Energy Efficiency and Renewable Energy (OEERE) has highlighted potential cyber risks associated with solar inverters. The OEERE notes several key threat vectors that could result from unpatched software, meaning data could be intercepted or manipulated, and the potential to embed malicious code in a system, that could spread more broadly across the power grid.[12] Furthermore, the NREL, has found that DER device data and communications are often unencrypted, lack secure firmware upgrades and basic authentication procedures, and are thus vulnerable to cyberattacks.[13]

The NREL notes that "the heightened cyber-physical interdependence between the electric grid and DERs allows attackers more ways to pivot between distribution resources and propagate to critical resources, which could lead to data loss or total operation failure. If vulnerabilities at the device, network, and application level of DERs are not addressed, DERs could potentially serve as attack vectors for the distribution grid".[14] Furthermore, "it is possible to disable and/or damage local grid operations by changing the frequency and/or voltage trip settings for grid interactive inverters; by disabling the underfrequency load-shedding; or by getting unauthorized access to the inverter's controls using eavesdropping, manipulation of the human-machine interface, traffic analysis, or other intrusion methods".[15]

Case study: CSCRC DER

Since 2020, the Cyber Security Cooperative Research Centre (CSCRC) has funded University of New South Wales (UNSW) research exploring cyber security threats to DER. As part of the project, researchers have examined cyber threats to solar inverters, running two simulations to illustrate how different attack vectors impact their function.

In the first simulation, command data between a solar inverter and a home energy management system was intercepted, then replayed to the solar inverter using a replay attack script. As a result, the solar inverter was able to be turned off and energy supply cut.

The second simulation involved an attack on a web service provider to which a solar inverter was connected. The web interface was disabled using a command injection technique, meaning owner access to the solar inverter was blocked, preventing remote control and monitoring.

While such attacks on one home solar system would not impact the grid more broadly, scaled, targeted simultaneous attacks could be catastrophic. CSCRC Research Director Professor Helge Janicke said that a widespread attack aimed at solar inverters had the potential to destabilise an entire power grid, leading to widespread blackouts. Conceivably such attacks could be so severe that they result in a 'black start' event, an effective restarting of a power-grid. It could take a week to recover from a black start because power plants would be incapable of turning back without reliance on an auxiliary power source.

Importantly, such scenarios are not the stuff of imagination – they have occurred.

In 2022, a Dutch hacker known as 'Jelle Ursem' gained access to solar inverter systems operated via a monitoring tool developed by Chinese manufacturer Solarman. As a result, the hacker was able to view personal customer data, create new customers and delete existing customers, find out how much electricity customers' solar panels generated via GPS coordinates, and download, adjust and upload inverter firmware.[16]

Are Chinese-made products a problem?

While concerns surrounding the cyber security of solar inverters has simmered over the last several years, in 2023 it has really come to the fore. In the US, in a hearing of the House Committee on Energy and Commerce, former Assistant Secretary of Defense Paul Stockton, directly linked solar inverter cyber risks with China-based manufacturing. Mr Stockton warned of "risks that China will exploit these products in order to conduct attacks on the grid".[17] Such concerns have been mirrored in Australia by Shadow Minister for Home Affairs and Cyber Security, Senator James Paterson, who recently stated that: "Almost 60% of Australia's smart inverters are supplied by Chinese manufacturers including Sungrow, GoodWe and Huawei – all of whom are subject to China's National Intelligence Law … Technical analysis has revealed they have exploitable flaws which are vulnerable to cyber attacks".[18]

Under Article 7 of China's National Intelligence Law: "Any organisation and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work".[19] In relation to Chinese companies providing essential goods and services to other nations – especially internet-connected devices – it is unsurprising such wording rings alarm bells. At best it is ambiguous, at worst it demands state-sanctioned interference or surveillance.

Such concerns and the national security risks associated with having internet-connected Chinese-made devices were clearly illustrated in Australia in 2012 and 2018, when the decision was made to ban 'high-risk vendors' from Australia's NBN and 5G networks.[20] As observed in 2018 by then Director-General of the Australian Signals Directorate Mike Burgess: "Our starting point was that, if 5G technology delivers on its promise, the next generation of telecommunications networks will be at the top of every country's list of critical national infrastructure … The stakes could not be higher. This is about more than just protecting the confidentiality of our information – it is also about integrity and availability of the data and systems on which we depend. Getting security right for our critical infrastructure is paramount".[21]

What are other nations doing?

IoT cyber security has become a matter of increased prominence on the global stage, as nations around the world grapple with the virtually unregulated proliferation of internet-connected devices. As a result, there have been some significant developments in this area, but Australia continues to lag.

In 2020, the Australian Government release a voluntary *Code of Practice: Securing the Internet of Things for Consumers* (the Code). The Code, which is designed for an industry audience, comprises 13 principles with emphases placed on addressing issues surrounding default passwords, vulnerability disclosure and security updates.[22] The same year, the CSCRC and CSIRO's Data 61 developed an *IoT Standards Compliance Rating* and accompanying report to help accelerate a domestic IoT cyber security rating system. Our research found consumers would be more likely to purchase an IoT device with a cybersecurity rating and assurances of low cyber security risk, recommending the Code be supported by a robust rating system.[23] Since this work was completed, significant reforms of the *Security of Critical Infrastructure Act 2018* (SOCI Act) have occurred, providing an opportunity for operation-critical IoT devices to be brought into the regime's scope.

The United States

Globally, the US has taken the most significant steps to manage IoT cyber risks. It was recently announced the US Government would introduce a cyber security certification and labelling program for IoT devices, coined the U.S. Cyber Trust Mark. According to the White House, the program, expected to be operational by 2024, would "raise the bar for cybersecurity across common devices, including smart refrigerators, smart microwaves, smart televisions, smart climate control systems, smart fitness trackers, and more".[24] The voluntary program aims to leverage stakeholder-led efforts to certify and label products, based on National Institute of Standards and Technology (NIST) criteria, focussed on unique and strong default passwords, data protection, software updates and incident detection capabilities.[25]

In 2020, the US also passed the *IoT Cybersecurity Improvement Act* (the Act). Under the Act, the NIST and Office of Management and Budget (OMB) are required to take specific steps to increase cybersecurity for IoT devices. NIST is responsible for developing and publishing standards and guidelines for the US Government on the appropriate use and management by agencies of IoT devices owned or controlled by an agency and connected to information systems owned or controlled by an agency, including minimum information security requirements for managing cyber security risks associated with such devices.[26]

The European Union

In the EU, progress has been made in relation to the passage of the *Cyber Resilience Act*, which proposes to introduce mandatory cyber security requirements for the design, development, production and sale of hardware and software products, harmonising the EU's approach to IoT cyber security regulation. The proposed legislation will apply to all products that are connected either directly or indirectly to another device or network, taking a 'whole-of-life' approach.[27] Furthermore, it would provide consumers with the ability to consider a device's cyber security features when purchasing hardware and software products.[28]

The United Kingdom

The UK's Code of *Practice for Consumer IoT Security* (the Code) takes a principles-based approach to establish steps for IoT manufacturers and other industry stakeholders to follow to help improve the security of consumer IoT products. The Code comprises 13 guidelines designed to support consumer privacy and safety and to prevent Distributed Denial of Service (DDoS) attacks being launched from poorly secured IoT devices and services.[29]

Recommendations

While renewable energy sources provide significant environmental benefits, as internet-connected devices the cyber security risks associated with solar inverters must be seriously considered. There is an opportunity to embed cyber security considerations into mandatory standards that solar inverters sold in Australia should be required to meet. More broadly, there is an opportunity for Australia to take a more hands-on approach to regulation of IoT cyber security, especially as it relates to the security of critical infrastructure.

Therefore, it is recommended that:

Cyber security impact assessments be completed for all solar inverters being sold in Australia, with vulnerabilities disclosed to manufacturers for remediation.

A cyber security impact assessment program could be established to test all solar inverters sold in Australia. Such a program would assess solar inverters for cyber vulnerabilities, which would be reported back to manufacturers for compulsory remediation, with ongoing assessment to ensure cyber vulnerabilities are appropriately addressed.

Mandatory cyber security ratings be introduced for solar inverters and other IoT devices related to the functioning of Australia's critical infrastructure, with a voluntary cyber security rating system applied to IoT devices more broadly.

Solar inverters and other IoT devices identified as being essential to the secure operation of critical infrastructure assets, as defined in the SOCI Act, should be subject to mandatory cyber security ratings. Such a rating would be based on the outcome of a cyber security impact assessment and a rating system, similar to that developed by the CSCRC and CSIRO's Data 61, applied. Furthermore, consideration should be given to banning IoT devices manufactured by high-risk vendors from critical infrastructure assets and high-value target government infrastructure. To enhance visibility into the cyber security of IoT devices more broadly, a voluntary rating program like that being established in the US could be introduced, aimed at lower risk personal IoT devices.

Solar inverters assessed as having serious cyber security vulnerabilities should be removed from sale and recalled from use.

Like any product that could expose Australians to risk, there is scope for the Federal Government to introduce a regime through which solar inverters with significant cyber security vulnerabilities could be removed from sale and recalled from use. These products would not be permitted for sale in Australia until all cyber vulnerabilities were remediated and a successful cyber security impact assessment completed, with ongoing monitoring to ensure standards are maintained.

REFERENCES

1. IoT connected devices worldwide 2019-2030 | Statista
2. What is a Solar Inverter? How to Choose a Good Inverter | Canstar Blue
3. Solar PV and batteries | energy.gov.au
4. Solar energy - Australian Renewable Energy Agency (ARENA)
5. Australia needs much more solar and wind power, but where are the best sites? We mapped them all (theconversation.com)
6. Executive summary – Solar PV Global Supply Chains – Analysis - IEA
7. The weekend read: Europe's inverted solar ambition – pv magazine International (pv-magazine.com)
8. Executive summary – Solar PV Global Supply Chains – Analysis - IEA
9. Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources (nrel.gov), P6
10. Distributed energy resources - Australian Renewable Energy Agency (ARENA)
11. Distributed energy resources - Australian Renewable Energy Agency (ARENA)
12. Solar Cybersecurity Basics | Department of Energy
13. Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources (nrel.gov)
14. Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources (nrel.gov), P2
15. Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources (nrel.gov), P6
16. Dutch agency investigates cybersecurity of PV inverters after hack – pv magazine International (pv-magazine.com)
17. US electric grid facing cyber risks from renewable energy tech | SC Media (scmagazine.com)
18. Statement on Labor's rush to renewables leaves Australia vulnerable to catastrophic cyber attack (senatorpaterson.com.au)
19. Huawei and the ambiguity of China's intelligence and counter-espionage laws | The Strategist (aspistrategist.org.au)
20. How China-Australia's relationship deteriorated after Huawei's 5G infrastructure ban (smh.com.au)
21. Mike Burgess, director-general ASD, on coming out from the shadows (themandarin.com.au)
22. Code of Practice, Securing the Internet of Things for Consumers (homeaffairs.gov.au)
23. IoT Code of Practice – Standards Compliance Rating
24. Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers | The White House
25. Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers | The White House
26. IoT Cybersecurity Improvement Act of 2020 | Congress.gov | Library of Congress
27. Cyber resilience act: member states agree common position on security requirements for digital products - Consilium (europa.eu)
28. Cyber resilience act: member states agree common position on security requirements for digital products - Consilium (europa.eu)
29. Code of Practice for consumer IoT security - GOV.UK (www.gov.uk)

Cyber Security Cooperative Research Centre

cybersecuritycrc.org.au