The Current State of Threat Modelling Pertaining to IoT Grid-Connected Rooftop Solar Inverters in Queensland, Australia

Subject: Research Methods and Professional Practice (April 2024)

Assignment: Literature Review

Student Name: Michael Botha

Student Number: 12686220

Programme: MSc Computer Science

Contents

1.) Introduction

Countries around the world are making a concerted effort to transition the traditional paradigms of electricity generation to that which is more aligned with a renewable energy model (Abnett et al., 2023). Part of this involves the use of Distributed Energy Resources (DER) where residential rooftop solar power plays an important role (AEMC, N.D.). A critical facet of these systems are inverters which comprise of various functional components including an embedded computer system (Microchip, N.D.). Furthermore, inverters are often monitored and supported through a Wi-Fi or cellular network connection making them an Internet of Things (IoT) device (Australian Government, N.D.; Oracle, N.D).

The state of Queensland in Australia has the highest rooftop solar take-up rate in the world (Simshauser et al., 2022). Therefore, it is important to review literature covering the possible cyber security risks within this region (National Cyber Security Centre, 2023a). Specifically, whether significant threat modelling has been produced (National Cyber Security Centre, 2024). Furthermore, by focussing on this highly solar dense area, more information may be attained which is relevant to the global DER sector.

Firstly, inverter system components will be explored, then what threats pertain to these, and finally what can be done to protect this domain (National Cyber Security Centre, 2024; Braiterman et al., N.D.; Kidd & Raza, 2024).

2.1) The Inverter System and its Domains

Yan and Li (2023) present a good diagrammatic representation of the physical elements of interest, useful for assessing the various applicable domains. Although there is sufficient granularity with regards to the Inverter, the diagram is too high level on the external system facets. Additionally, there is no clear acknowledgement of the software complexities. More functional insight is provided by Tuyen et al. (2022) who mention the areas of concern as they pertain to the important features of monitoring and control. Although Rekeraho et al. (2024) discuss the more general theme of cybersecurity in IoT-based renewable energy they do highlight the typical architectural elements of IoT systems.

The cyber-physical nature of these systems is stressed directly or by inference in many of the sources reviewed. For instance, Zografopoulos et al. (2023) point out the criticality of considering the cyber-physical features of DER. Moreover, Falk & Brown (2023) as well as Musleh et al. (2024) mention how the interrelationship of the cyber and physical domains produces an extended area of influence, being the electrical distribution grid that the inverters are connected to. The energy system is part of the critical infrastructure of a country, therefore, requires special attention (Fortinet, N.D.).

In terms of remote access that might be required to an inverter Ravi et al. (2021) and the Australian Government (N.D.) list the key stakeholders as: inverter manufacturers, the Distributed Network Service Provider (DNSP), building management systems, and the Australian Energy Market Operator (AEMO). There is no clear description in any of the available documentation regarding the infrastructure layout of these domains, however, one can assume the use of standard Internet equipment and web applications. Additionally, which of the stakeholder connections may be implemented in any inverter installation is not lucid, as this is state and organisation dependent. Moreover, this is still an area that is being assessed by the relevant parties, although, it is expected that more remote grid operations will be needed (Australian Renewable Energy Agency, 2023; Poggioli, 2024). Further to the stakeholder connections, Dafalla et al. (2020) argue that other IoT devices sharing the same home network as the inverter could also influence the security posture of the setup.

Inverter brands is also a topic of relevance as different organisations maintain varying cyber security and product standards, besides the fact that the devices could be designed and constructed using alternative methods and electronic components respectively (Musleh et al., 2024; Falk & Brown, 2023; Chirgwin, 2023). Falk & Brown (2023) explain how some countries have policies that force organisations to support national intelligence programs via their products.

Although there is various information pertaining to how an inverter system looks and what the various domains are that pertain to such, specifically concerning the physical and electrical facets, certain areas are not well represented in the literature. For instance, the software architectures that undergird this environment, and the scope that different cyber users of the devices should get (National Cyber Security Centre, 2024). Additionally, there is no lucid data flow between processing endpoints presented, despite the fact that Internet connectivity is one of the biggest cyber concerns (National Cyber Security Centre, 2024).

2.2) Applicable Threats

Various threats were presented in the literature, however, only a few sources presented any formal threat modelling techniques. Rahim et al. (2023) mention that by trying to achieve standard threat modelling outcomes, where the STRIDE and DREAD frameworks were used in the process, 220 threats were identified. However, only 20 were used in their assessment. Another area of concern is that these frameworks were specifically designed for Information Technology (IT) systems and are not necessarily considerate of cyber-physical aspects (Rahim et al., 2023). One can assume that many of the applicable threats will be accommodated via an IT focus, but this is not a holistic approach. Rahim et al. (2023) also do not focus on the solar roof-top environment but rather the integration of solar farms. Zografopoulos et al. (2023) present a handful of threats and focus on the general DER environment. A point of note is their use of MITRE’s ATT&CK for Industrial Control Systems (ICSs) framework which shifts the focus to a more appropriate context.

The most severe threat presented was that of a broad attack across multiple inverters within a focussed region, where the concern is grid instability which could result in localised or even wide-ranging blackouts (Dafalla, 2020; Falk & Brown, 2023; Poggioli, 2024; Australian Cyber Security Magazine, 2023). A threat actor could achieve this in multiple ways, where one method would be simultaneously disconnecting inverters from the grid, or connecting inverters to the grid, perhaps by switching them off or on respectively (Musleh et al., 2024). Other techniques involve altering configuration parameters causing the inverters to disconnect through an electrical trip, or to operate in a mode which could stress the grid (Falk & Brown, 2023). This threat is extremely relevant to higher-density solar deployments such as that found in Queensland, Australia, because of the high reliance on solar generation by the greater energy market (Musleh et al., 2024; Simshauser et al., 2022).

Some of the generally heightened threats within this industry include:

- Attacks by state actors (Ratnam et al., 2020; Australian Cyber Security Magazine, 2023)
- Supply chain attacks targeting electronic components or firmware to cause device failures (Rekeraho et al., 2024; Zografopoulos et al., 2023; Falk & Brown, 2023)
- Denial of Service attacks to take inverters offline so that their remote monitoring is impossible (Tuyen, 2022)

Additionally, Zografopoulos et al. (2023) raises the threat of limited processing power on the embedded computers of these devices.

Overall, many threats are presented using multiple assessment techniques. However, a gap is presented in that no attack tree models and paradigms are used (National Cyber Security Centre, 2023b). This is an important technique as it considers the various steps an attacker or situation would take to reach an ultimate goal (National Cyber Security Centre, 2023b). Thereby, linking various aspects and providing a holistic approach (National Cyber Security Centre, 2023b). Many threats are also focussed on the inverter and not on the cloud and industry services that remotely connect to them, which is certainly an oversight that requires remedy. Attacks can also be launched from an inverter towards these centralised data centres, resulting in severe consequences.

2.3) Mitigation Strategies

As a foundational requirement for a secure system the general consensus of the literature is for governments to put regulations surrounding solar systems in place (Falk & Brown, 2023; Musleh, 2024; Poggioli, 2024; Australian Cyber Security Magazine, 2023). For instance, Falk & Brown (2023) representing the Australian context suggest that compulsory cyber security ratings should be implemented for inverters. They even go as far as saying that banning of high-risk vendors should be considered (Falk & Brown, 2023). However, regulation is sure to drive up the costs associated with these systems, which inevitably would lead to consumers pulling back on investment (National Association of Manufacturers, 2023). Which raises an interesting point: how can solutions be implemented for systems forming part of critical infrastructure yet owned and maintained by private persons from the general public. Future studies will need to consider this thoroughly when suggesting mitigation solutions.

Various relevant standards that use best practices pertaining to IT security, communication protocols, IoT, cyber-physical systems and the like have already been created (Ravi et al., 2021; Musleh, 2024; Li & Yan, 2023). Some of these standards were created directly for the Australian context (Ravi et al., 2021). A concern is that although many of these standards exist, most of them have not been implemented (Ravi et al., 2021). Additionally, many inverters using insecure protocols have already been deployed (Ravi et al., 2021; Zografopoulos, 2023). In an Australian based report

Australia is said to be lagging other advanced countries such as the United States of America and the United Kingdom with regards to the application of IoT cyber security standards (Falk & Brown, 2023). However, the government is currently driving projects and research to kerb this (Kaufmann, 2024).

Due to the fluidity of the environment and the many variables some have suggested using Intrusion Detection Systems (IDSs) to monitor for anomalies at the cyber and physical levels using various techniques (Li & Yan, 2023; Tuyen et al., 2022). Which seems intuitive, however, one might question how capable an embedded computing device is at running the necessary algorithms. Furthermore, the use of Artificial Intelligence schemes has been suggested, but again the computing and networking throughput capabilities of inverters could be an adoption barrier (Tuyen et al., 2022). One important security aspect that seems to have received little attention in the available literature is the physical protection of inverter devices (National Institute of Standards and Technology, 2020). Most rooftop solar installations in Queensland leave systems relatively accessible to individuals with nefarious intent. Hypothetically, a sufficiently coordinated effort by a big group of people could physically disable a problematically significant number of units (National Institute of Standards and Technology, 2020).

Overall, there is no single solution presented, however, by the application of multiple efforts significant mitigation can be achieved (Rekeraho et al., 2024). There is certainly a lot of research required in terms of guaranteeing the same level of security that traditional state-owned generation facilities provide.

3) Conclusion

This review aimed to ascertain the cybersecurity posture of IoT grid-connected rooftop solar inverters in the state of Queensland in Australia, specifically as it pertains to the current threat modelling which has been performed. The findings show that although the relevant physical equipment and boundaries have been captured, there remains areas which are unknown in terms of software features and capabilities residing at the central data centres connecting to multiple inverters. Additionally, the responsibility demarcation of the significant stakeholders is not clear.

In terms of applicable threats general IT concerns exist, however, due to the cyber-physical nature of the systems in question, as well as the critical infrastructure connected to, the most important threat is that concerning grid energy supply. In this instance, if a largescale attack were to be successful at simultaneously affecting a significant number of inverters connected to the grid, it could become unstable and cause a dire situation. It was noted that there has been no attack tree modelling performed, which is an important technique required when threat modelling.

Concerning controls put in place the government is working on regulations that would improve the industry, however, this comes with various challenges. For example, how the responsibility for different aspects of the system will fall when the relevant parties are both government and individual members of the public. Regarding technical solutions on the horizon AI and other advanced algorithms have been proposed, but these face the underlying computational limitations of IoT devices.

It is proposed that future studies look at attack tree modelling and consider the various paths a threat actor might take to achieve a specific attack goal. Specifically, a large-scale grid-focused attack which incorporates the mentioned data centres. Moreover, a survey needs to be performed on who the parties of interest are that intend on connecting to inverters, and what their security posture is like. Lastly, various detection and prevention algorithms should be run on standard inverter embedded computing architectures to see what performance can be achieved.

4.) References

Abnett, K., Volcovici, V., Stanway, D. (2023) Countries promise clean energy boost at COP28 to push out fossil fuels. Available from: https://www.reuters.com/sustainability/climate-energy/over-110-countries-set-join-cop28-deal-triple-renewable-energy-2023-12-02/ [Accessed 23 May 2024].

AEMC. (N.D.) Distributed energy resources. Available from: https://www.aemc.gov.au/energy-system/electricity/electricity-system/distributed-energy-resources#:~:text=Distributed%20energy%20resources%20(DER)%20refers,battery%20storage [Accessed 23 May 2024].

Australian Cyber Security Magazine. (2023) Cyber Vulnerabilities Identified in Australia’s Rooftop Solar Systems. Available from: https://australiancybersecuritymagazine.com.au/cyber-vulnerabilities-identified-in-australias-rooftop-solar-systems/#:~:text=%E2%80%9CSolar%20inverters%20are%20now%20web,%2C%20including%20hacking%2C%20malware%20attacks%2C [Accessed 13 May 2024].

Australian Government. (N.D.) Monitor your solar system. Available form: https://www.energy.gov.au/solar/use-your-solar-system/monitor-your-solar-system [Accessed 23 May 2024].

Australian Renewable Energy Agency. (2023*) Common Smart Inverter Profile – Australia*. Available from: https://arena.gov.au/assets/2021/09/common-smart-inverter-profile-australia.pdf [Accessed 13 May 2024].

Braiterman, Z., Shostack, A., Marcil, J., de Vries, S., Michlin, I., Wuyts, K., Hurlbut, R., Schoenfield, B., Scott, F., Coles, M., Romeo, C., Miller, A., Tarandach, I., Douglen, A., French, M. (N.D.) Threat Modeling Manifesto. Available from: https://www.threatmodelingmanifesto.org/ [Accessed 09 June 2024].

Chirgwin, R. (2023) Solar inverter cyber security standards coming: Addressing security of critical infrastructure. Available from: https://www.iothub.com.au/news/solar-inverter-cyber-security-standards-coming-601869 [Accessed 13 May 2024].

Clean Energy Council. (2021) New Inverter Standard to Improve Grid Stability. Available from: https://www.cleanenergycouncil.org.au/news/new-inverter-standard-to-improve-grid-stability [Accessed 24 May 2024].

Dafalla, Y., Liu, B., Hahn, D., Wu, H., Ahmadi, R., Bardas, A. (2020) Prosumer Nanogrids: A Cybersecurity Assessment. *IEEE Access* 8: 131150-131164. DOI: 10.1109/ACCESS.2020.3009611.

Falk, R., Brown A. (2023) *Solar Inverters and Silent Cyber Threat. Cyber Security Cooperative Research Centre*. Available from: https://cybersecuritycrc.org.au/sites/default/files/2023-11/3320_cscrc_powerout_art_web.pdf [Accessed 13 May 2024].

Fortinet. (N.D.) What is Critical Infrastructure Protection (CIP). Available from: https://www.fortinet.com/resources/cyberglossary/critical-infrastructure-protection [Accessed 24 May 2024].

Institute for Energy Research. (2022) Rooftop solar in South Australia Causes Grid Issues. Available from: https://www.instituteforenergyresearch.org/renewable/solar/rooftop-solar-in-south-australia-causes-grid-issues/ [Accessed 24 May 2024].

Kaufmann, S. (2024) Enhancing Data Security in a changing energy landscape. Available from: https://www.csiro.au/en/news/All/Articles/2024/April/energy-transition-and-data-security [Accessed 13 May 2024].

Kidd, C., Raza, M. (2024) What is Theat modelling. Available from: https://www.splunk.com/en_us/blog/learn/threat-modeling.html [Accessed 09 June 2024].

Li, Y., Yan, J. (2023) Cybersecurity of Smart Inverters in the Smart Grid: A Survey. *IEEE Transactions on Power Electronics* 38(2): 2364-2383, DOI: 10.1109/TPEL.2022.3206239.

Microchip. (N.D.) Solar Inverters: Designing Solar Inverters. Available from: https://www.microchip.com/en-us/solutions/sustainability/solar-inverters [Accessed 24 May 2024].

Musleh, A., Ahmed, J., Ahmed, N., Xu, H., Chen, G., Kerr, S., Jha, S. (2024) Experimental Cybersecurity Evaluation of Distributed Solar Inverters: Vulnerabilities and Impacts on the Australian Grid. *IEEE Transactions on Smart Grid*. DOI: 10.1109/TSG.2024.3393439.

National Association of Manufacturers. (2023) Regulatory Onslaught Costing Small Manufacturers More Than $50,000 Per Employee. Available from: https://nam.org/regulatory-onslaught-costing-small-manufacturers-more-than-50000-per-employee-29236/?stream=series-press-releases [Accessed 14 June 2024].

National Cyber Security Centre. (2023a) Risk Management: The fundamentals and basics of cyber risk. Available from: https://www.ncsc.gov.uk/collection/risk-management/the-fundamentals-and-basics-of-cyber-risk [Accessed 25 May 2024].

National Cyber Security Centre. (2023b) Risk Management: Using Attack trees to understand cyber security risk. Available from: https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-understand-cyber-security-risk [Accessed 25 May 2024].

National Cyber Security Centre. (2024) Risk Management: Threat Modelling. Available from: https://www.ncsc.gov.uk/collection/risk-management/threat-modelling [Accessed 25 May 2024].

National Institute of Standards and Technology. (2020) Security and Privacy Controls for Information Systems and Organizations. *NIST Special Publication* 800-53 Revision 5. DOI: https://doi.org/10.6028/NIST.SP.800-53r5.

Oracle. (N.D.) What is IoT. Available from: https://www.oracle.com/au/internet-of-things/what-is-iot/ [Accessed 23 May 2024].

Poggioli, L. (2024) Fixing the Gap in Australia’s Cybersecurity Legislation. Available from: https://australiancybersecuritymagazine.com.au/fixing-the-gap-in-australias-cybersecurity-legislation/ [Accessed 13 May 2024].

Rekeraho, A., Cotfas, D., Cotfas, P., Balan T., Tuyishime, E., Acheampong, R. (2024) Cybersecurity challenges in IoT-based smart renewable energy. *International Journal of Information Security*, 2024(23):101–117. DOI: https://doi.org/10.1007/s10207-023-00732-9.

Rahim, F., Ahmad, N., Magalingam, P., Jamil, N., Cob, Z., Salahudin, L. (2023) Cybersecurity Vulnerabilities in Smart Grids with Solar Photovoltaic: A Threat Modelling and Risk Assessment Approach. *International Journal of Sustainable Construction Engineering and Technology.* 14(3): 210-220.
DOI: https://doi.org/10.30880/ijscet.2023.14.03.018.

Ratnam, E., Baldwin, K., Mancarella, P., Howden, M., Seebeck, L. (2020) Electricity system resilience in a world of increased climate change and cybersecurity risk. *The Electricity Journal* 33(9): 1-6. DOI: https://doi.org/10.1016/j.tej.2020.106833.

Ravi, R., Tripathy, D., Pathirana, V., Seifollahi, S., Jolfaei, A., Zhao, H. (2021) Secured Integration of Distributed Energy Resources into Energy Ecosystems. *2021 31st Australasian Universities Power Engineering Conference (AUPEC)*. pp. 1-6. DOI: 10.1109/AUPEC52110.2021.9597747.

Simshauser, P., Nelson, T., Gilmore, J. (2022) The sunshine state: cause and effects of mass rooftop PV take-up rates in Queensland. *Centre for Applied Energy Economics & Policy Research: Working Paper Series* 2022(05). Available from: https://www.griffith.edu.au/__data/assets/pdf_file/0033/1799250/No.2022-05-Queensland-Solar-Cause-and-effects-of-mass-rooftop-solar-PV-take-up-rates.pdf [Accessed 25 May 2024].

Tuyen, N., Quan, N., Linh, V., Van Tuyen, V., Fujita, G. (2022) A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy. *IEEE Access* 10: 35846-35875. DOI: 10.1109/ACCESS.2022.3163551.

U.S. Department of Energy. (N.D.a) Solar Photovoltaic Technology Basics. Available from: https://www.energy.gov/eere/solar/solar-photovoltaic-technology-basics [Accessed 23 May 2024].

U.S. Department of Energy. (N.D.b) Solar Photovoltaic System Design Basics. Available from: https://www.energy.gov/eere/solar/solar-photovoltaic-system-design-basics [Accessed 23 May 2024].

Zografopoulos, I., Hatziargyriou, N., Konstantinou, C. (2023) Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations. *IEEE Systems Journal* 17(4): 6695-6709. DOI: 10.1109/JSYST.2023.3305757.