4E Efficient, Demand Flexible Networked Appliances EDNA

Cybersecurity for Demand Flexible Appliances

NOVEMBER 2024

Technology Collaboration Programme
by iea

The Technology Collaboration Programme on Energy Efficient End-Use Equipment (4E TCP), has been supporting governments to co-ordinate effective energy efficiency policies since 2008.

Fourteen countries and one region have joined together under the 4E TCP platform to exchange technical and policy information focused on increasing the production and trade in efficient end-use equipment. However, the 4E TCP is more than a forum for sharing information: it pools resources and expertise on a wide a range of projects designed to meet the policy needs of participating governments. Members of 4E find this an efficient use of scarce funds, which results in outcomes that are far more comprehensive and authoritative than can be achieved by individual jurisdictions.

The 4E TCP is established under the auspices of the International Energy Agency (IEA) as a functionally and legally autonomous body.

Current members of 4E TCP are: Australia, Austria, Canada, China, Denmark, the European Commission, France, Japan, Korea, Netherlands, New Zealand, Switzerland, Sweden, UK and USA.

Further information on the 4E TCP is available from: **www.iea-4e.org**

The Efficient, Demand Flexible Networked Appliances Platform of 4E (EDNA) provides analysis and policy guidance to members and other governments aimed at improving the energy efficiency and demand flexibility of connected devices and networks.

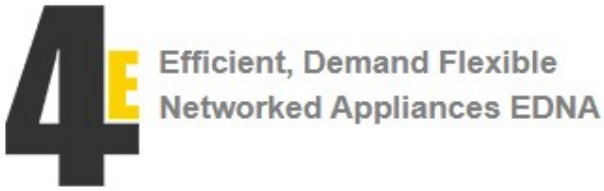
Further information on EDNA is available from: **www.iea-4e.org/edna**

This report was commissioned by the EDNA Platform of the 4E TCP and authored by Strategic Energy Ltd in partnership with CyberPractice.io Pty Ltd. The views, conclusions and recommendations are solely those of the authors and do not state or reflect those of EDNA, the 4E TCP or its member countries.

Views, findings and publications of EDNA and the 4E TCP do not necessarily represent the views or policies of the IEA Secretariat or its individual member countries.

DF5 Cybersecurity for Demand Flexible Appliances

Prepared for:



Prepared by:

Strategic Energy Ltd in partnership with CyberPractice.io Pty Ltd

November 2024

StrategicEnergy

info@strategicenergy.co.nz

cyberpractice.io

info@cyberpractice.io

Executive Summary

Cybersecurity in the context of demand-flexible networked appliances is an important issue globally as the number of connected devices and total associated load is already large and is increasing rapidly.

In order to effectively manage and optimize electricity supply networks, electricity organizations utilize the opportunity to manage millions of connected Demand Flexible Appliances (DFA) such as residential photovoltaic systems and batteries, electric vehicle chargers and home air conditioning systems. This ability to digitally access these DFA introduces a level of risk arising from the opportunity for individuals and organizations with dishonest intentions to cause potential disruption to electricity supply, electricity price or to bring about other consequences such as data theft.

This report focuses mainly on issues that have the potential to disrupt the electricity supply system. This work has included researching current and potential future threats in relation to demand flexible networked appliances, investigating what is being done, or considered, by relevant organizations and jurisdictions, and summarizing the issues that policy makers should consider in relation to minimizing and mitigating cybersecurity risks.

The research involved in this project comprised literature/internet based research, discussions with a number of stakeholders and was supplemented by the authors' knowledge and experience of this subject.

The DFA cybersecurity landscape is complex and rapidly evolving. As DFA systems become increasingly integrated into our energy infrastructure, they bring with them new vulnerabilities and challenges. Addressing these issues requires a multi-faceted approach, involving standardization efforts, improved visibility and control mechanisms, robust security measures, and adaptive regulatory frameworks.

Many jurisdictions around the world are facing a similar situation of increasing electricity demand and increasing levels of DFA and the need to manage electricity supply and demand in an optimal way.

Original equipment manufacturers (OEMs) that produce devices such as photovoltaic panels, residential storage batteries, electric vehicle chargers etc are generally global companies selling into many different markets, so an international approach is required to address these products.

There are numerous examples of legislation, standards, guidelines and other initiatives that have been established around the world to help address cybersecurity risks in relation to devices connected to electricity grids. Some mechanisms are Government legislation or national/ international standards that must be complied with. Other useful initiatives such as Cyber Trust marks and the ioXt Alliance are voluntary schemes.

DFA cybersecurity is a complex, multifaceted challenge that sits at the intersection of technology, policy, and market dynamics. As DFA continue to proliferate and play an increasingly critical role in

our energy systems, the imperative to address these cybersecurity challenges becomes ever more urgent.

Key themes that emerge from the analysis include:

- The need for a risk-based, adaptive approach to security that can keep pace with the rapid evolution of both DFA technologies and cyber threats.
- The importance of international cooperation and standardization to address the global nature of DFA supply chains and cyber threats.
- The challenge of balancing security requirements with the need for interoperability, innovation, and cost-effectiveness in DFA systems.
- The critical role of human factors, including consumer awareness and industry expertise, in maintaining robust cybersecurity postures.
- The necessity of developing comprehensive, DFA-specific cybersecurity frameworks that can guide policy, standards, and industry practices.

In the future, it is clear that addressing DFA cybersecurity will require a collaborative effort involving policymakers, industry stakeholders, researchers, and consumers. The path ahead involves not just technical solutions, but also the development of robust governance frameworks, economic models that incentivize security, and educational initiatives to build cybersecurity awareness and expertise across the DFA ecosystem.

The security of our evolving, distributed energy systems is paramount not just for the stability of our power grids, but also for the broader economic and social systems that depend on reliable, secure energy. As we continue to harness the transformative potential of DFA, ensuring their cybersecurity must remain a top priority, driving innovation, collaboration, and continuous improvement in our approach to protecting these critical systems.

Key policy options for improving DFA cybersecurity include:

- Implement a Global Public Key Infrastructure (PKI) for DFA.
- Develop Risk-Based Cybersecurity Standards for DFA.
- Establish an International DFA Cybersecurity Information Sharing Platform.
- Mandate Secure-by-Design Principles for DFA Manufacturers.
- Implement Comprehensive Incident Response and Recovery Plans for DFA.
- Develop and Enforce Interoperable Cybersecurity Standards for DFA.
- Implement Continuous Monitoring and Adaptive Security Measures for DFA.

By understanding and proactively addressing the challenges associated with demand flexible networked appliances, we can harness the benefits of DFA while maintaining the security and reliability of our energy systems. As the energy landscape continues to evolve, so too must our approach to cybersecurity, ensuring that our increasingly distributed and interconnected energy infrastructure remains resilient in the face of emerging threats.

Table of Contents

1 Introduction

Cybersecurity concerns related to demand-flexible networked electrical appliances are becoming increasingly critical as these devices become integral to modern energy management systems. These appliances, such as air-conditioning systems, residential and small-scale solar photovoltaic (PV) systems, household batteries and electric vehicle (EV) chargers interact with networks to optimize energy use based on demand and user preferences. However, their connectivity also introduces vulnerabilities that could be exploited by malicious actors, leading to significant risks such as data breaches, service disruptions, and even safety hazards.

This project has been commissioned by the International Energy Agency's Energy Efficient End-use Equipment (IEA 4E) Technology Collaboration Program, through its Efficient, Demand Flexible Networked Appliances platform (EDNA). EDNA provides analysis and policy guidance to members and other governments aimed at improving the energy efficiency and demand flexibility of connected devices and networks.

The objective of this work is to research and report on the challenges and evolution of current and potential future threats in relation to demand flexible networked appliances, investigate what is being done, or considered, by various relevant organizations and countries, and to summarize the issues that policy makers need to be aware of in relation to minimizing and mitigating cybersecurity risks.

To meet this objective, research was carried out into the current cybersecurity landscape, current and future threats, and a review of existing policies and standards that have been developed by stakeholders globally. Each of these areas of research is addressed in a separate chapter in this report.

This research comprised desktop and literature research supplemented by discussions with a range of stakeholders and the authors' own knowledge of this subject.

On the basis of that research, a number of policy options, standards and potential legislation are identified and assessed in the Summary and Conclusions (Chapter 5) of this document. This is followed by the identification of potential cybersecurity options and next steps for policy makers to consider.

The term "demand flexible appliances" (DFA) is used in this report to describe products where a significant amount of power can be switched on or off via a communications network to benefit the electricity grid.

DFA encompasses items referred to as Distributed Energy Resources (DER) and Customer Energy Resources (CER) that sit behind the meter. While most demand flexible appliances are owned by the customer, there is a wide range of commercial and control arrangements within and across markets.

A Glossary of acronyms and terms relevant to cybersecurity is provided in Chapter 8 and a number of key concepts in cybersecurity are outlined in Appendix 2.

1.1 Product characteristics of DFA

As a device class DFA has a number of features which represent a material departure from the assets which the electricity industry is experienced in managing. These include:

- One of the key features of DFA vs. traditional assets is that they are internet connected. They are connected either through dedicated communications capabilities on the device, or via the Home Wi-Fi - but it is this connectivity that makes them different.
- Individual devices are small with loads ranging from a few hundred watts to a few kilowatts.
- The capabilities of these devices can vary materially - from varying levels of metrology (from basic consumption readings through interval data and quite sophisticated power quality data), to varying levels of power functions - import, export, voltage/ watt response, frequency/ watt response etc.
- DFA customer offerings can also vary in terms of the auxiliary services, for example many come with online portals where devices can be monitored and usage patterns seen.
- Some DFA allow control over other devices i.e. Home Energy Management Systems (HEMS) or some inverters can function as HEMS in concert with other devices
- These are devices which receive firmware updates 'over the air' and much more frequently than other devices in the home. The version of firmware being run by a device may not be directly controlled by the manufacturer, or the utility, but may rely on the consumer to update these products
- Some DFA are designed, installed and used specifically to deliver electric services, for example a solar inverter and panels have no purpose other than the generation of electricity. While the primary purpose of other types of DFA (e.g. a Wi-Fi connected Air Conditioner) is not about electricity, but rather some other benefit for the household. This is illustrated in Figure 1 below.

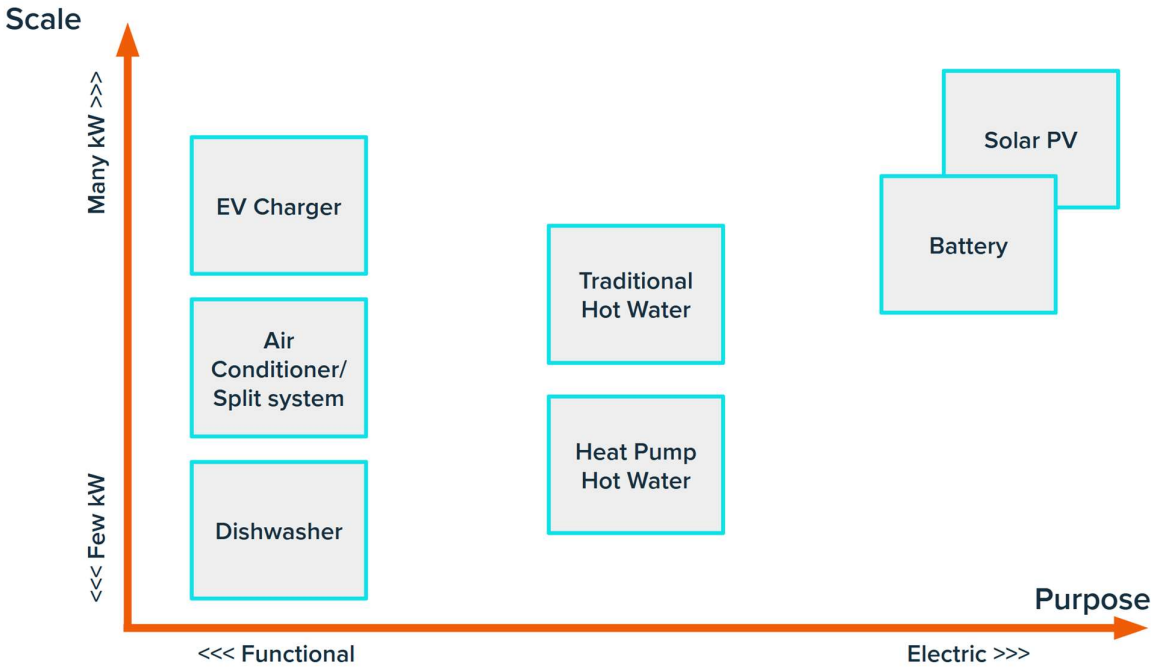


Figure 1: Example DFA illustrating potential scale and purpose

1.2 Market Characteristics of DFA

On top of product characteristics which make DFA novel in the electricity sector, there are many market factors which are unlike other classes of assets and technology we are used to managing, including:

- There are many players. Not just in terms of device classes, but each category of device often has many manufacturers. There may be, for example, 10 different brands which cover 95% of a device class.
- For Original Equipment Manufacturer (OEMs), some DFA markets are very large and advanced, while many other DFA markets are much smaller. Small markets have the additional challenges for OEMs with regards to cybersecurity where any attempt to do anything bespoke will either directly drive up costs for consumers, and/ or force OEMs out of the market likely increasing costs for consumers.
- The pace of innovation is rapid, and for DFA, it is multi-dimensional because innovation is happening in the technologies themselves, the web based management platforms, the communications technologies and the commercial models. All this is occurring while the cybersecurity landscape is continuing to evolve. This pace of evolution is not something that the electricity industry is used to managing.
- Adoption rates vary by DFA class, and by jurisdiction, for example Australia has an extraordinarily high penetration of residential solar - but very few EVs – which is the opposite of the situation in the UK.
- The value of a DFA, either for the purposes of network/ system support, or for wholesale market or other price participation, is negligible. Because of their small size, and the potential to send commands to great numbers of devices simultaneously, DFA are inherently more valuable when they are aggregated into a Virtual Power Plant (VPP).

1.3 Vulnerabilities in DFA Systems

DFA systems present vulnerabilities and combinations of vulnerabilities that the electricity sector has not previously had to manage. These can be viewed from two perspectives: the vendor/OEM side and the utility side.

On the vendor/OEM side, vulnerabilities include:

- Management and understanding of device communication protocol vulnerabilities: DFA devices often use a variety of communication protocols, each with its own potential security flaws.
- Firmware vulnerabilities: Outdated or improperly secured firmware can provide an entry point for attackers. This is especially pernicious in an environment where consumer technology is evolving so rapidly.
- Security of consumer portals: Web-based interfaces for consumers to manage their DFA devices can be a weak point if not properly secured. This can expose personal information from customer names and addresses to billing information depending upon the products being offered.
- Internet-based visibility and control issues: The ability to remotely monitor and control DFA devices introduces potential attack vectors.

- Vulnerabilities in home internet-based communication pathways: Many DFA devices rely on consumers' home internet connections, which may not be secure.

On the utility side, vulnerabilities include:

- Understanding and managing vulnerabilities in device communication protocols: Utilities must be able to securely communicate with a diverse array of DFA devices.
- Scaling challenges inherent to DFA systems: As the number of connected devices grows, so does the complexity of managing and securing them.
- Device registration approaches (often not covered in standards): The process of securely registering and authenticating new DFA devices on the network is crucial but often overlooked in existing standards.
- Establishing trust in trustless environments: Utilities must find ways to ensure the authenticity and integrity of communications with DFA devices that may be outside their direct control.
- Security of consumer portals: Utilities often provide their own interfaces for consumers to manage DFA devices, which must be secured against potential attacks.
- Internet-based visibility and control issues: The ability to remotely monitor and control large numbers of DFA devices introduces new attack surfaces for utilities to defend.
- Home internet-based communication vulnerabilities: Utilities must consider the security implications of relying on consumers' internet connections as part of their infrastructure.

These vulnerabilities differ significantly from those in traditional energy infrastructure, presenting new challenges for cybersecurity professionals in the energy sector. The distributed nature of DFA systems means that there are many more potential points of entry for attackers, and the consequences of a successful attack could be more widespread and difficult to contain.

1.4 Characteristics of DFA that must be managed

DFA represent a fundamental shift in the electricity sector, introducing a level of complexity and diversity that sets them apart from traditional energy assets. Unlike centralized power plants or large-scale transmission infrastructure, DFA encompass a wide array of smaller, often consumer-owned devices such as rooftop solar panels, battery storage systems, electric vehicle chargers, and smart appliances. This fundamental difference necessitates a reimagining of how we approach cybersecurity and risk management in the energy sector.

The characteristics of DFA – their distributed nature, consumer interface, rapid technological evolution, and internet connectivity – create a risk profile that is distinctly different from that of conventional energy infrastructure. These devices, while individually small, can collectively have a significant impact on grid stability and energy markets when aggregated at scale. Moreover, the cybersecurity practices and capabilities of DFA manufacturers vary widely, adding another layer of complexity to the risk landscape.

These differences make it clear that traditional approaches to energy sector cybersecurity are insufficient. The industry must adapt its risk assessment and management strategies to address the challenges posed by these diverse, numerous, and rapidly evolving consumer devices.

The electricity sector needs to look beyond the heavily regulated utility model and towards consumers and their devices.

2 DFA Cybersecurity Landscape

The rapid proliferation of DFA technologies is transforming the traditional centralized energy model into a more decentralized and complex network. This transformation brings both opportunities and challenges, particularly in terms of cybersecurity.

The integration of DFA into our energy infrastructure is happening by default because, as devices are installed and plugged in, they become part of our grid. Every day there are more solar panels, more batteries, more heating, ventilation and air conditioning and more EV chargers being installed by customers. 167 GW of distributed PV systems were installed globally between 2019 and 2021, which means their combined peak output is higher than combined peak consumption of France and Britain. In 2020, EV stock surpassed 10 million vehicles and almost 180 million heat pumps were in operation[1].

With appropriate regulation and incentives, integration should follow a basic pattern of evolution: first comes deployment, then visibility, and finally control. However, this process raises several critical questions regarding our ability to manage the integration of these systems:

- Do we have visibility of what's being installed and at what rate?
- Can we track consumer adoption and rollout of these devices?
- Do we understand the capacity and usage patterns of these devices?
- Can these devices be controlled, and if so, by whom and to what end?
- What are the methods and purposes of this control? Have the use cases been defined? (whether for system stability, easing local network constraints, or market based incentives)
- What vulnerabilities do these devices have?
- Has customer consent been captured?
- Is there an agreed, scalable, functional control methodology and approach in place?

These questions highlight the challenges in gaining comprehensive visibility and control over the rapidly expanding DFA landscape. The answers to these questions are crucial for network operators, regulators, and policymakers to effectively manage and make secure the evolving energy ecosystem.

[1] Executive summary – Unlocking the Potential of Demand Flexible Appliances – Analysis - IEA

2.1 DFA Cybersecurity Landscape Overview

The cybersecurity landscape for DFA is complex, dynamic, and rapidly evolving. As DFA systems become increasingly integrated into our energy infrastructure, they introduce challenges and vulnerabilities that traditional cybersecurity approaches struggle to address, specifically:

Traditional Cybersecurity Approach	DFA Considerations
Centralized IT infrastructure protection	Highly distributed architecture requiring protection of numerous remote endpoints and edge devices
Well-defined network perimeters	Multiple network boundaries across various locations, stakeholders, and ownership models
Regular patching cycles	Challenging to patch due to operational requirements, remote locations, and legacy equipment
Standard IT protocols and systems	Mix of proprietary, legacy, and modern protocols across both IT and OT systems
Controlled physical access	Limited physical security at grid-edge deployments, often in public or customer premises
Relatively predictable attack surfaces	Dynamic and complex attack surfaces due to constant addition of new DFA and changing grid configurations

At its core, the DFA cybersecurity landscape is characterized by a vast and diverse network of interconnected devices. This distributed nature creates an expansive attack surface, with millions of potential entry points for malicious actors.

Key features of the DFA cybersecurity landscape include:

1. **Diverse Stakeholders**: The landscape involves a wide range of participants, including device manufacturers, utilities, aggregators, regulators, and consumers. Each of these stakeholders has different security needs, capabilities, and responsibilities.
2. **Rapid Technological Evolution**: DFA and communications technologies are advancing quickly, often outpacing the development of security measures and regulations. This rapid change introduces new vulnerabilities and challenges on a regular basis.
3. **IT/OT Convergence**: DFA systems blur the lines between Information Technology (IT) and Operational Technology (OT), requiring cybersecurity approaches that can bridge these traditionally separate domains.
4. **Data Privacy Concerns**: The vast amount of data generated by DFA devices, including energy usage patterns and personal information, raises significant privacy concerns.
5. **Grid Stability Implications**: Cyberattacks on DFA systems have the potential to impact grid stability, making cybersecurity a critical component of overall grid resilience.
6. **Regulatory Complexity**: The regulatory landscape for DFA cybersecurity is fragmented, with varying requirements across different jurisdictions and a lack of comprehensive, globally accepted standards.
7. **Emerging Threat Vectors**: As DFA systems become more sophisticated, they face evolving threats, including AI-enhanced attacks, quantum computing risks, and exploitation of emerging technologies.

8. **Supply Chain Vulnerabilities**: The global nature of DFA device manufacturing introduces supply chain risks that need to be carefully managed.

Navigating this complex landscape requires a multi-faceted approach that combines technological solutions, policy frameworks, industry best practices, and international cooperation. As we delve deeper into specific aspects of DFA cybersecurity, it's crucial to keep this broader context in mind, understanding how each challenge and solution fits into the larger picture of securing our increasingly distributed and interconnected energy future.

2.2 Risks and Key Concepts of Cybersecurity

Central to the assessment of cybersecurity is the concept of risk. Risk is the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. It's often expressed as a function of the likelihood of an event occurring and the potential impact of that event.

With regards to DFA, because of the special nature of the systems used to operate these devices, and the (often) multi-party access provided to those devices, scenarios exist where an attack may result in a handful of devices, across several OEMs being impacted, or widespread cross border impacts. This wide range of risks associated DFA make them distinct within the context of the electricity industry.

Core Definitions

Risk: Potential for loss, calculated as Likelihood × Impact

Asset: Items of value requiring protection (e.g., customer databases, systems)

Threat: Potential danger that could harm assets (e.g., hackers, malware)

Vulnerability: System weaknesses that could be exploited (e.g., unpatched software)

Attack Vector: Method used to exploit vulnerabilities (e.g., phishing emails)

Response Framework

Control: Protective measures (technical, administrative, or physical)

Mitigation: Actions to reduce risk severity or attack impact

Incident: Events that compromise or threaten system security

Practical Application

The above concepts work together in a chain: Threat actors use attack vectors to exploit vulnerabilities in assets, creating risks. When realized, these become incidents with measurable impacts. This is illustrated in Figure 2 below. Organizations implement controls and mitigation strategies to break this chain and protect their assets.

For example, a phishing attack targeting untrained employees (vulnerability) could compromise email systems (asset), leading to data theft (incident). Implementation of security training and email filtering (controls) helps mitigate this risk.

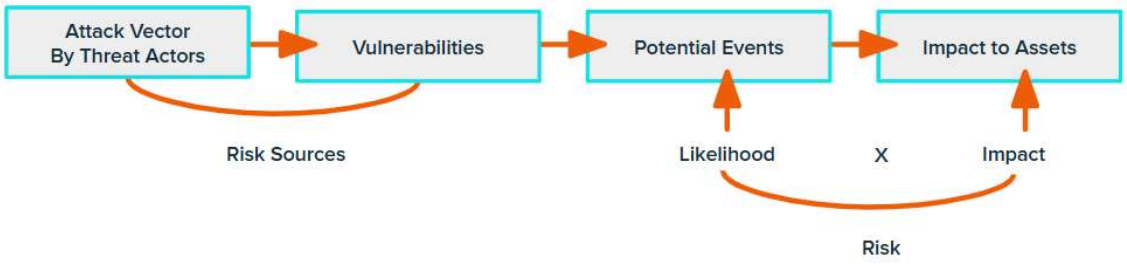


Figure 2: Relationships between the elements of risk concept

2.3 A Lack of Standardization Challenges Integration and Therefore Security

One of the primary challenges in DFA integration is the lack of standardization in technologies and approaches. While standards such as openADR, CSIP, CSIP-Aus, MATTER, and OCPP[2] exist, there has been little incentive for Original Equipment Manufacturers (OEMs) to adopt them uniformly. Standards vary significantly across jurisdictions, including the USA, Japan, the European Union, the UK and Australia/NZ.

This lack of standardization creates a fragmented landscape where devices from different manufacturers may not communicate effectively or securely with each other or with the broader grid infrastructure. It also complicates efforts to implement unified security protocols across the DFA ecosystem.

For OEMs, adhering to specific jurisdictional cyber standards represents an additional expense. Beyond meeting their internal cybersecurity needs – for which they often take a risk-based approach – OEMs must weigh the costs and benefits of complying with various regional standards. This cost-benefit analysis often leads to inconsistent implementation of security measures across different products and markets.

Another significant challenge, particularly affecting network operators, is the shift in focus from Operational Technology (OT) to Information Technology (IT) systems to deal with DFA integration. Traditionally, network operators have been accustomed to working with OT – heavily secure, behind-the-firewall, on-premise technology. Many network operators are not experienced with cloud-based technologies, and regulatory environments often aren't conducive to the adoption of such technologies.

The shift from OT to the cloud requires a significant change in mindset, skills, and infrastructure for network operators. Network operators must now manage a hybrid environment that combines traditional OT systems with more modern, cloud-based IT solutions. This transition introduces new

[2] Refer to Glossary, Chapter 8 for definitions of these terms

security challenges, as IT systems often have different vulnerabilities and require different security approaches compared to traditional OT systems.

2.4 Threat Landscape for DFA

The threat landscape for DFA encompasses various types of attacks, including malware, ransomware, physical tampering, and sabotage. However, a key concern is the potential for attackers to gain control of DFA fleets for the purpose of creating grid and market instability.

While there are no known DFA-specific attacks to date, the increasing sophistication of cyberattacks targeting energy systems generally is a cause for concern. An IEA report[3] notes that from 2020 to 2022 the number of cyber-attacks on critical gas and electricity infrastructure has more than doubled from 504 to 1101 per week. This report also notes that information on significant cybersecurity incidents is limited due to under-reporting and lack of detection.

Attackers could potentially exploit vulnerabilities in DFA systems to:

- Manipulate energy production or consumption, leading to grid instability
- Access sensitive consumer data
- Disrupt energy markets by falsifying data or manipulating DFA behaviour
- Use compromised DFA devices as entry points to launch broader attacks on utility networks

The broader impacts of cyberattacks on DFA vendors, such as intellectual property (IP) theft and industrial espionage, also need to be considered. Attackers may target DFA manufacturers to steal proprietary technology or gain insights into vulnerabilities that could be exploited in future attacks.

As DFA systems become more prevalent and interconnected, they may become increasingly attractive targets for cybercriminals and state-sponsored actors alike. The potential for cascading effects, where an attack on DFA systems could impact the broader power grid, makes this an area of particular concern for energy security.

[3] Cybersecurity – is the power system lagging behind? IEA August 2023.

2.4.1 Current Threats

Weak Authentication and Authorization

Many DFA devices are deployed with inadequate authentication mechanisms, often relying on default or weak passwords. This vulnerability can lead to unauthorized access, potentially allowing attackers to control or manipulate devices.

Impact	Mitigation Considerations
Compromised devices could be used to disrupt grid operations, steal sensitive data, or serve as entry points for broader network attacks.	• Implement strong, unique passwords for all devices • Use multi-factor authentication where possible • Regularly update and audit access credentials

Lack of Encryption

Data transmitted by DFA devices is often unencrypted, exposing sensitive information to interception and manipulation.

Impact	Mitigation Considerations
Attackers could intercept and modify control signals, energy usage data, or personal information, leading to privacy breaches or operational disruptions.	• Implement end-to-end encryption for all data transmissions • Use secure protocols (e.g., TLS) for device communications • Regularly update encryption methods to address new vulnerabilities

Firmware and Software Vulnerabilities

Outdated or unpatched firmware and software in DFA devices can contain known vulnerabilities that attackers can exploit.

Impact	Mitigation Considerations
Exploited vulnerabilities could allow attackers to gain unauthorized control of devices, inject malicious code, or cause device malfunctions.	• Implement secure, automated update mechanisms • Conduct regular security audits and penetration testing • Establish a vulnerability disclosure program with device manufacturers

Supply Chain Risks

DFA devices and components often involve complex, global supply chains, increasing the risk of compromised hardware or software being introduced during manufacturing or distribution.

Impact	Mitigation Considerations
Compromised supply chains could lead to widespread vulnerabilities across multiple devices or systems, potentially creating large-scale security issues.	• Implement rigorous supply chain security practices • Conduct thorough vetting of suppliers and components • Use tamper-evident packaging and secure delivery methods

Communication Protocol Vulnerabilities

Many DFA devices use standard communication protocols (e.g., Modbus, DNP3) that may have inherent security weaknesses if not properly configured or updated.

Impact	Mitigation Considerations
Vulnerabilities in these protocols could allow attackers to intercept or manipulate communications between DFA devices and control systems.	• Use secure versions of protocols where available • Implement additional security layers (e.g., VPNs) for critical communications • Regularly assess and update protocol configurations

Case Study: Ukraine Power Grid Attack (2015)

In December 2015, a cyberattack on Ukraine's power grid left approximately 230,000 people without electricity for up to 6 hours. The attackers exploited vulnerabilities in the grid's communication protocols and remote access tools. This incident highlights the potential real-world impact of cyberattacks on energy infrastructure and the importance of securing all aspects of the grid, including DFA systems.

Insider Threats

Employees or contractors with privileged access to DFA systems could intentionally or unintentionally compromise security.

Impact	Mitigation Considerations
Insider threats could lead to data breaches, sabotage of systems, or provide external attackers with valuable inside information.	• Implement principle of least privilege for system access • Conduct regular security awareness training for all personnel • Monitor and audit system access and activities

Physical Security Vulnerabilities

Many DFA devices are deployed in physically accessible locations, making them vulnerable to tampering or direct attacks.

Impact	Mitigation Considerations
Physical access to devices could allow attackers to install malware, extract sensitive data, or directly manipulate device operations.	• Implement physical security measures (e.g., locks, tamper-evident seals) • Use tamper-resistant hardware designs • Deploy physical intrusion detection systems

2.4.2 Emerging Technologies and Future Threats

As in other industries, the increasing adoption of AI in the energy sector is shaping the way in which cyberattacks may be carried out. AI technologies could be leveraged by attackers to identify vulnerabilities more efficiently or to orchestrate more sophisticated, coordinated attacks on DFA systems.

As DFA systems continue to evolve and expand, new threat vectors are likely to emerge. Understanding these potential future threats is crucial for proactive security planning.

Potential AI-enabled threats include:

- Automated vulnerability discovery in DFA systems
- Advanced social engineering attacks targeting utility employees or consumers
- Intelligent malware capable of evading traditional detection methods
- Coordinated attacks that learn and adapt to defensive measures in real-time

Other emerging technologies, such as advanced IoT devices and 5G networks, will likely introduce new threats to DFA cybersecurity. The proliferation of IoT devices in the energy sector increases the attack surface, while 5G networks could enable faster, more complex attacks.

Future threats may also arise from:

- Quantum computing, which could break current encryption methods
- Advanced persistent threats (APTs) specifically targeting DFA infrastructure
- Exploitation of vulnerabilities in blockchain-based energy trading platforms

As these technologies evolve, so too must our approach to securing DFA systems. This will require ongoing research, development of new security technologies, and adaptive regulatory frameworks.

AI and Machine Learning-Enhanced Attacks

Advancements in AI and machine learning could lead to more sophisticated, automated attacks that are harder to detect and mitigate.

Potential Impact	Future Considerations
• Adaptive malware that can evade traditional detection methods • Automated vulnerability discovery and exploitation • Large-scale, coordinated attacks on multiple DFA systems	• Develop AI-powered defence systems to counter AI-enhanced threats • Invest in advanced anomaly detection and behavioural analysis tools • Establish industry collaborations to share threat intelligence on AI-based attacks

Quantum Computing Threats

The advent of practical quantum computing could potentially break many current encryption methods, posing a significant threat to DFA cybersecurity.

Potential Impact	Future Considerations
• Compromise of encrypted communications and stored data • Invalidation of current public key infrastructures • Need for widespread updates to cryptographic systems	• Invest in quantum-resistant cryptography research and development • Plan for large-scale cryptographic transitions in DFA systems • Develop strategies for protecting currently encrypted data against future decryption

5G and Advanced Connectivity Risks

The rollout of 5G networks and other advanced connectivity technologies will increase the attack surface for DFA systems.

Potential Impact	Future Considerations
• New vulnerabilities in 5G infrastructure affecting DFA communications • Increased risk of large-scale DDoS attacks due to higher bandwidth • Potential for more sophisticated man-in-the-middle attacks	• Develop security standards specific to DFA systems in 5G environments • Implement advanced network segmentation and isolation techniques • Enhance monitoring and anomaly detection for high-speed, low-latency communications

Advanced Persistent Threats (APTs) Targeting DFA

A sophisticated threat actor, typically a state-sponsored group or professional cybercrime organization, that gains and maintains unauthorized access to a network over an extended period while evading detection. APTs use advanced techniques, custom malware, and multiple attack vectors to achieve specific long-term objectives. As DFA becomes more critical to grid operations, it's likely to attract more attention from sophisticated, state-sponsored APT groups.

Potential Impact	Future Considerations
• Long-term, stealthy infiltration of DFA systems • Potential for large-scale, coordinated attacks on national energy infrastructure • Theft of proprietary technology and sensitive operational data	• Enhance threat intelligence sharing among energy sector stakeholders • Develop advanced APT detection and response capabilities specific to DFA environments • Implement rigorous, ongoing security assessments and red team exercises

Emerging Threat Scenario: Coordinated DFA Manipulation

Imagine a scenario where an APT group gains control over a large number of residential solar and battery systems. By coordinating the behavior of these systems – for example, simultaneously cutting power export during peak demand – they could cause significant grid instability. This type of attack could have cascading effects on the broader power system and potentially lead to widespread outages.

IoT Botnet Exploitation

The growing number of connected DFA devices, which are running more powerful hardware, presents an attractive target for botnet operators, who could harness compromised devices for various malicious activities.

Potential Impact	Future Considerations
• Use of DFA devices in large-scale DDoS attacks • Crypto-mining operations leveraging DFA computational resources • Degradation of DFA performance and grid stability due to botnet activities	• Implement robust device authentication and access controls • Develop advanced botnet detection techniques for DFA networks • Establish industry-wide rapid response protocols for botnet mitigation

Exploitation of Emerging DFA Technologies

As new DFA technologies emerge (e.g., vehicle-to-grid systems, advanced demand response systems), they may introduce unforeseen vulnerabilities.

Potential Impact	Future Considerations
• New attack vectors specific to emerging technologies • Potential for cascading failures due to interconnected systems • Exploitation of gaps between new technologies and existing security measures	• Integrate security considerations into the design phase of new DFA technologies • Develop flexible, adaptable security frameworks that can accommodate technological evolution • Establish cross-industry collaborations to address security challenges in converging technologies

Social Engineering and Phishing Evolving with DFA

As DFA systems become more consumer-facing, social engineering and phishing attacks may evolve to target DFA users and operators more specifically.

Potential Impact	Future Considerations
• Compromise of user accounts controlling DFA devices • Manipulation of consumer behaviour to impact grid operations • Theft of personal and financial data related to DFA operations	• Develop DFA-specific cybersecurity awareness programs for consumers • Implement advanced authentication methods for consumer-facing DFA interfaces • Enhance detection of DFA-related phishing and social engineering attempts

2.5 Potential Impacts of Cyberattacks on Grid Stability

The consequences of cyberattacks on DFA systems for overall grid stability and reliability can be severe. The impact is directly related to DFA penetration levels and can range from localized disruptions to effects on zone substations and even transmission-level issues. The primary concern is the potential for attackers to manipulate large amounts of load, destabilizing networks and potentially causing widespread outages.

Scenarios for potential attacks include:

- Simultaneous shutdown of a large number of DFA devices, causing a sudden drop in power generation
- Rapid fluctuations in power output from DFA devices, leading to frequency instability
- Overloading of local distribution networks by manipulating DFA behaviour
- Falsification of data from DFA devices, leading to incorrect decisions by grid operators

The scale of impact can vary depending upon the nature of the attack:

- Localized: Affecting a single neighbourhood or small area, typically a Low Voltage Feeder. A small, targeted attack could shift load in such a way that protection gear could be triggered and the network taken down.
- Zone Substation: Impacting a larger area served by a particular substation. Like localised impacts, substations could be targeted, but it is also likely that a broader switching of DFA could create impact on a zone substation with a high penetration of DFA.
- Transmission: In cases of high DFA penetration, attacks could potentially affect transmission-level stability. A practical example would be springtime in South Australia[4] where, if residential solar was to be turned off simultaneously across the state (i.e. over a 7min period), total generation from other sources would need to increase by up to 70% across the state.

The potential for such attacks highlights the need for proactive cybersecurity measures in this rapidly evolving field. As DFA penetration increases, the potential impact of such attacks grows, making it crucial to address these vulnerabilities proactively.

2.6 Role of State-Based Actors

State-based actors pose a significant threat to DFA systems as part of broader cyber warfare strategies. These actors often have substantial resources and sophisticated capabilities, making them particularly dangerous in the context of critical infrastructure such as energy systems.

Two notable examples illustrate the potential for such attacks:

1. The December 2015 cyberattack on Ukraine's power grid: This attack, attributed to Russian state-sponsored hackers, resulted in widespread power outages affecting over 200,000 consumers. While this attack targeted traditional power infrastructure, it demonstrates the potential for state actors to disrupt energy systems.
2. Russia's ongoing efforts to destabilize Ukraine by targeting electricity infrastructure: These attacks have included both cyber and physical elements, highlighting the multi-faceted approach that state actors can take in targeting energy systems.

The involvement of state-based actors adds a layer of complexity to DFA cybersecurity, as these threats may be driven by geopolitical motives rather than purely financial ones. This necessitates a coordinated response involving not just utilities and regulators, but also national security agencies and international cooperation.

2.7 Examples of Cybersecurity Attacks in Energy

The incidents shown in Figure 3 below underscore the geopolitical implications of cyberattacks on energy systems, including DFA, and their potential impact on national security and energy independence.

[4] sapowernetworks.com.au/data/309066/smarter-homes-regulation-now-in-effect/

As DFA systems become more prevalent, they may become attractive targets for state-based actors seeking to:

- Demonstrate technological capabilities
- Cause economic disruption
- Undermine public confidence in energy systems
- Gain strategic advantage in conflicts

Figure 3: A brief history of energy cyber incidents - Ref Summer Preparedness (aemo.com.au)

Reference links for the cyberattacks shown in Figure 3 are as follows:

sPower it the first renewable energy provider hit by a cyber attack (securityaffairs.com)

SolarWinds hack explained: Everything you need to know (techtarget.com)

Colonial Pipeline hack explained: Everything you need to know (techtarget.com)

Vestas data 'compromised' by cyber attack | Reuters

Cyber Threat to Queensland's Electricity - Australian Cyber Security Magazine

German wind turbine maker shut down after cyberattack (therecord.media)

Nordex hit by cyber security incident, shuts IT systems | Reuters

Case Study: Viasat Attack | CyberPeace Institute

Aurecon cyber attack under investigation - Cyber Daily

2.8 Data Privacy and Security Concerns

DFA systems raise important data privacy issues, particularly concerning consumer data collected by smart devices. This includes not only usage data and control logs but also private information such as email addresses, mobile numbers, physical addresses, and potentially credit card information.

The types of data at risk include:

- Energy consumption patterns

- Device operation schedules
- Personal identification information
- Financial data related to energy transactions
- Location data (for mobile DFA such as electric vehicles)

This data, if compromised, could be used for various malicious purposes, including:

- Identity theft
- Targeted phishing attacks
- Burglary (by identifying when homes are likely to be empty)
- Market manipulation (by aggregating consumption data)

While there are often regulatory requirements for utilities regarding data protection, DFA-specific cybersecurity regulations are frequently lacking. This creates a gap in consumer protection and data security that needs to be addressed. The challenges include:

- Defining ownership and control of data generated by DFA devices
- Ensuring secure data transmission and storage across diverse DFA systems
- Balancing data accessibility for grid management with consumer privacy rights
- Implementing robust consent mechanisms for data sharing
- Ensuring compliance with varying data protection regulations across jurisdictions

Addressing these challenges requires a coordinated effort between DFA manufacturers, utilities, regulators, and consumers to establish clear guidelines and implement robust security measures.

2.9 Current Mitigation Strategies

Security Measures and Industry Best Practice

The security measures and best practices adopted by DFA manufacturers and operators vary widely. Some adhere to generic standards such as ISO27001, while others follow more specific cybersecurity requirements such as the Australian Energy Sector Cybersecurity Framework (AESCSF). However, there is a notable lack of DFA-specific cybersecurity protocols or standards.

Current security measures often include:

- Encryption of data in transit and at rest
- Access control mechanisms
- Regular security updates and patches
- Network segmentation
- Intrusion detection and prevention systems

Best practice for DFA cybersecurity should encompass:

- Secure by design principles in DFA device development[5]
- Regular security assessments and penetration testing
- Incident response planning specific to DFA-related scenarios
- Employee training on DFA cybersecurity risks and best practices

[5] nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf

- Supply chain security measures to ensure the integrity of DFA components

This variability in security measures creates significant room for improvement and highlights the need for collaboration across jurisdictions to develop comprehensive, DFA-specific security standards. Such standards could help ensure a baseline level of security across the DFA ecosystem, making it more resilient to cyber threats.

Regulatory and Policy Landscape

The current regulatory and policy landscape for DFA cybersecurity varies significantly across different jurisdictions. While some regions have begun to implement DFA-specific cybersecurity regulations, many are still relying on broader energy sector or general cybersecurity policies.

Key aspects of the regulatory landscape include:

- Varying requirements for data protection and privacy
- Differing approaches to DFA integration and control
- Inconsistent standards for DFA device security
- Evolving frameworks for incident reporting and response

Policy plays a crucial role in shaping secure practices and encouraging the adoption of robust cybersecurity measures. However, the rapid pace of DFA adoption often outstrips the speed of regulatory development, creating potential security gaps.

Efforts to improve the regulatory landscape should focus on:

- Developing flexible, technology-neutral regulations that can adapt to evolving threats
- Harmonizing standards across jurisdictions to reduce complexity for manufacturers and operators
- Incentivizing investment in cybersecurity measures for DFA
- Establishing clear lines of responsibility and liability for DFA cybersecurity
- Promoting information sharing and collaboration between stakeholders

More detail of cybersecurity standards, guidelines and other initiatives is provided in Chapter 3.

2.10 Growth in Cybersecurity Services

In response to the growing cybersecurity challenges in the DFA space, there has been a significant increase in companies providing cybersecurity and AI services. These range from more generic cybersecurity capabilities to specialized services for the energy sector.

Key areas of growth include:

- Incident response capabilities: Services that help organizations quickly detect, respond to, and recover from cyberattacks.
- Security Information and Event Management (SIEM) products: Tools that provide real-time analysis of security alerts generated by DFA and other network devices.

- Firewall-based security solutions: Advanced firewalls designed to protect against sophisticated cyber threats targeting energy infrastructure.
- Cloud application security products: Services that secure cloud-based DFA management and control systems.

Other emerging services include:

- AI-powered threat detection and response systems
- Specialized DFA device security solutions
- Supply chain security services for DFA manufacturers
- Cybersecurity training and awareness programs for energy sector employees

While these services provide valuable tools for securing DFA systems, it's important to note that many are not specifically tailored to the specific challenges of DFA cybersecurity. As the field evolves, we can expect to see more specialized services emerging to address the specific needs of DFA systems.

A list of prominent firms providing cybersecurity services is provided in Appendix 5.

3 Review of Current Policies, Standards and Other Cybersecurity Initiatives

DFA proliferation has triggered a variety of responses from governments, industry bodies, and other stakeholders worldwide. The speed, or appropriateness, of these changes will not be examined here as this chapter provides an overview of existing policies, standards, and cybersecurity initiatives relevant or adjacent to DFA. The review in this chapter is not exhaustive, but is intended to be illustrative, showcasing examples of approaches taken in different jurisdictions and by various organizations, identifying key themes.

Our examination reveals a patchwork of regulations, guidelines, and industry-led initiatives that, while addressing some aspects of DFA cybersecurity, often fall short of providing a comprehensive and cohesive framework. This fragmented approach is partly due to the complex and rapidly changing nature of DFA technologies, compounded by the varying priorities and capabilities of different jurisdictions, and the difficulties of international coordination.

Several key gaps emerge from this review:

- Lack of a comprehensive Public Key Infrastructure (PKI): Perhaps the most glaring gap, and one that warrants particular emphasis, is the lack of a comprehensive Public Key Infrastructure (PKI) for DFA, both within individual jurisdictions and internationally.
- **Inconsistency:** There is a notable absence of globally harmonized standards specific to DFA cybersecurity, leading to inconsistencies across borders, OEM device classes, OEM vendors and therefore potential vulnerabilities.
- **Inability to Address Existing Threats:** Many existing policies and standards struggle to keep pace with rapidly evolving cyber threats, and while some may rightly identify legitimate concerns about emerging technologies like AI and quantum computing, there are many ‘basics’ which can be delivered first to lift baseline performance across the sector.
- **Limited Focus on Supply Chain Security:** While some initiatives address supply chain risks, there's generally insufficient emphasis on securing the global DFA device manufacturing and distribution processes. It is important to acknowledge that there are potential geo-political challenges which may impact the ability to fully resolve this challenge.

Key Gap: Public Key Infrastructure

Public Key Infrastructure (PKI) is a framework of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and public keys. PKI enables secure electronic transfer of information by providing the mechanisms to establish trust through identity validation and digital signatures.

PKI is crucial for ensuring secure, authenticated communication between DFA devices, utilities, and other stakeholders. Its absence represents a significant vulnerability in the DFA ecosystem, potentially exposing critical infrastructure to unauthorized access, data tampering, and other cyber threats.

An overview of PKI is provided in Appendix 1.

The following sub-sections describe a range of legislation, standards, guidelines and other initiatives relevant to cybersecurity of DFA and other infrastructure. Figures showing the applicability of the various initiatives in different parts of the world are provided in Section 3.4.

Over these sub-sections, it's important to keep the above-mentioned gaps in mind. Understanding where current efforts fall short is crucial for identifying areas that require urgent attention and for developing more robust, comprehensive approaches to DFA cybersecurity for governments and industry bodies as the sector moves forward.

3.1 Acts and Legislation

International legislation in relation to cybersecurity tends to relate to either products that are capable of being network connected, or to critical infrastructure.

Important features and strengths of legislation that relate to products include:

- The applicability and scope tend to be wide, i.e. any hardware that is capable of being connected to the internet or other network, as well as relevant software and information and communications technology.
- The intention is that cybersecurity is integrated throughout the product lifecycle from design phase through to the end of the product's lifecycle including post-market updates and patches to address emerging vulnerabilities.
- Security standards are defined for a range of products, services and processes.
- Processes are standardized and harmonized across a region, e.g. the EU.
- Risk based certification is used, tailoring certification to the level of risk associated with a product or service with assurance levels ranging from basic to high, based on the potential impact of cybersecurity threats.
- Some requirements in critical sectors are mandatory, while those in less critical areas are voluntary, thus providing flexibility in the approach taken.
- Administering agencies have a mandate to continue development of certification schemes and provide expert advice.
- Incident reporting can be included.
- Penalties can be applied for non-compliance thus assisting with ensuring only secure products are available.
- There is a focus on the protection of personal data and preventing unauthorized access to the device.
- In some cases manufacturers are required to conduct security assessments of their IOT products before they can be sold.

Important features and strengths of legislation that relate to critical infrastructure include:

- Facilitating information sharing between government and private sectors.
- Requirement to report significant cybersecurity incidents within a specified timeframe, ensuring timely responses to threats.
- A proactive approach to cybersecurity, requiring continuous monitoring, incident reporting, and timely updates to address emerging threats and to mitigate cybersecurity risks.

- Collaboration between government and the private sector, enhancing the sharing of threat intelligence and best practices, which is crucial for defending against sophisticated cyberattacks.
- Development and maintenance of a comprehensive risk management program that includes cybersecurity as a core component.
- Providing Governments with the authority to intervene in the management of critical infrastructure during significant cyber incidents.
- Establishment of a register for critical infrastructure assets, providing the government with detailed information on ownership, operational control, and the security measures in place, including cybersecurity protocols.

3.2 Standards and Guidelines

Important features and strengths of the key standards and guidelines relevant to the cybersecurity of connected devices include:

- Standards and guidelines tend to be internationally recognised and widely recognised within the relevant industries. Some have been developed with a global intention, while others such as those developed by the US National Institute of Standards and Technology (NIST) have been developed with a US focus, but have been widely adopted in other locations as a best practice framework.
- Standards and guidelines are generally based on a systematic approach to managing sensitive information, ensuring the confidentiality, integrity and availability of data that is crucial for the cybersecurity of connected devices.
- The focus is generally on end-to-end security thus ensuring that every component of the IOT ecosystem from devices to networks and applications is secured. This includes a security by design philosophy requiring manufacturers to consider cybersecurity from the earliest stages of appliance design. This concept extends to full lifecycle security where there is a focus on maintaining security from design and development through to operation and finally decommissioning.
- Standards and guidelines tend to be comprehensive and applicable to a wide range of products e.g. IOT devices, control systems, sensors, data storage and communications systems and to a wide range of organization sizes and industry types.
- Standards and guidelines use a risk-based approach to identify potential security threats to connected devices and to implement appropriate controls and risk management strategies to mitigate these risks.
- They generally provide a framework for managing risks on a holistic basis and for continuous improvement.
- Some Standards and guidelines include certification and compliance aspects.
- Some Standards and guidelines focus on particular sectors such as information security management systems and energy management systems (ISO/IEC 27019).

- Standards and guidelines tend to offer scalability and flexibility allowing them to be adapted to different use cases and technologies and to small scale and large scale IOT deployments.
- Some Standards and guidelines outline key baseline cybersecurity measures that manufacturers should or must implement including addressing secure storage of credentials, secure communications, software update mechanisms and protection of personal data.
- Some Standards and guidelines include requirements for vulnerability disclosure policies for manufacturers to implement.
- There is generally a forward looking focus on emerging technologies recognizing the potential for emerging IOT technologies in this rapidly evolving field.

3.3 Codes of Practice/Other Initiatives

Important features and strengths of the key codes of practice and other initiatives relevant to the cybersecurity of connected devices include:

- While legislation and standards tend to be produced by Governments or by standards organizations such as ISO, codes of practice and other initiatives tend to be developed by a range of organizations and alliances, sometimes with Government backing and support.
- These initiatives and processes tend to be of a voluntary nature, rather than an Act or Standard that must be followed. Their strengths lie in a collaborative approach working with industry stakeholders, policymakers and academia.
- The intention is to promote security standards and certifications that ensure IoT products are secure, reliable and trusted by consumers and businesses. The ioXt Alliance includes a set of security pledges to help meet this objective.
- Initiatives tend to be focused on developing best practice frameworks of security principles that will improve the security of a wide range of IoT devices.
- There is a focus on security by design implementing security measures from the earliest stages of product development through to the entire lifecycle including regular updates and patch management.
- Initiatives generally include a risk assessment to assess and mitigate risks with devices, taking into account potential threats and impacts.
- Some initiatives include certification and compliance aspects.
- Cyber Trust Marks are offered in the USA and Singapore that certify or label connected devices to verify that they meet established cybersecurity standards. The UK has a Code of Practice for Consumer IoT Security which will lead to a cybersecurity label intended to inform consumers about the security level of IoT products.
- There is a focus on ensuring that security practices are transparent in nature and provide baseline security requirements such as eliminating default passwords which are often exploited in cyberattacks.

- Initiatives are generally applicable to a range of organization types and sizes and many initiatives are applicable to small to medium sized businesses seeking to cost-effectively improve their cybersecurity position.

3.4 Summary of Initiatives by Geographic Region

International

The following figures shows applicable acts, codes of practice and other initiatives and their applicability in various regions.

Figure 4: Cybersecurity standards, guidelines, codes of practice and other initiatives applicable globally

Europe

Figure 5: Cybersecurity standards, guidelines, codes of practice and other initiatives – applicable in Europe

North America

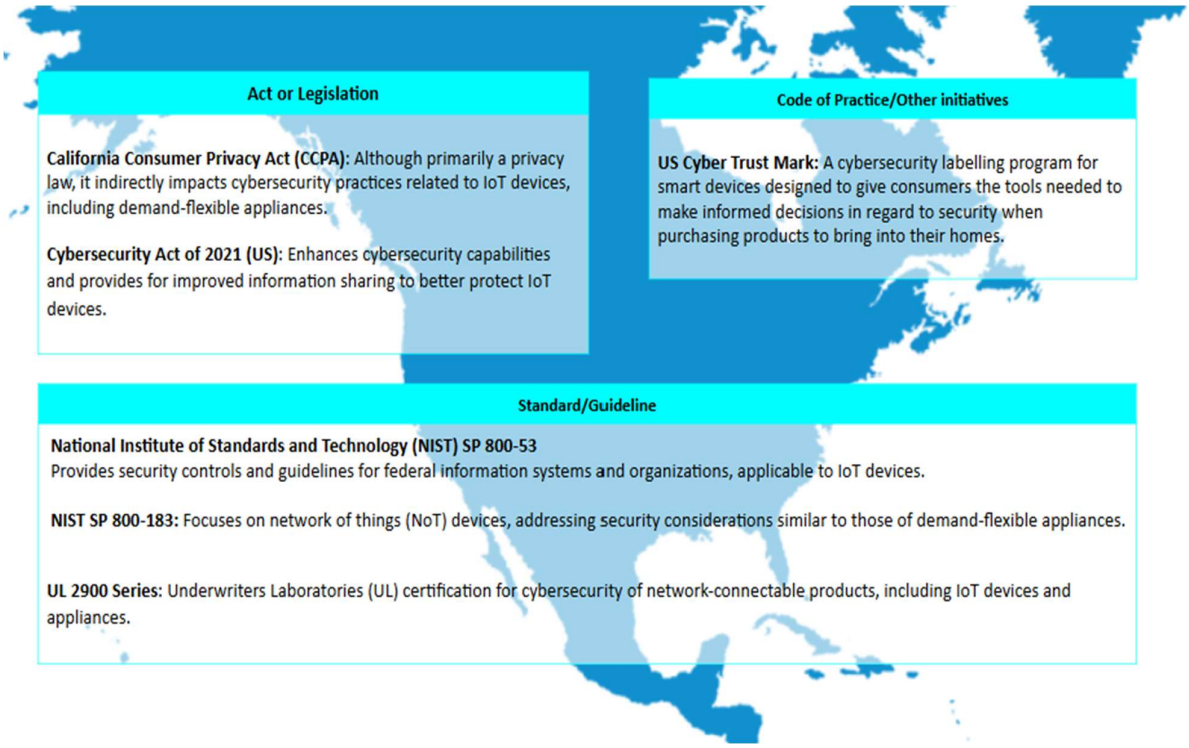


Figure 6: Cybersecurity standards, guidelines, codes of practice and other initiatives – applicable in North America

Asia

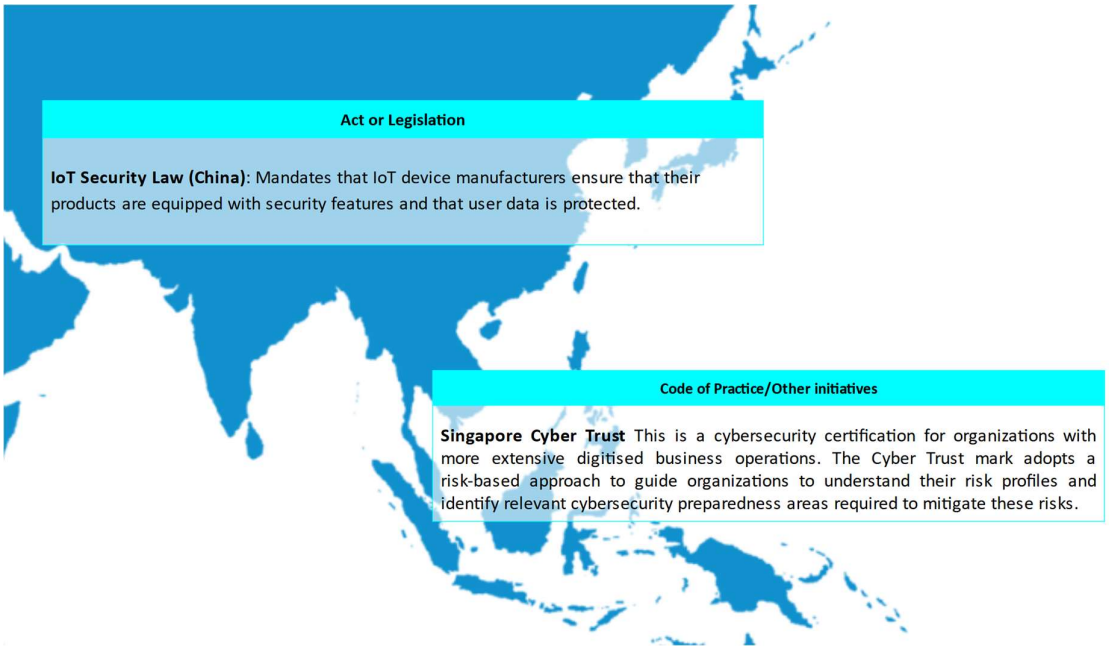


Figure 7: Cybersecurity standards, guidelines, codes of practice and other initiatives – applicable in Asia

4 Perspectives from Industry

As part of this work program, discussions were held with personnel working in a range of organizations, jurisdictions and activities relevant to cybersecurity in the electricity sector. This included organizations operating in the categories shown in Figure 8 below.

The purpose of these discussions was to gain perspectives from a range of industry participants on the cybersecurity of connected devices. It was not feasible, nor within the scope of this project, to interview personnel from a full range of these industries and across a comprehensive range of jurisdictions. A sample of organizations was chosen in a bid to obtain a cross-section of views on the main issues arising. The cooperation and contributions from the individuals spoken to is appreciated.

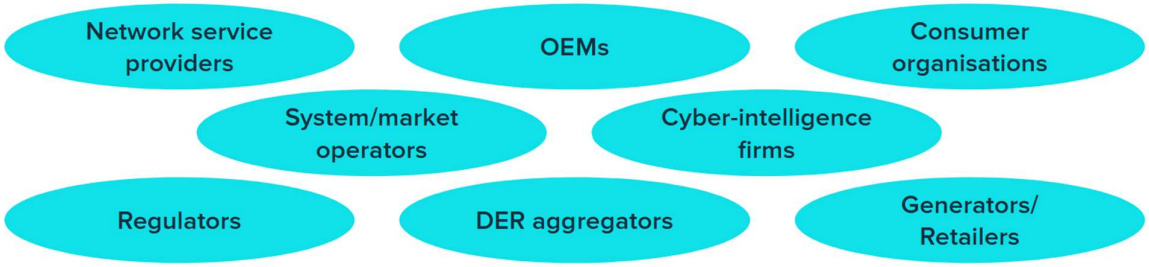


Figure 8: Industry categories where perspectives on cybersecurity were discussed

From these discussions, it was possible to identify key themes and issues faced by DFA stakeholders and these are summarized below:

Challenges faced by OEMs

- An OEM may not have any ongoing relationship with a purchaser once they've bought a device creating challenges on the monitoring and updating of security elements - and with that an inability to be responsible.
- The issue of explicit vs implicit control of devices was raised as a key area for OEMs to manage. Explicit control is where the OEM has control of the device and implicit control is where another actor has control of the device to manage electricity demand or price.
- Allowing integration with OEM systems, and potentially ceding control of their devices to a third party, introduces operational/reputational risk to OEMs.
- In general, every smart grid device which is either producing energy or consuming energy could be used as a vector to destabilize the connected grid, and therefore OEMs should be assessed in line with the real risk of this device - rather than foist cybersecurity obligations onto OEMs when utilities may not have their 'house in order'.
- Any variations in cybersecurity obligations and standards between jurisdictions creates cost. There are jurisdictions which are creating and enforcing obligations on OEMs but with no commensurate price recovery mechanism.
- A high focus on product security should start at the very beginning of the product development lifecycle, including consideration of the principles of security by design and security by default.

- There needs to be an industry discussion on cybersecurity, although OEMs are typically sceptical that this can occur cross-jurisdiction.

Current and anticipated cybersecurity threats, existing mitigation strategies, and gaps/opportunities in current practices

- There is a need for a national (at least), or preferably a global, approach. Many DFA vendors are global technology companies delivering product lines across multiple continents.
- The scale of both the risk and effort needed to mitigate that risk should not be underestimated. While this varies materially across jurisdictions; it involves millions of devices and GW of capacity. This is set to grow at an accelerating rate as well as adding emerging technology types such as vehicle to grid (V2G).
- When considering mechanisms for threat detection and alerting, acknowledgment must be made of the huge amounts of data (commands, telemetry, other information) which are generated across fleets of hundreds of thousands of devices.
- There is a need to consider how quickly to address a threat or event after becoming aware of it, and what the consequences of any delay may be, e.g. EV charger outages will eventually result in personal mobility restrictions.
- There is a need to consider and develop a risk assessment criteria which could be used to inform a 'Data Driven Regulation' approach to categorize supplier risk and obligate vendors and roles based upon their risk.
- There is a need to ensure compliance by OEMs with (European) cybersecurity legislation.
- Consumers can't be expected to be cognisant of the cybersecurity risks. The risks should lie with those that are best positioned and resourced to manage the risk.
- Manipulation of customer accounts could leak or steal personal information e.g. geolocation, address, account details of the end customer or associated service provider.
- Data protection and separation is an important consideration. Customer data and system data should be stored separately to avoid cyberattacks.
- Standardization in the data models used for DFA management Consider potential standardization of the way in which DFA are managed will reduce the cost and complexity of cybersecurity threat detection and incident response.
- Inverters installed in Australia/NZ need to comply with AS/NZS4777, but this does not address cybersecurity aspects.

Market Operators and DNSPs' experiences in DFA integration, cybersecurity concerns, and the impact of potential threats to grid reliability

- Consider how we identify behaviour that is outside of expectations, and assess this in the light of what may be caused by a genuine infrastructure issue or fault, rather than an attack. DNSPs will need to have sufficient visibility of their network to help determine this.
- Consider the impact on the spot market of aggregated load. Materiality is the key issue. MW of DFA as a proportion of the asset capacity could be used as the basis of a risk assessment. Use a graduated assessment of risk, rather than simply a binary approach,

e.g. low MW = low risk, high MW = high risk approach. Risk assessment may also need to be considered in the context of the size of the local market.

- Think in terms of considering the magnitude of what harm can be done if a device was being operated incorrectly.
- DFA limits and bounds need to be tightly defined. Consider proportional control/response e.g. if a limit is exceeded by any multiple then this is likely to be a problem.
- Consider the ability to isolate a device(s) when performance goes outside established boundaries.
- Consider the nature and impact on customers. Disruption to hot water may mean a cold shower which is inconvenient, but disruption to EV chargers may mean the loss of mobility with a range of consequences arising from that.
- Consider how many customers are affected when dealing with aggregators. This will impact on the risk. Need to differentiate a single asset from aggregated assets and treat them as different types of risk.
- Consider the impact or significance of fake signals to a device compared with other market threats such as faking a market signal.
- DFA cybersecurity can't just be left to the market to address.
- PKI is the way to provide a solution to give a level of trust and predictability, ideally delivered by a national entity with sovereign capability to standardize and harmonize procedures. A centralised model should also be cheaper to deliver, although does have an impact on cybersecurity risk through common mode failure.

Device registration and managing access to data and control of these devices both within jurisdictions and internationally

- Cybersecurity of DFA is an international issue. Australia has a lot of DFA, but is small in the context of the OEM market, so there is a need to work within a global system.
- Consideration needs to be given not just to DFA or the connected networks or market systems, but also to other connecting infrastructure e.g. telecommunications networks, cloud infrastructure etc.
- Understanding versioning of technologies from the utility server down to the device firmware is important. Tracking and managing device firmware for a single vendor is complex, dealing with this across global DFA systems will be much more complex.
- PKI[6] could be part of authentication/certification.
- The success rate of dispatch commands can be as low as 85% owing to poor Wi-Fi coverage and lack of customer engagement.
- It is useful to consider whether OEMs should have the right to produce their own cybersecurity certificates and work on the basis that products meet the required standard unless disproven, so as to avoid continually checking.

[6] Public Key Infrastructure – as described in Appendix 1

Challenges faced by retailers in managing consumer data privacy and security in the context of DFA technologies

- Retailers typically have no visibility of device firmware updates. A real issue is understanding versioning of technologies from the utility server right down to device firmware.
- There are already legislative requirements in relation to customer privacy.
- Consider whether policies should be applied at an OEM level or aggregator level, or (more likely) both.

Cross industry reflections on device-specific vulnerabilities, existing security features, and future plans for enhancing cybersecurity

- Need to consider where to draw the line with different technologies. It is useful to consider what the primary function of an item is and how related it is to electricity. For example, the primary function of a dishwasher is not electricity grid related. At the other end of the scale are batteries and PV. Other products such as EVs and EV chargers come in between.
- A global approach is required. DFA vendors are typically global technology companies and the more common regulations, standards and approaches apply across jurisdictions, thus lowering compliance costs and improving the efficacy of those solutions.
- There is a shift from highly trusted OT systems to operating in a trustless environment over the internet.
- V2G will become a significant factor in the short to medium term and it will be important to ensure that this is addressed.
- Servers can be made to appear as though they are in another country.
- Some classes of devices have never been regulated.
- Any monitoring must be independent, i.e. can't trust a device to monitor that device. Monitoring should be provided by a product from another vendor.

5 Summary and Conclusions

The rapid and relentless growth of DFA is transforming the energy landscape, offering new and exciting opportunities for grid flexibility to support the broader energy transition. However, this transformation also introduces cybersecurity challenges that must be addressed to ensure the reliability, resilience, and security of our energy systems. This chapter synthesizes the key findings from our examination of DFA cybersecurity, reflecting on the risks, current landscape, industry perspectives, emerging threats, and existing policy frameworks.

As we navigate this complex terrain, it becomes clear that the cybersecurity of DFA is not just a technical challenge, but a multifaceted issue that intersects with policy, economics, and social considerations. The scale of DFA adoption – with millions of devices being connected to power grids worldwide – amplifies both the potential benefits and the risks. Our analysis reveals a sector in transition, grappling with the need to balance innovation and security. Action needs to be taken to address these challenges whether between jurisdictions, or between stakeholders in specific classes of DFA.

5.1 DFA Represents Specific Risks

The integration of DFA into our energy infrastructure presents a specific set of risks that differ from those associated with traditional, centralized power systems. Key observations include:

- **Scale and Diversity:** The sheer number and variety of DFA devices – from solar inverters and battery storage systems to electric vehicle chargers and smart appliances – create an expansive and diverse attack surface paired with traditional electricity assets (networks and generators). This diversity provides potentially millions of entry points for malicious actors and complicates security efforts, as different device types may require different security approaches.
- **Aggregation Risks:** While individual DFA devices may have limited impact, the aggregation of thousands or millions of devices can pose significant risks to grid stability if compromised. This risk is particularly acute as DFA aggregation reaches gigawatt scale in some markets.
- **Consumer Interface:** Many DFA devices are owned and operated by consumers, introducing human factors and potential vulnerabilities that are less prevalent in traditional energy infrastructure. Consumer behaviour, awareness, and privacy concerns all play crucial roles in the overall security posture.
- **Rapid Technological Evolution:** The fast pace of technological change in the DFA sector means that security measures must be adaptable and forward-looking. What's secure today may not be sufficient tomorrow.
- **Market and Operational Impacts:** Cybersecurity breaches in DFA systems could have far-reaching consequences beyond just energy supply, potentially affecting energy markets, pricing, and even broader economic stability.

These risk factors underscore the need for a comprehensive, risk-based approach to DFA cybersecurity that can adapt to the evolving threat landscape.

5.2 The DFA Cybersecurity Landscape is complex and evolving

Our examination of the current DFA cybersecurity landscape reveals a sector that is not just complex, but is continuing to evolve, with several key characteristics:

- **Fragmentation:** The current approach to DFA cybersecurity is often fragmented, with varying standards and practices across different regions and device types. This lack of uniformity creates potential vulnerabilities and complicates efforts to implement comprehensive security measures.
- **Utilities grappling with the shift from Operational Technology (OT) to Information Technology (IT):** The integration of DFA is driving a significant shift from traditional (OT) to IT-centric, cloud based, approaches. This transition introduces new security challenges, as many utilities and grid operators are more accustomed to dealing with closed, proprietary OT systems rather than open, interconnected IT systems.
- **Emerging Standards:** While several standards and protocols (such as IEEE 2030.5, IEC 61850, and OpenADR) are emerging to address DFA integration and communication, there is still a lack of comprehensive, globally accepted cybersecurity standards specific to DFA.
- **Supply Chain Concerns:** The global nature of DFA device manufacturing introduces supply chain risks that need to be addressed. Ensuring the integrity of devices and software throughout the supply chain is a growing concern.
- **Data Privacy and Security:** The vast amount of data generated by DFA devices raises significant privacy and security concerns. Balancing the need for operational data with consumer privacy rights remains a challenge.
- **Cloud and Edge Computing:** The increasing use of cloud and edge computing in DFA management introduces new security considerations, particularly around data transmission and storage.

This evolving landscape highlights the need for a more coordinated, standardized approach to DFA cybersecurity that can address these challenges while fostering innovation and growth in the sector.

5.3 Perspectives from Industry are Varied and Focused on Outcomes

Our engagement with industry stakeholders across various sectors – including utilities, DFA manufacturers, aggregators, and cybersecurity firms – revealed several key themes:

- **Varied Maturity Levels:** There is a wide range of cybersecurity maturity levels across the industry. While some organizations have sophisticated security measures in place, others are still in the early stages of addressing DFA-specific cybersecurity challenges.
- **Economic Considerations:** Many stakeholders, particularly device manufacturers, expressed concerns about the economic impact of implementing robust cybersecurity measures. There's a perceived tension between security requirements and maintaining competitive pricing.
- **Regulatory Uncertainty:** Industry players often cited the lack of clear, consistent regulatory frameworks as a challenge. There's a desire for more guidance and standardization, but also concerns about overly prescriptive regulations stifling innovation.

- **Interoperability Challenges:** The need for interoperability between different DFA devices and systems was frequently mentioned as both a necessity and a security challenge. Balancing openness for interoperability with security is an ongoing concern.
- **Skill Gap:** Many organizations reported difficulties in finding and retaining cybersecurity talent with specific expertise in DFA and energy systems. This skill gap is seen as a significant barrier to improving security postures.
- **Incident Response Preparedness:** While larger utilities often have incident response plans in place, many smaller players in the DFA ecosystem lack comprehensive plans for dealing with cybersecurity incidents.
- **Information Sharing:** There was broad agreement on the need for better information sharing mechanisms within the industry, but also concerns about potential competitive disadvantages and legal liabilities associated with sharing sensitive information.

These industry perspectives highlight the complex interplay of technical, economic, and organizational factors that influence DFA cybersecurity practices and point to the need for collaborative, industry-wide approaches to addressing these challenges.

5.4 Current and Future Threats are Broad and Real

Our analysis of the threat landscape for DFA systems reveals a range of current vulnerabilities and emerging threats:

- **Device-level Vulnerabilities:** Many current DFA devices lack robust security features, such as secure boot processes, encrypted communications, or regular security updates. These vulnerabilities could be exploited to gain unauthorized access or control.
- **Communication Protocol Exploits:** Weaknesses in communication protocols used by DFA systems, particularly those based on older standards, present opportunities for man-in-the-middle attacks or unauthorized command injection.
- **Aggregation Attacks:** As DFA aggregation becomes more prevalent, the potential impact of coordinated attacks on multiple devices increases. Such attacks could potentially destabilize grid operations or manipulate energy markets.
- **Advanced Persistent Threats (APTs):** State-sponsored actors and sophisticated cybercriminal groups are showing increasing interest in energy infrastructure, including DFA systems. These APTs can remain undetected in systems for long periods, gathering intelligence or waiting to cause disruption.
- **AI and Machine Learning Threats:** The growing use of AI in both attack and defence mechanisms is likely to lead to more sophisticated, automated attacks that can adapt to defensive measures in real-time.
- **Quantum Computing Risks:** While still on the horizon, the advent of practical quantum computing could potentially break many current encryption methods, necessitating the development of quantum-resistant security measures.
- **Supply Chain Attacks:** The complex, global supply chains for DFA devices and software components present opportunities for the insertion of malicious code or hardware, potentially compromising devices before they're even installed.

- **Social Engineering and Insider Threats:** As DFA systems involve more human interactions, particularly at the consumer level, the risk of social engineering attacks and insider threats increases.
- **IoT Botnet Exploitation:** The large number of connected DFA devices presents an attractive target for botnet operators, who could use compromised devices for distributed denial-of-service (DDoS) attacks or other malicious activities.
- **Firmware and Software Update Vulnerabilities:** The process of updating firmware and software in DFA devices, if not properly secured, could be exploited to distribute malware or unauthorized modifications.

These current and emerging threats underscore the need for a proactive, adaptive approach to DFA cybersecurity that can anticipate and respond to evolving attack vectors.

5.5 Review of Current Policies and Standards

Our examination of existing policies, standards, and initiatives related to DFA cybersecurity reveals a complex and evolving regulatory landscape:

- **Regional Variations:** There are significant differences in approach across different regions. For example, the European Union's Network Code on Cybersecurity provides a comprehensive framework for energy cybersecurity, while approaches in other regions may be more fragmented.
- **Sectoral Standards:** Several industry-specific standards, such as IEC 62351 for power systems management and associated information exchange, provide valuable guidance but may not fully address the challenges of DFA.
- **General Cybersecurity Frameworks:** Broader cybersecurity frameworks such as the NIST Cybersecurity Framework are often applied to DFA systems but may require adaptation to fully address DFA-specific issues.
- **Emerging DFA-Specific Guidelines:** Initiatives like the IEEE 1547-2018 standard for interconnection and interoperability of DFA with associated electric power systems are beginning to address DFA-specific cybersecurity concerns, but implementation and adoption remain inconsistent.
- **Critical Infrastructure Protection:** In many jurisdictions, large-scale DFA are increasingly being considered as critical infrastructure, subject to more stringent cybersecurity regulations. However, the treatment of smaller, distributed systems remains less clear.
- **Data Protection Regulations:** General data protection regulations, such as GDPR in the EU, have implications for DFA cybersecurity, particularly regarding the handling of consumer energy usage data.
- **Voluntary vs. Mandatory Measures:** There is a mix of voluntary guidelines and mandatory requirements across different jurisdictions, leading to potential inconsistencies in implementation.
- **Certification and Compliance:** Some regions are moving towards cybersecurity certification schemes for DFA devices, but these are not yet widely adopted or standardized globally.

This review highlights the need for more harmonized, comprehensive policies and standards that can address the specific cybersecurity challenges of DFA while promoting innovation and interoperability.

5.6 Conclusions

The discussion of DFA cybersecurity reveals a complex, multifaceted challenge that sits at the intersection of technology, policy, and market dynamics. As DFA continue to proliferate and play an increasingly critical role in our energy systems, the imperative to address these cybersecurity challenges becomes ever more urgent.

Key themes include:

- The need for a risk-based, adaptive approach to security that can keep pace with the rapid evolution of both DFA technologies and cyber threats.
- The importance of international cooperation and standardization to address the global nature of DFA supply chains and cyber threats.
- The challenge of balancing security requirements with the need for interoperability, innovation, and cost-effectiveness in DFA systems.
- The critical role of human factors, including consumer awareness and industry expertise, in maintaining robust cybersecurity postures.
- The necessity of developing comprehensive, DFA-specific cybersecurity frameworks that can guide policy, standards, and industry practices.

As we move forward, it's clear that addressing DFA cybersecurity will require a collaborative effort involving policymakers, industry stakeholders, researchers, and consumers. The path ahead involves not just technical solutions, but also the development of robust governance frameworks, economic models that incentivize security, and educational initiatives to build cybersecurity awareness and expertise across the DFA ecosystem.

The security of our evolving, distributed energy systems is paramount not just for the stability of our power grids, but for the broader economic and social systems that depend on reliable, secure energy. As we continue to harness the transformative potential of DFA, ensuring their cybersecurity must remain a top priority, driving innovation, collaboration, and continuous improvement in our approach to protecting these critical systems.

6 The Way Forward

The rapid growth of DFA is transforming the global energy landscape, offering both opportunities and significant cybersecurity challenges. Addressing these challenges is crucial to ensure the reliability, resilience, and security of our evolving energy systems.

The recommendations presented in this chapter represent an idealized roadmap for enhancing DFA cybersecurity. They are the result of comprehensive analysis and stakeholder input, distilled into actionable strategies. However, it is important to recognize that implementing these recommendations, particularly on a global scale, will be challenging due to differing regulatory environments, technological landscapes, and national priorities.

We strongly advocate for individual jurisdictions to address each recommendation, adapting them to local conditions while actively seeking opportunities for international coordination. This dual approach – localized implementation coupled with global harmonization – offers the best chance of creating a robust and secure global DFA ecosystem.

These recommendations are designed to be flexible objectives rather than prescriptive solutions, allowing for adaptation to rapid technological changes and evolving threats. They span a range of actions, from technical measures like implementing a global Public Key Infrastructure (PKI) for DFA, to policy-oriented steps such as developing risk-based cybersecurity standards, and operational strategies like establishing comprehensive incident response plans.

By addressing these recommendations, stakeholders can significantly enhance the cybersecurity posture of DFA systems, ensuring their resilience and trustworthiness as they become increasingly integral to our energy infrastructure. The following sub-sections will explore each recommendation in detail, outlining its importance, benefits, and key considerations.

6.1 Implement a Global Public Key Infrastructure (PKI) for DFA

PKI is crucial for securing communication between DFA devices, utilities, and aggregators. It provides a framework for authentication, encryption, and non-repudiation, addressing key cybersecurity challenges in DFA integration.

Why it's important: As DFA systems become more interconnected and complex, the need for secure, authenticated communication becomes paramount. Without a robust PKI system, DFA networks are vulnerable to man-in-the-middle attacks, unauthorized access, and data tampering.

Benefits of implementation:

- Enhanced security through strong authentication and encryption
- Improved interoperability between different DFA systems and manufacturers
- Increased trust in DFA communications, facilitating greater adoption and integration
- Reduced risk of cyberattacks that could destabilize the grid or compromise user data

Key elements include:

- Establish an international working group for PKI standards
- Create hierarchical certifying authority structure

- Develop certificate management protocols
- Implement automated systems

Considerations:

- Ensuring interoperability between different regions and manufacturers
- Managing the computational overhead on resource-constrained DFA devices
- Addressing the costs associated with implementing and maintaining PKI systems

6.2 Develop Risk-Based Cybersecurity Standards for DFA

The impact of cyberattacks can vary greatly depending on the size and type of DFA. A risk-based approach ensures that security measures are proportional to the potential threat.

Why it's important: Not all DFA systems pose the same level of risk to the grid or to user privacy. By tailoring security requirements to the specific risk profile of different DFA types and sizes, we can achieve a balance between security and practicality.

Benefits of implementation:

- More efficient allocation of cybersecurity resources
- Reduced burden on smaller DFA operators while maintaining high security for critical systems
- Increased adoption of DFA due to right-sized security requirements
- Improved overall resilience of the DFA ecosystem

Key elements include:

- Create risk assessment template
- Establish tiered security requirements
- Develop standards for high-risk DFA
- Implement regular risk reassessments

Considerations:

- Balancing security needs with the cost burden on manufacturers and operators
- Ensuring standards are flexible enough to accommodate technological advancements
- Harmonizing risk assessment methodologies across different jurisdictions

6.3 Establish International DFA Cybersecurity Information Sharing

Cybersecurity threats evolve rapidly, and sharing information about vulnerabilities and attacks is crucial for maintaining a robust defence.

Why it's important: Cyber threats in the DFA space are often global in nature. An attack method used in one region could quickly spread to others. Rapid sharing of threat intelligence and mitigation strategies is essential for staying ahead of potential attackers.

Benefits of implementation:

- Faster response to emerging threats
- Improved collective defence against cyberattacks
- Reduced duplication of effort in threat analysis and mitigation
- Enhanced global cooperation in DFA cybersecurity

Key elements include:

- Create secure platform for threat intelligence
- Establish rapid information dissemination protocols
- Develop anonymization techniques
- Organize international cybersecurity exercises

Considerations:

- Overcoming potential reluctance to share sensitive information
- Ensuring the platform itself is secure against attacks
- Managing information flow to prevent overwhelming smaller stakeholders

6.4 Mandate Secure-by-Design Principles for DFA Manufacturers

Integrating security from the earliest stages of product development is more effective and cost-efficient than retrofitting security measures.

Why it's important: Many cybersecurity vulnerabilities stem from design flaws that are difficult and expensive to fix after a product is deployed. By mandating secure-by-design principles, we can significantly reduce the attack surface of DFA devices from the outset.

Benefits of implementation:

- Reduced long-term costs for security maintenance and updates
- Improved consumer confidence in DFA technologies
- Decreased likelihood of large-scale cyber incidents
- Faster and easier security certifications for compliant devices

Key elements include:

- Develop DFA-specific secure-by-design guidelines
- Implement certification processes
- Provide manufacturer training and resources
- Establish "Cyber Trust Mark" for compliant devices

Considerations:

- Balancing security requirements with time-to-market pressures
- Ensuring guidelines are flexible enough to accommodate innovation
- Managing the cost impact on smaller manufacturers

6.5 Implement Incident Response and Recovery Plans for DFA

Given the potential for widespread impact from DFA-related cyberattacks, having robust incident response and recovery plans is crucial.

Why it's important: In the event of a successful cyberattack, the speed and effectiveness of the response can significantly mitigate damage. Well-prepared incident response plans can mean the difference between a minor disruption and a major grid failure.

Benefits of implementation:

- Minimized downtime and financial losses in case of an attack
- Improved stakeholder confidence in DFA resilience
- Enhanced coordination between different entities during a crisis
- Valuable insights from post-incident analysis to prevent future attacks

Key elements include:

- Develop DFA-specific incident response templates
- Establish clear communication lines
- Conduct regular drills and simulations
- Create rapid isolation mechanisms

Considerations:

- Coordinating response efforts across multiple stakeholders and jurisdictions
- Balancing the need for rapid response with thorough investigation and evidence preservation
- Ensuring plans are adaptable to various types and scales of incidents

6.6 Develop and Enforce Interoperable Cybersecurity Standards for DFA

The global nature of DFA manufacturing and deployment necessitates harmonized standards to ensure consistent security across different regions and device types.

Why it's important: Inconsistent security standards across different regions create vulnerabilities and increase costs for manufacturers and operators. Harmonised standards can improve overall security while reducing complexity and expense.

Benefits of implementation:

- Simplified compliance processes for global manufacturers
- Improved interoperability between different DFA systems
- Reduced costs through economies of scale in security implementation
- Enhanced overall security posture of the global DFA ecosystem

Key elements include:

- Form international consortium for standards development

- Align with existing frameworks
- Create compliance testing and certification process
- Establish regular review mechanisms

Considerations:

- Navigating different regulatory environments across jurisdictions
- Ensuring standards are flexible enough to accommodate rapid technological change
- Balancing comprehensive security with the need for simplicity and ease of implementation

6.7 Continuous Monitoring & Adaptive Security Measures for DFA

The dynamic nature of both DFA systems and cyber threats requires an ongoing, adaptive approach to security.

Why it's important: Static security measures quickly become obsolete in the face of evolving threats and changing DFA landscapes. Continuous monitoring and adaptive security ensure that defences remain effective over time.

Each jurisdiction will have to consider the most appropriate institution or organisation to undertake such monitoring. Additionally, consideration may be given to the require for cross border monitoring and co-ordination.

Benefits of implementation:

- Real-time threat detection and mitigation
- Improved visibility into DFA system behavior and anomalies
- Ability to quickly adapt to new threats or vulnerabilities
- Enhanced long-term resilience of DFA systems

Key elements include:

- Develop real-time monitoring protocols
- Implement AI/ML for threat detection
- Establish rapid security update processes
- Create ongoing security assessment framework

Considerations:

- Managing the large volumes of data generated by continuous monitoring
- Ensuring privacy and data protection in monitoring activities
- Balancing autonomous security responses with human oversight

7 References

200,000 Colorado Springs Utilities notified after unauthorized data access of subcontractor's system – DataBreaches.Net

A Security Architecture for 5G Networks | IEEE Journals & Magazine | IEEE Xplore

Cost of a data breach 2024 | IBM

Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures — TU Delft Research Portal

Cybersecurity and Distributed Energy Resources | National Renewable Energy Laboratory (NREL)

Cybersecurity and Distributed Energy Resources (nrel.gov)

Cybersecurity – is the power system lagging behind? – Analysis - IEA

https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind

Cybersecurity Strategy for Distributed Energy Resources and Inverter-Based Resources | U.S. Department of Energy

Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid.pdf

Enhancing cyber resilience in electricity systems – Analysis - IEA

European Wind-Energy Sector Hit in Wave of Hacks - WSJ

How hackers target smart meters to attack the grid (smart-energy.com)

IBM Security Report: Energy Sector Becomes UK's Top Target for Cyberattacks as Adversaries Take Aim at Nation's Critical Industries

Towards Secure and Intelligent Network Slicing for 5G Networks | IEEE Journals & Magazine | IEEE Xplore

Unlocking the Potential of Distributed Energy Resources | IEA May 2022

https://www.iea.org/reports/unlocking-the-potential-of-distributed-energy-resources/executive-summary

8 Glossary

Term	Details
AESCSF	Australian Energy Sector Cybersecurity Framework
APT	Advanced persistent threats
BESS	Battery Energy Storage System
Botnet	Short for “robot network” - a network of computers infected by malware that are under the control of a single attacking party.
Blockchain	The underlying technology that constructs a decentralized digital ledger that enables exchanges between multiple parties in a secure, irreversible manner.
CER	Consumer Energy Resources
Cloud based technologies	The delivery of computing services, including servers, storage, databases, networking, software, analytics, and intelligence over the Internet
CSIP	Common Smart Inverter Profile
CSIP-Aus	Common Smart Inverter Profile - Australia
DDoS	Distributed denial-of-service
DER	Distributed Energy Resources
DFA	Demand Flexible Appliances
DNSP	Distributed Network Service Provider.
Firmware	A form of microcode or program embedded into hardware devices to help them operate effectively.
GDPR	General Data Protection Regulation
HEMS	Home Energy Management System
IoT	Internet of Things - The collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.
IT	Information Technology
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Term	Details
MATTER	Build With Matter | Smart Home Device Solution - CSA-IOT (Connectivity Standards Alliance Internet of Things)
OCPP	Open Charge Point Protocol
OEM	Original Equipment Manufacturer
OpenADR	Open Automated Demand Response
OT	Operational Technology
Phishing	A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.
PKI	Public Key Infrastructure (PKI) is a system of digital certificates, certificate authorities, and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction.
Quantum computing	An area of computing focused on developing computer technology based on the principles of quantum theory, which explains the behaviour of energy and material on the atomic and subatomic levels and is used to solve complex problems that classical computers or supercomputers can't solve, or can't solve quickly enough.
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
SIEM	Security Information and Event Management
State based actor	A person or group acting on behalf of a government or government body.
TLS	Transport Layer Security (TLS)
VPN	Virtual Private Network
VPP	Virtual Power Plant - the aggregation of a large number of small devices which, when operated as a fleet, can have similar performance to that of a traditional power plant.
ZSS	Zone Substation

Appendix 1: An Overview of PKI

Public Key Infrastructure (PKI) is a system of digital certificates, certificate authorities, and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction. In the context of Demand Flexible Appliances (DFA) in the electricity sector, PKI plays a crucial role in ensuring secure, authenticated, and encrypted communications between NSPs, Retailers (or other DFA aggregators who require visibility or control of those assets) and the DFA OEMs.

The integration of DFA into the power grid presents several cybersecurity challenges:

1. Device Authentication: Ensuring that only authorized devices can connect to the grid.
2. Data Integrity: Protecting against unauthorized modifications of data in transit.
3. Confidentiality: Safeguarding sensitive information from unauthorized access.
4. Non-repudiation: Preventing denial of sent commands or data.

PKI addresses these challenges by providing a framework for secure communication:

- Digital Certificates: PKI uses digital certificates to authenticate the identity of devices and systems. Each DFA device is issued a unique digital certificate that serves as its digital identity.
- Public and Private Keys: PKI utilizes asymmetric cryptography, where each entity has a pair of keys - a public key and a private key. The public key is freely distributed, while the private key is kept secret.
- Certificate Authorities (CAs): These trusted entities issue and manage digital certificates. In the DFA context, utilities or grid operators often act as CAs.
- Certificate Revocation Lists (CRLs): CRLs allow for the revocation of compromised or obsolete certificates, enhancing security.

Implementation of PKI in DFA systems

Implementation of PKI will involve the following steps:

1. Certificate Issuance: When a new DFA device is installed, it's issued a digital certificate by the CA after verifying its identity and credentials.
2. Mutual Authentication: Before establishing a connection, both the DFA device and the grid management system authenticate each other using their digital certificates.
3. Secure Communication: Once authenticated, communications are encrypted using the public key of the recipient, ensuring confidentiality.
4. Digital Signatures: Commands and data are digitally signed using the sender's private key, ensuring integrity and non-repudiation.

Benefits of PKI in DFA

- Enhanced Security: PKI provides a robust security framework that protects against various cyber threats.
- Scalability: As more DFA devices are added to the grid, PKI can scale to accommodate the growing number of devices.

- Interoperability: PKI standards enable secure communication between devices from different manufacturers.
- Regulatory Compliance: PKI helps utilities comply with cybersecurity regulations and standards.

Challenges in Implementing PKI for DFA

- Complexity: PKI systems can be complex to set up and manage, especially for smaller utilities.
- Cost: Implementing and maintaining a PKI system can be expensive.
- Performance: The computational overhead of cryptographic operations may impact the performance of resource-constrained DFA devices.
- Certificate Management: Managing the lifecycle of certificates for numerous DFA devices can be challenging.

Standards and Protocols

Several standards and protocols support the implementation of PKI in DFA systems:

- IEC 62351: This standard specifies security requirements for power system management and information exchange.
- IEEE 2030.5: Also known as Smart Energy Profile 2.0, this standard defines a protocol for applications such as smart energy management and DFA integration.
- X.509: This standard defines the format of public key certificates used in PKI.

Future Trends

As DFA adoption continues to grow, we can expect to see the following developments in PKI implementation:

- Automated Certificate Management: To handle the increasing number of DFA devices, automated systems for certificate issuance, renewal, and revocation will become more prevalent.
- Edge Computing: PKI systems may evolve to better support edge computing architectures, where more processing is done closer to DFA devices.

Conclusion

In conclusion, PKI plays a vital role in securing the communication and control of Demand Flexible Appliances in the electricity sector. As the power grid becomes more decentralized and complex, the importance of robust cybersecurity measures like PKI will only increase. While challenges exist in implementation and management, the benefits of enhanced security, scalability, and interoperability make PKI an essential component of modern DFA systems. As technology evolves, PKI systems will need to adapt to meet new security challenges and support the continued growth of Demand Flexible Appliances.

Appendix 2: Key Concepts in Cybersecurity

Concepts

Below is an outline of some of the key concepts in cybersecurity. When engaging with Cybersecurity personnel, communicating with these concepts is important to establish mutual understanding.

Asset: An asset is anything of value to an organization, including hardware, software, data, and even personnel. Assets are what threats target and what cybersecurity measures aim to protect.

Example: A database containing customer information is a critical asset for many businesses.

Attack Vector: An attack vector is the method or pathway that a threat actor uses to gain unauthorized access to a network or system. It's essentially the route by which a threat can exploit a vulnerability.

Example: Phishing emails are a common attack vector used to trick users into revealing their login credentials.

Control: A control is a safeguard or countermeasure designed to avoid, detect, counteract, or minimize security risks. Controls can be technical, administrative, or physical.

Example: A firewall is a technical control that helps protect a network from unauthorized access.

Exploit: An exploit is a piece of software, chunk of data, or sequence of commands that takes advantage of a vulnerability to cause unintended or unanticipated behaviour in a system.

Example: A zero-day exploit takes advantage of a previously unknown vulnerability.

Impact: Impact refers to the magnitude of harm that can result from the exploitation of a vulnerability by a threat. It's the consequence or outcome of a successful attack.

Example: The impact of a ransomware attack could include financial losses, operational disruption, and reputational damage.

Incident: An incident is an event that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information it processes, stores, or transmits.

Example: A successful phishing attack that results in compromised user credentials is an incident.

Mitigation: Mitigation refers to the actions taken to reduce the severity of a risk or the impact of a successful attack. It involves implementing controls to address vulnerabilities and reduce the likelihood or impact of threats.

Example: Implementing multi-factor authentication mitigates the risk of unauthorized access due to stolen passwords.

Risk: Risk is the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. It's often expressed as a function of the likelihood of an event occurring and its potential impact.

Risk = Likelihood x Impact

Example: The risk of a data breach due to weak passwords is high if the likelihood of exploitation is high and the potential impact is severe.

Threat: A threat in cybersecurity is a potential danger that could exploit a vulnerability in a system, network, or asset. It's any circumstance or event that has the potential to cause harm to an organization's IT infrastructure or data.

Example: A hacker group with the intent to steal sensitive data is a threat.

Vulnerability: A vulnerability is a weakness or flaw in a system, network, or application that could be exploited by a threat to gain unauthorized access or perform unauthorized actions.

Example: An unpatched software vulnerability could allow an attacker to execute malicious code on a system.

To illustrate how these terms interrelate:

A threat actor (e.g. a hacker group) might use an attack vector (such as a phishing email) to exploit a vulnerability (such as a user's lack of security awareness) in an asset (e.g., the email system). This creates a risk (potential for unauthorized access) which, if realized, could lead to an incident (actual data breach) with significant impact (financial loss, reputational damage). To address this, the organization might implement controls (security awareness training, email filters) as part of their mitigation strategy to reduce the risk.

Appendix 3: Trustless Computing and DFA Cybersecurity

Trustless computing is a paradigm that aims to minimize the need for trust between parties in a distributed system. In the context of cybersecurity for Demand Flexible Appliances (DFA), this concept is particularly relevant as it addresses the challenges of securing a decentralized network of energy resources without relying on a single trusted authority.

Key aspects of trustless computing in DFA cybersecurity:

Decentralization

Trustless systems distribute control and decision-making across multiple nodes in the network. For DFA, this means that instead of relying on a central utility or grid operator to manage all aspects of energy distribution and security, control is shared among various participants.

Example: Each DFA device (solar panel, BESS, etc.) can have its own decision-making capabilities based on predefined rules and real-time data.

Consensus Mechanisms

These are protocols that ensure all nodes in the network agree on the state of the system without needing to trust each other. In DFA, consensus mechanisms can be used to validate transactions, verify the authenticity of energy production and consumption data, and manage grid operations.

Example: Proof-of-Stake or Practical Byzantine Fault Tolerance algorithms could be used to reach consensus on energy transactions or grid state changes.

Cryptographic Proofs

These mathematical techniques allow one party to prove to another that a statement is true without revealing any information beyond the validity of the statement itself. In DFA, this can be used to verify the integrity and origin of data without exposing sensitive details.

Example: A DFA device could prove it's operating within specified parameters without revealing its exact energy production data.

Zero-Knowledge Proofs

These allow one party to prove they know a value without conveying any information apart from the fact that they know the value. This can enhance privacy in DFA systems while still allowing necessary verifications.

Example: A DFA device could prove it's authorized to participate in the grid without revealing its exact identity or location.

Homomorphic Encryption

This allows computations to be performed on encrypted data without decrypting it. In DFA, this could enable grid operators to perform calculations on energy data without accessing the raw, potentially sensitive information.

Example: Aggregating energy consumption data across multiple households without revealing individual consumption patterns.

Benefits of Trustless Computing in DFA Cybersecurity:

- Improved Resilience: By removing single points of failure, trustless systems can enhance the overall resilience of the DFA network.
- Enhanced Privacy: Minimizing the need to share sensitive data can protect the privacy of energy consumers and producers.
- Increased Security: Distributing control and validation across the network can make it more difficult for attackers to compromise the system.
- Transparency: Trustless systems often provide greater transparency in operations, which can increase confidence in the DFA network.

Challenges and Considerations:

- Scalability: Ensuring trustless systems can handle the volume and speed of transactions in large-scale DFA deployments.
- Regulatory Compliance: Aligning trustless systems with existing energy regulations and standards.
- Interoperability: Ensuring different DFA devices and systems can effectively participate in the trustless network.
- Performance: Managing the computational overhead of cryptographic operations, especially for resource-constrained DFA devices.
- Quantum Computing Threat: Preparing for the potential threat that quantum computers could pose to current cryptographic methods.

As DFA systems become more prevalent and complex, trustless computing principles offer a promising approach to enhancing their security, privacy, and resilience. By reducing reliance on central authorities and enabling peer-to-peer interactions, trustless systems could pave the way for more robust, efficient, and secure distributed energy grids. However, careful consideration of the challenges and ongoing research and development will be crucial to realizing the full potential of this approach in DFA cybersecurity.

Appendix 4: DFA Volumes by Jurisdiction

United States

As of 2023, approximately 3.2 million homes in the United States have solar power installations. This represents about 4.7% of viable owner-occupied homes. The solar industry has been growing rapidly, with a projected increase in residential installations expected to more than triple by 2030 . https://theroundup.org/solar-power-statistics/

United Kingdom

By the end of 2023, the UK had an installed solar capacity of around 15.7 GW. The number of homes with solar installations has been increasing steadily, driven by favourable government policies and incentives. https://theroundup.org/solar-power-statistics/

Australia

Australia leads in solar adoption, with more than 3.7 million rooftop solar systems installed by early 2024, covering over 31.46% of all households. The country's solar capacity continues to grow, reflecting a strong commitment to renewable energy https://www.solarquotes.com.au/australia/ https://solarcalculator.com.au/blog/solar-energy-facts-and-statistics/ .

New Zealand

New Zealand has a smaller but growing solar market. The exact number of residential installations is less frequently reported, but there is a steady increase in solar adoption due to rising electricity costs and government incentives. https://theroundup.org/solar-power-statistics/

Japan

Japan has been a significant player in the solar market, with widespread adoption of residential solar systems. The country continues to expand its solar capacity, especially with rooftop installations becoming increasingly popular https://theroundup.org/solar-power-statistics/

Germany

As of 2023, Germany leads Europe with 14.1 GW of new solar installations in a single year, reflecting a robust solar market with a significant number of residential systems.

Spain

Spain installed 8.2 GW in 2023, showing strong growth in residential solar adoption.

Italy, Poland, and the Netherlands

These countries also have substantial solar markets, with installations of 4.8 GW, 4.6 GW, and 4.1 GW respectively in 2023. https://www.solarpowereurope.org/press-releases/new-report-eu-solar-reaches-record-heights-of-56-gw-in-2023-but-warns-of-clouds-on-the-horizon

Overall, solar adoption continues to rise across these regions, driven by environmental concerns, economic incentives, and technological advancements. The growth trends suggest that solar will play an increasingly vital role in the global energy mix in the coming years.

Appendix 5: Prominent Cybersecurity Firms

Below is a list of Cybersecurity companies and products which are either directly, or tangentially, related to DFA.

Company/Product	Description
Claroty	Delivers comprehensive visibility, threat detection, and secure remote access for industrial networks. Their platform helps protect critical infrastructure and manufacturing environments. https://www.claroty.com/
Crowdstrike Falcon XDR	An extended detection and response solution that unifies device, identity, and threat intelligence data to stop breaches. https://www.crowdstrike.com/products/endpoint-security/falcon-xdr/
Cyberbit	Offers a range of cybersecurity products, including OT security solutions and a cyber range platform for training and simulation. https://www.cyberbit.com/
CyberX (now part of Microsoft)	Provides continuous OT and IoT security monitoring and asset management. Their platform uses behavioral analytics and machine learning to identify threats. https://www.microsoft.com/en-us/security/business/threat-protection/azure-defender-for-iot
Dragos	Specializes in industrial cybersecurity, offering threat detection, vulnerability management, and incident response for industrial control systems and operational technology environments. https://www.dragos.com/
ExtraHop Reveal(x) 360 (XDR)	A cloud-native XDR solution that uses AI to detect and respond to threats across on-premises, cloud, and IoT environments. https://www.extrahop.com/products/cloud/
Heimdal Threat Hunting and Action Center (THAC)	A unified threat hunting, SIEM, and incident response platform that provides real-time threat intelligence and automated remediation. https://heimdalsecurity.com/en/products/threat-hunting-and-action-center
IBM Security QRadar XDR	An extended detection and response platform that uses AI to quickly identify and respond to threats across hybrid cloud environments. https://www.ibm.com/products/qradar-xdr
Indegy (now part of Tenable)	Specializes in industrial cybersecurity, providing visibility, security, and control for industrial control networks. https://www.tenable.com/products/tenable-ot

LogPoint SIEM & Log Management	A next-gen SIEM solution that combines security information management, security analytics, and automated response in a single platform. https://www.logpoint.com/en/product/siem/
ManageEngine Log360 (SIEM)	An integrated SIEM solution that combines log management, compliance reporting, and user behavior analytics. https://www.manageengine.com/log-management/
McAfee Enterprise Security Manager (ESM)	A security information and event management (SIEM) solution that delivers actionable intelligence and integrates with other security products. https://www.mcafee.com/enterprise/en-us/products/enterprise-security-manager.html
Micro Focus ArcSight ESM	An enterprise SIEM solution that provides real-time threat detection, compliance automation, and security analytics. https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview
Microsoft Sentinel	A cloud-native SIEM and security orchestration automated response (SOAR) solution that provides intelligent security analytics across the enterprise. https://azure.microsoft.com/en-us/services/microsoft-sentinel/
Mission Secure	Provides OT cybersecurity solutions for critical infrastructure, including protection, monitoring, and response capabilities for industrial control systems. https://missionsecure.com/
Nozomi Networks	Provides industrial cybersecurity and operational visibility solutions for industrial control systems (ICS) and operational technology (OT) networks. Their products help secure critical infrastructure and industrial operations. https://www.nozominetworks.com/
Palo Alto Networks Cortex XDR	An extended detection and response platform that natively integrates network, endpoint, and cloud data to stop sophisticated attacks. https://www.paloaltonetworks.com/cortex/cortex-xdr
Radiflow	Develops cybersecurity solutions for critical infrastructure and industrial networks, including threat detection and secure remote access tools. https://radiflow.com/
Rapid7 InsightIDR	A cloud-native SIEM that enables security teams to detect and respond to threats quickly across their entire ecosystem. https://www.rapid7.com/products/insightidr/
SCADAfence	Offers a non-intrusive cybersecurity platform for industrial OT networks, providing full coverage of large-scale networks and distributed sites.

	https://www.scadafence.com/
SIEMENS AG - Xcelerate SIEM	A SIEM solution specifically designed for operational technology (OT) environments, helping to secure industrial control systems. https://new.siemens.com/global/en/products/energy/services/digital-services/operational-technology/xcelerate-cybersecurity.html
SolarWinds Security Event Manager (SEM)	A SIEM solution that helps organizations automate security monitoring, threat detection, and incident response. https://www.solarwinds.com/security-event-manager
Sophos Intercept X (EDR)	An endpoint detection and response solution that uses deep learning and anti-exploit technology to prevent, detect, and respond to threats. https://www.sophos.com/en-us/products/endpoint-antivirus
Splunk Enterprise Security (SES)	A SIEM solution that provides security analytics, advanced threats detection, and automated incident response. https://www.splunk.com/en_us/software/enterprise-security.html
Verve Industrial Protection	Offers a comprehensive OT/ICS cybersecurity platform that combines asset inventory, vulnerability management, and secure configuration management. https://verveindustrial.com/