4SECURE®

SECURITY BRIEF

Cybersecurity for Renewable Energy Operations

How secure, policy-enforced data transfer enables safe operational modernisation

THE CHANGING RISK LANDSCAPE IN RENEWABLES

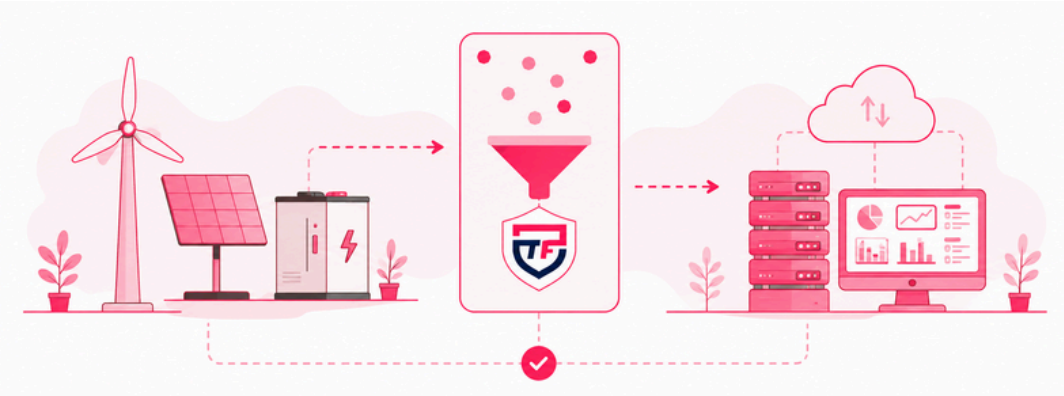
Renewable energy has always been operationally demanding. Wind, solar, battery storage, and distributed generation assets must perform continuously, often in remote locations, with minimal tolerance for downtime. The shift towards digitalisation – centralised monitoring, cloud-based analytics, remote diagnostics, and AI-assisted maintenance – is delivering genuine operational benefit. It is also expanding the cyber attack surface in ways that were not a primary concern a decade ago.

Operational technology (OT) environments – the SCADA systems, historians, PLCs, and control networks that manage generation assets – were traditionally isolated from external networks. That isolation is eroding. Today, OT data routinely flows into IT environments, cloud platforms, and third-party systems. Each connection that enables visibility also creates a potential path for compromise.

The consequences of a cyber incident in a renewable energy environment are not abstract. Disruption to generation assets affects grid stability, revenue, contractual obligations, and in some configurations, safety systems. Nation-state actors and ransomware groups have demonstrated sustained interest in energy infrastructure, and the renewable sector is not exempt from that attention.

The central challenge for renewable operators is not choosing between operational progress and cyber security.

It is ensuring that the connection between OT environments and IT or cloud systems is governed by clear, enforced policy – so thatoperational data can flow out where it is needed, without exposing control systems to unauthorised access.



WHY OT–IT CONVERGENCE REQUIRES A DIFFERENT APPROACH

Conventional network security – firewalls, segmented VLANs, access controls – was designed primarily for IT environments. IT security operates on a model of bidirectional communication: credentials are verified, connections are authenticated, and threats are detected and blocked. This model assumes that the underlying systems can be patched, updated, and replaced on relatively short cycles.

OT environments do not share these characteristics. Control systems and industrial devices in renewable assets are often designed for operational lifespans of fifteen to twenty-five years. They run on proprietary or industrial protocols, may not support frequent software updates, and cannot be taken offline for patching without operational consequence. Many were designed and deployed before cyber threat was a primary design consideration. Applying IT security models directly to OT environments creates two problems. The first is technical: IT security tools may not understand or support industrial protocols, and their deployment can introduce instability into systems where uptime is a hard requirement. The second is governance: without clear policy enforced at the point where OT data crosses into IT or cloud environments, organisations are reliant on broad network access and trust assumptions that are difficult to audit and easy to misconfigure.

What renewable operators need is not simply more connectivity, and not simply more restriction. It is the ability to inspect, validate, and enforce policy on data before it crosses a security boundary – so that only explicitly authorised data moves, regardless of which systems sit either side of that boundary, and regardless of whether the connection is one-way or controlled bidirectional exchange.

OPERATIONAL USE CASES IN RENEWABLE ENERGY

Use Case	Operational Application
SCADA telemetry and production data	Generation, performance, and condition data from wind, solar, and BESS control systems transmitted to enterprise platforms and cloud analytics, with policy enforced at the point of transfer.
Historian replication	Process and production history replicated from on-site historian platforms (including AVEVA PI) to centralised reporting and analytics environments, without exposing the source control network.
Multi-site portfolio segmentation	Controlled data exchange between sites with different criticality classifications. A compromise of IT systems or a supplier network is prevented from propagating into OT environments across the portfolio.
Offshore wind operational visibility	Real-time generation data and alarm management from offshore turbines transmitted to onshore operations centres over constrained links, governed by policy rather than open connectivity.
OEM and vendor data sharing	Turbine OEMs, inverter manufacturers, and maintenance contractors receive the data they need for diagnostics and performance optimisation, through a controlled exchange rather than broad network access.
Security monitoring and SIEM integration	Security and operational logs from OT environments fed into central SIEM platforms, giving security teams visibility of OT activity without opening a path into control systems.
Industrial messaging and IoT data	MQTT and other industrial messaging traffic from distributed sensors and edge devices validated and passed on to cloud platforms under enforced policy.
Digital transformation enablement	AI-assisted maintenance, predictive analytics, and centralised operations programmes depend on consistent, trustworthy OT data. Policy-enforced transfer provides the secure data pipeline these programmes require.

REGULATORY AND ASSURANCE CONTEXT

Regulatory expectations for OT cybersecurity in the energy sector have increased materially in recent years, and the direction of travel is clear. Operators and their boards are being asked to demonstrate, rather than simply assert, that appropriate controls are in place.

Framework	Relevance to Renewable Operators
NIS Regulations (UK) / NIS2 (EU)	Operators of essential services are required to implement appropriate technical and organisational measures to manage cyber risk. OT security and incident reporting are within scope. Boards carry accountability for compliance.
IEC 62443	The international standard series for industrial automation and control system security. Increasingly referenced in procurement, insurance, and audit processes. Policy-enforced data transfer aligns to zone and conduit architecture principles.
NCSC OT Cyber Guidance	UK government guidance recommending segmentation of OT from IT networks as a foundational control, with data crossing that boundary subject to clear, enforced policy.
Cyber insurance requirements	Insurers are increasing scrutiny of OT security controls as a condition of coverage. Demonstrable, auditable data flow controls are increasingly expected as standard.

TRUSTEDFILTER®

SECURE DATA TRANSFER FOR RENEWABLE OPERATIONS

TrustedFilter® is 4Secure's cybersecurity software suite, built to let renewable energy operators move operational data where it needs to go – across remote assets, production environments, and business systems – without increasing cyber risk.

By inspecting, validating, and enforcing policy on data before it crosses a security boundary, TrustedFilter enables controlled connectivity between OT, IT, and cloud environments while maintaining the integrity of critical operations.

TrustedFilter is architecture flexible. It supports strict one-way data transfer where that is the right control for the environment, and controlled bidirectional exchange where operational requirements call for it including integration with existing data diodes and firewalls, rather than requiring their replacement. It can be deployed on premise, integrated with cloud platforms, and scaled consistently across multi-site renewable portfolios, from single substations to distributed offshore wind estates.

For renewable energy operators, this gives operations and security teams a consistent way to enable portfolio wide monitoring, vendor and OEM data sharing, and digital transformation initiatives, while keeping clear, auditable control over exactly what data is permitted to move and where it is permitted to go.

Capability	Detail
Policy-based inspection and enforcement	Data is inspected, validated, and checked against policy before it is permitted to cross a security boundary. Unauthorised data is blocked.
Architecture flexibility	Supports one-way transfer and controlled bidirectional exchange, with on premise and cloud deployment options.
Integration with existing infrastructure	Works alongside existing data diodes and firewalls and integrates with established network architectures rather than requiring a redesign.
Broad protocol support	Supports MQTT, OPC UA, TCP, HTTPS, AMQP, and a wide range of additional industrial and IT protocols.
High assurance data types	Handles production and process data, SCADA telemetry, historian replication (including AVEVA PI), industrial messaging, and security logs into SIEM platforms.
Scalable multi-site deployment	Consistent policy enforcement across single sites, multi-site portfolios, and distributed or offshore environments.

Supported protocols include:

HTTPS

TCP

AMQP

MQTT
and industrial messaging protocols

OPC UA

Additional industrial and enterprise protocols, assessed on a per-deployment basis.

About 4Secure

4Secure is a specialist OT cybersecurity company. We protect the operational technology environments that underpin critical infrastructure – including energy generation, utilities, and industrial operations. TrustedFilter, our cybersecurity software suite for secure data transfer, is deployed by operators across the energy sector to enable safe IT/OT convergence without compromising the integrity of operational systems.

Get in touch
› alex.ball@4-secure.com

Visit our website
› www.4-secure/renewables