



SUNSPEC
— ALLIANCE —

Secure SunSpec Modbus: A Familiar Interface Ready for a New Reality

Strengthening Trust. Enabling Interoperability.
Securing the Future of Energy.



Open Standards.
Proven Solutions.
Stronger Together.

sunspec.org

SECURE SUNSPEC MODBUS: A FAMILIAR INTERFACE READY FOR A NEW REALITY

Modbus TCP Security has been around for decades. It is simple, widely implemented, and deeply embedded in industrial control. In the Distributed Energy Resource (DER) industry, SunSpec Modbus over TCP has become something even more important than “common,” it is a shared language. A practical way for software, inverters, meters, and controllers to speak to one another.

That strength is also the reason the industry has a new challenge.

Traditionally, Modbus TCP based systems have not been designed for a world where DER fleets are managed remotely, where control signals traverse semi-public networks, or where device interfaces might be exposed beyond a gated Local Area Network (LAN). As the industry evolves and adopts these designs and use cases, the question is how they will do so safely, predictably, and at scale.

That is the gap Secure SunSpec Modbus is built to close.¹

What “Secure SunSpec Modbus” Means

Secure SunSpec Modbus is a requirements specification for Secure SunSpec Modbus TCP. It keeps the core value that made SunSpec Modbus successful: straightforward programmatic interoperability and a stable, vendor-neutral data model. But it adds what modern deployments require:

- Encrypted communications using TLS
- Mutual authentication (client and server authenticate each other)
- Role-based access control (RBAC) so permissions can be limited to what a user or system is supposed to do, and nothing more

This matters because DER Modbus use cases are no longer confined to someone standing in front of a cabinet with a laptop and a cable. They increasingly include cloud software platforms, aggregators, utility systems, and remote operations. That is a very different risk surface than the environments Modbus has traditionally been applied in the DER industry. Secure SunSpec Modbus makes that shift explicit and standardizes the security expectations so the ecosystem can move forward together.¹

Why Now

Cybersecurity itself is not controversial. What is changing is *where* Modbus is being used. In the DER context, Modbus traffic historically lived on private networks. But deployments are evolving:

- More assets are networked, managed, and updated remotely
- More stakeholders legitimately need access (utilities, aggregators, vendors, site operators, service providers, owners)

- More control use cases are emerging, not just monitoring
- More pressure is coming from load growth and system complexity, including electrification and large new loads such as data centers²

At the same time, the energy transition is scaling quickly and unevenly across regions. Globally, renewables have represented the vast majority of new capacity additions in recent years, reinforcing the need for “interoperability that travels” across vendors and markets.³

In other words: the systems are scaling, the networks are expanding, and the interfaces are being used more broadly. Security has to be built into the baseline, not bolted on.

The Security Architecture in Plain Language

Secure SunSpec Modbus introduces a security posture you can describe in one sentence:

Encrypt the connection, verify who is on each end, and grant only the necessary access required for the task.

Under the hood, that translates to a few core mechanisms:

1) Mutual authentication and verifiable identity

The spec requires mutual client/server authentication as part of the TLS handshake.¹ This is foundational: if you cannot reliably verify device and client identity, you cannot reliably secure communications.

Certificates are central to this approach. The spec requires the use of X.509 v3 certificates for identity/authentication by TLS.¹

The devices must provide at minimum the following TLS v1.2 cipher suites:

1. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
2. TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
3. TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8

If the devices support TLS v1.3, these cipher suites must be provided at minimum:

1. TLS_AES_128_GCM_SHA256
2. TLS_CHACHA20_POLY1305_SHA256
3. TLS_AES_128_CCM_SHA256

2) Role-Based Access Control (RBAC), aligned with IEC 62351-8

The spec brings RBAC to Secure SunSpec Modbus by using roles transferred via certificate extensions, and it explicitly aims to align with **IEC 62351-8**, the security standard focused on RBAC for power system management.¹⁴

This is not a cosmetic detail. RBAC is how you translate “secure” into operational reality when multiple parties interact with the same system or device interface. “Read telemetry” and “change protection settings” should not be the same permission set. RBAC is what allows that distinction to be standardized.

Secure SunSpec Modbus defines required roles and also notes that device vendors may add IEC 62351-8 roles such as VIEWER, OPERATOR, ENGINEER, INSTALLER, and security-focused administrative roles.¹

3) Predictable multi-vendor behavior, with fewer surprises

Security is not just about cryptography—it’s about consistency.

When integrators and operators can rely on a common approach to identity, roles, and access, multi-vendor integration becomes simpler and more predictable. Testing gains real meaning, and “secure by design” no longer depends on one-off engineering heroics.

The Secure SunSpec Modbus Certification program is enabled by a combination of robust test procedures, a trusted network of authorized third-party test labs, a growing commercial test software ecosystem, and SunSpec membership benefits that accelerate adoption. Together with traditional SunSpec Modbus Compliance Certification and the recently approved SunSpec Modbus Client Test Procedures, companies now have a clear path to demonstrate and guarantee both interoperability and secure communications.

That is the real value of embedding security into a shared specification: it transforms security from a custom effort into infrastructure.

4) Adaptable, agile, future proof

A key element of the Secure SunSpec Modbus Specification and Test Procedures is that it is designed with future cybersecurity requirements and evolving cipher suites in mind. This means the Secure SunSpec Modbus framework is designed to adapt as regulatory requirements change, new cipher suites are introduced, and old cipher suites are deprecated. Through the SunSpec Modbus Work Group, Secure SunSpec Modbus is the most agile cybersecurity specification in the industry.

Five Current Use Cases (and what they tell us)

Appendix A in the Secure SunSpec Modbus Specification includes five example use cases. They are intentionally practical. Not futuristic. Not hypothetical. Just clear scenarios where encrypted communications and authenticated access are directly relevant.¹

A.1 Utility control of DER devices

This scenario addresses a utility that wants direct control over DER devices, potentially over the public internet, with devices and DERMS commissioned under a shared trust model (for example, a national PKI root CA or a utility-owned root CA).¹

This is “secure remote control” without improvisation. A clear trust anchor, clear credentials, and defined access expectations.

A.2 VPP or aggregator control of DER devices

Aggregators and VPP operators often need the ability to read measurements and control active/reactive power functions, without needing to modify protection settings.¹

This is where RBAC is especially important. The difference between “operate” and “reconfigure protection” is not academic. It is an operational boundary that must be enforced.

A.3 DER vendor diagnostics tracking for DER operations

Vendors often have alternate comms channels to their equipment (APIs, SSH, MQTT, and so on), but the spec recognizes that Modbus interfaces may still be used to gather telemetry data.¹

This is also where the market line between “vendor monitoring” and “grid services” begins to blur. Some vendors may act on behalf of operators or aggregators, which makes role clarity and authentication even more critical.

A.4 DER control for a home or campus microgrid operator

Microgrids raise the bar because the need extends beyond diagnostics. Controls matter. The spec highlights that Secure SunSpec Modbus is designed so self-signed certificates can be used for local encrypted communications, with the user generating and loading the appropriate CAs and certs on the product.¹

This is a key point: not every secure use case is “public internet.” Secure local control is still secure control.

A.5 Homeowner DER access

This is the prosumer and hobbyist reality that often gets overlooked in “grid” conversations.

Some homeowners want read-only access to measurement data. Others want full control. The spec frames how a homeowner might provision roles and certificates (including SunSpec roles such as ReadOnlySunSpec and SuperAdministratorSunSpec) to enable local encrypted access.¹

This is not about encouraging unsafe DIY. It is the opposite. It is acknowledging that direct device interaction will happen, and defining a secure, standard way for that interaction to take place.

A Useful “Bridge” for Deployments: running secure and traditional interfaces together

Appendix B in the Secure SunSpec Modbus Specification provides a pragmatic implementation example: it is possible to run a Secure SunSpec Modbus Server on one port (example shown: 802) and a traditional Modbus Server on the default port (502) on the same product. The secure interface can be used when communications are routed on a public network, while the unencrypted interface can be reserved for local interactions as the industry adapts to TLS requirements.¹

This is worth calling out because it recognizes how deployments actually evolve. It offers a migration path that does not require everything to change overnight, while still making the secure path the default for exposed networks.

The Bigger Story: standards unlock use innovations and cases we cannot fully predict

If all of this sounds familiar, it should.

This is the same arc many of us have watched with **IEEE 2030.5**: early implementations focused on enabling a broad spectrum of advanced grid supporting functions, and then as the ecosystem learned what was possible, leading use cases emerged. This process continues to this day.

That is the real promise here. Secure SunSpec Modbus is not just “Modbus with TLS.” It is a standard foundation for:

- Verified device identity
- Secure access boundaries
- Predictable multi-vendor behavior
- A growing set of operational models, across regions and market structures

Appendix A is not the finish line. It is the starting point.

The SunSpec Dashboard: a reference implementation and developer tool

One of the fastest ways for standards to gain traction is to make them testable.

The SunSpec Dashboard is a Windows software tool for developing SunSpec Modbus communication interfaces for DER products and devices. It is a practical way to reduce development time, prepare products for certification, and access SunSpec Certified products in the field.⁵

If you are implementing Secure SunSpec Modbus:

- You need a way to test client and server behavior
- You need a place to validate assumptions about data mapping and access control
- You need repeatable, concrete communications to test against

Reference implementations and developer tools do not replace the spec. They help the industry *use* the spec.

Next Steps

If you are a manufacturer, software provider, utility, aggregator, or test lab, Secure SunSpec Modbus is worth a close read now, while deployments and use cases are accelerating.

A practical path forward looks like this:

1. Join the SunSpec Alliance as a Contributing Member.
2. Read the Secure SunSpec Modbus Specification and focus on the security requirements: TLS, mutual authentication, role handling, and certificate expectations.¹
3. Review the Appendix A use cases and map them to your own deployment reality (including what “public network” means in your environment).¹
4. Adopt RBAC intentionally, and keep the IEC 62351-8 alignment in view as you design roles and permissions.¹⁴
5. Use the SunSpec Dashboard to validate behavior and shorten the feedback loop between implementation and testing.⁵
6. Engage with the SunSpec community as the ecosystem develops additional guidance, tooling, and field learnings.

Because the most important part of secure interoperability is not the document. It is the shared adoption.

References

1. SunSpec Alliance, *Secure SunSpec Modbus Specification* (Version 1.0, Status: Approved; promoted to Approved on December 10, 2025), PDF.
2. SunSpec Alliance, “SunSpec Dashboard,” SunSpec Alliance website (overview of the Dashboard and its role as a development/troubleshooting tool).
3. International Renewable Energy Agency (IRENA), “Record-Breaking Annual Growth in Renewable Power Capacity,” press release (March 26, 2025) (notes renewables accounted for a 92.5% share of total global power capacity expansion in 2024).
4. International Electrotechnical Commission (IEC), *IEC 62351-8:2020* (publication page describing role-based access control for power system management).
5. SunSpec Alliance, “Specifications,” SunSpec Alliance website (index page listing SunSpec specifications, including Secure SunSpec Modbus).