GREAT HARDWARE

Troubleshooting Guide

SmartGrid™ Control Suite

SG-244-13GH-0XX

Version 2.3

September 2025

Symbols Legend

	**Information:** Provides background details or context to help you better understand a feature, step, or specification. This content is not safety-critical.
	**Warning:** Indicates a potential hazard that could cause personal injury, equipment damage, or process interruption if the instructions are not followed correctly.
	**Error:** Highlights an incorrect action, condition, or result. May also point to a system fault or diagnostic code that requires immediate attention.
	**Tip**: Offers practical advice, shortcuts, or best practices to make troubleshooting more efficient, safe, and effective.
	**Note:** Calls attention to important details, exceptions, or references that are relevant to the procedure at hand.

Troubleshooting Guide

SmartGrid™ Control Suite

SG-244-13GH-0XX

Version 2.3

Published: September 2025

Table of Contents

1. About This Publication

This Troubleshooting Guide supports engineers, operators, and integrators working with the SmartGrid™ Control Suite. It provides systematic approaches to identifying and resolving issues, while ensuring compliance with ISO safety standards.

The guide does not replace the **User Manual** or **Installation Guide**. Instead, it complements them by focusing on problem-solving in daily operations.

Purpose of this Guide

The SmartGrid™ Control Suite is designed for critical environments such as microgrids, renewable energy systems, and industrial power distribution networks. While highly reliable, unexpected conditions may arise. This guide provides structured procedures for diagnosing problems, verifying system health, and restoring normal operation.

Intended Audience

This guide is intended for:

- **Field Engineers** responsible for installation, commissioning, and service.
- **System Operators** overseeing day-to-day control of distributed power systems.
- **SCADA Administrators** maintaining integrations and data visibility.

2. System Overview

The **SmartGrid™ Control Suite** is an integrated platform for managing distributed energy resources (DERs), microgrids, and industrial power distribution systems. It combines modular hardware controllers, advanced optimization algorithms, and SCADA-compatible monitoring to ensure safe, reliable, and cost-efficient energy operations. This overview describes the main components, operational layers, and key interactions that users should understand before troubleshooting.

Architecture at a Glance

SmartGrid™ Control Suite operates across three functional layers:

1. **Hardware Layer**
    - Modular Power Controller Units (PCUs)
    - Sensors and measurement inputs
    - Safety relays and isolation circuits
2. **Control & Optimization Layer**
    - Real-time energy optimization algorithms
    - Load balancing and peak shaving modules
    - Renewable energy integration logic
3. **Supervisory Layer**
    - SCADA integration (Modbus/TCP, IEC 61850)
    - Human–Machine Interface (HMI) dashboards
    - Event logging and compliance reporting

Modular Power Controller Units

The **PCUs** are the foundation of the SmartGrid™ system.

- **Scalable design**: Each unit can be added or removed without system downtime.
- **Flexible I/O**: Supports analog, digital, and high-speed communication interfaces.
- **Redundancy**: Units can be configured in parallel for fail-safe operation.

Energy Optimization Algorithms

The control suite includes built-in algorithms designed to minimize operating costs while ensuring system stability.

Key functions:

- **Peak Shaving** – Reduces demand charges by limiting maximum grid draw.
- **Load Prioritization** – Ensures critical equipment receives uninterrupted power.
- **Renewable Forecasting** – Predicts solar or wind availability and optimizes storage.
- **Demand Response** – Interfaces with utility signals for grid support participation.

Algorithms operate on a **real-time decision cycle**, typically every 250 ms, ensuring rapid response to fluctuations in load or generation.

SCADA-Compatible Monitoring

SmartGrid™ Control Suite is fully compatible with modern industrial SCADA platforms.

- **Protocols supported**: Modbus/TCP, IEC 61850, OPC UA.
- **Data points**: Voltage, current, frequency, power factor, harmonic distortion.
- **Event notifications**: Faults, alarms, and operator overrides are published in real time.

Operators can configure **custom dashboards** to display KPIs such as:

- Renewable contribution (%)
- System load vs. capacity
- Alarm frequency by category

- Create a dedicated “Troubleshooting” view in SCADA to highlight recent alarms, log trends, and controller status in one panel.

ISO-Compliant Safety Features

Safety and compliance are embedded into every layer of the system.

- **Emergency Stop Circuits (E-Stop)** – Hardwired interlock across all PCUs.
- **Safety Relays** – Monitor current, voltage, and relay continuity.
- **Overcurrent & Overvoltage Protection** – Automated trip logic ensures rapid shutdown in <100 ms.
- **Audit Logging** – All safety events are timestamped and stored for compliance with ISO 13849 and IEC 61508.

Safety Feature	Function	Typical Trigger
E-Stop Circuit	Shuts down all PCUs instantly	Operator pushbutton, external safety system
Relay Supervision	Confirms relay health and contact continuity	Internal relay fault detected
Overcurrent Trip	Prevents conductor overheating	Load > 120% rated current

---

⚠ Never disable or bypass safety interlocks. Doing so violates international compliance standards and exposes personnel and equipment to severe risk.

Typical Deployment Scenarios

SmartGrid™ Control Suite is used in a variety of settings:

- **Microgrids**: Seamless coordination of renewable sources, batteries, and backup generators.
- **Industrial Power Distribution**: Load balancing across multiple production lines to avoid costly downtime.
- **Renewable Energy Plants**: Optimization of solar, wind, and storage integration for stable grid export.
- **Isolated Grids (Islands/Remote Sites)**: Ensures energy independence with built-in redundancy and black-start capability.

Why Understanding the System Matters

Troubleshooting is most effective when technicians understand the interplay of hardware, algorithms, and supervisory systems. Many issues stem from

misconfigured optimization settings, **incomplete SCADA integration**, or **safety triggers**. By keeping the architecture in mind, users can rapidly narrow down root causes.

Always begin troubleshooting with a system-wide perspective before focusing on individual alarms or components. This prevents misdiagnosis and wasted downtime.

3. General Troubleshooting Approach

Troubleshooting the **SmartGrid™ Control Suite** requires both a structured process and awareness of the specific context in which the system operates. The following approach ensures consistency, reduces downtime, and prevents incorrect assumptions.

Troubleshooting Workflow

A disciplined sequence of steps is critical when diagnosing issues:

1. **Identify the Symptom**
   - Gather initial reports from operators or alarms shown on the HMI.
   - Record error codes, alarm IDs, and timestamps.
   - Confirm whether the issue is localized (single controller) or systemic.
2. **Gather Evidence**
   - Retrieve recent log files from `/var/log/smartgrid/`.
   - Capture screenshots or SCADA data trends leading up to the fault.
   - Perform a visual inspection for hardware indicators such as LED codes, tripped breakers, or burnt fuses.
3. **Verify System State**
   - Ensure controllers have stable DC supply voltage.
   - Confirm network connectivity between PCUs and SCADA.
   - Check safety interlocks and emergency stops are not engaged.
4. **Isolate the Cause**
   - Compare behavior with a known-good reference site if available.
   - Disable non-essential modules to reduce system complexity.
   - Swap suspected faulty modules with spare parts to confirm the issue.
5. **Apply Corrective Action**
   - Follow the specific resolution steps outlined in the “Common Issues” section of this guide.
   - Document every action taken to maintain traceability.
6. **Confirm Recovery**
   - Verify normal operation resumes across all modules.
   - Re-check safety and compliance states.
   - Monitor the system for at least one operational cycle before declaring the issue resolved.

Best Practices

- **Change one variable at a time**: Avoid simultaneous modifications that complicate diagnosis.
- **Use approved tools**: Non-certified diagnostic software or cabling may yield false results.
- **Record environmental conditions**: Temperature, humidity, and dust can impact performance in industrial settings.
- **Collaborate with operations staff**: Operators often observe subtle patterns not visible in logs.

Maintain a central troubleshooting logbook that includes operator observations, error codes, corrective actions, and results. This historical data is invaluable for both internal learning and vendor escalation.

4. Common Issues

The most frequent operational issues are grouped by functional area. Each issue includes symptoms, causes, diagnostic steps, and resolutions.

System Startup Failures

Startup failures often occur during commissioning, after firmware updates, or following a power outage.

Typical Symptoms:

- Controllers do not power on.
- Controllers stuck in reboot loop.
- HMI displays “System Offline.”
- SCADA connection fails at boot.

Symptom	Likely Cause	Diagnostic Step	Resolution
Controllers not powering on	Low DC supply voltage	Measure input with multimeter	Ensure ≥ 24 V DC, check breakers and cabling
Continuous reboot cycle	Firmware mismatch	Compare versions with `sg_status`	Update all units to same certified release
HMI shows “Offline”	Safety interlock engaged	Inspect emergency stop & relay continuity	Reset E-stop, replace relay if faulty
No SCADA link after boot	Network misconfiguration	Ping controller IP, check subnet	Correct IP settings, verify firewall ports

Diagnostics and Resolutions

⚠ Always power down and discharge capacitors before handling controller modules. Live servicing can result in electric shock.

Energy Optimization Issues

Optimization failures may result in higher energy costs or reduced system efficiency.

Key Scenarios:

- Peak shaving not activating.
- Renewable inputs ignored.
- Unintended load shedding.

Symptom	Possible Cause	Resolution
Peak demand charges remain	Optimization disabled	Enable “Peak Shaving” under dashboard Energy Settings
Solar/wind input not used	Sensor calibration error	Recalibrate CTs and voltage sensors
Loads disconnected unexpectedly	Demand thresholds too strict	Adjust parameters to align with site load profile

Diagnostic Table

Test optimization settings in Simulation Mode before applying changes to live systems.

Load Balancing Instability

Load balancing ensures equitable distribution across controllers and feeders. Instability may manifest as power fluctuations, oscillations, or uneven loading.

Checks to Perform:

- Verify NTP synchronization across all PCUs.
- Inspect communication latency on site network switches.
- Review harmonic filter health and grounding connections.

Resolution:

- Re-establish time synchronization using NTP.
- Replace failing Ethernet switch hardware.

- Service or replace faulty harmonic filters.

5. Communication & SCADA Integration

SCADA integration is critical for visibility and automation. Communication issues are among the most reported problems.

Connectivity Issues

Connectivity failures may prevent data exchange between SmartGrid™ controllers and SCADA servers.

Checklist:

- Verify each PCU has a unique IP address.
- Confirm required ports (502 for Modbus/TCP, 102 for IEC 61850) are open.
- Check physical cabling and switch link LEDs.
- Ensure SCADA drivers match firmware versions.

Code	Description	Action
COM-120	Connection lost	Verify cabling, restart network switch
COM-202	Invalid packet	Update SCADA driver, confirm protocol selection
COM-305	Time sync mismatch	Re-enable NTP service on controllers

Common Error Codes

Data Accuracy Problems

If SCADA displays incorrect or unstable values:

- Verify sensor calibration.
- Confirm system clock sync to NTP server.
- Review network latency.

ℹ Accurate timestamps are mandatory for ISO compliance. Always re-verify time sync after firmware updates or system restarts.

6. Safety & Compliance Troubleshooting

The **SmartGrid™ Control Suite** is designed to meet international safety standards such as **ISO 13849** and **IEC 61508**. These standards ensure that energy management systems operate with a predictable level of safety integrity, protecting both personnel and equipment.

Failures in the safety chain are always **critical** and must be investigated thoroughly before the system is restarted. This page describes how to identify, classify, and respond to safety-related events.

Importance of Safety & Compliance

Unlike other troubleshooting areas, safety and compliance issues carry **legal, regulatory, and human risk**.

- **Human Safety**: Prevents electric shock, arc flash incidents, or fire.
- **Equipment Protection**: Avoids catastrophic failures of controllers, transformers, and loads.
- **Regulatory Compliance**: Ensures the system remains certified and insurable.

⚠ Always treat a safety-related alarm as genuine. Do not attempt to bypass or suppress alarms without root cause verification.

ISO-Compliant Safety Features

The following features are embedded into the SmartGrid™ Control Suite:

- **Emergency Stop (E-Stop) Circuits**
  - A hardware-level interlock that instantly disconnects power from all Power Controller Units (PCUs).
  - Must be accessible at key operator locations.
- **Safety Relays**
  - Verify electrical continuity and switch states.
  - Supervised to ensure they respond within defined time frames.
- **Overcurrent and Overvoltage Protection**
  - Trips when conditions exceed rated safe values.
  - Can trigger local shutdown or system-wide isolation.

- **Audit Logging**
  - All safety events are timestamped with precision.
  - Logs cannot be tampered with and must be archived for compliance audits.

Alarm Reference Table

Alarm Code	Category	Description	Required Action
SAF-101	Emergency Stop	Operator-activated E-Stop	Inspect circuit wiring, confirm intentional use, reset switch
SAF-210	Relay Fault	Relay supervision failure	Replace faulty relay, test before restart
SAF-260	Relay Response Delay	Relay exceeded safety timing window	Verify relay coil and contactor, replace if needed
SAF-320	Isolation Failure	Ground fault or failed isolation barrier	Perform insulation resistance test, repair wiring
SAF-350	Overcurrent	Load exceeded safe operating current	Inspect wiring and breakers, reduce demand
SAF-410	Overvoltage	Input exceeded safe voltage range	Check upstream supply, replace damaged surge protection
SAF-499	Unknown Safety Event	Undefined error captured	Escalate to vendor support with logs

---

Common Safety-Related Scenarios

Emergency Stop Activation

- **Symptom**: All controllers shut down immediately, alarms SAF-101 raised.
- **Diagnosis**: Inspect E-Stop switch and cabling. Confirm whether pressed intentionally.
- **Resolution**: Reset switch, test function, log event in compliance records.

Relay Supervision Failure

- **Symptom**: SAF-210 or SAF-260 alarms triggered.
- **Diagnosis**: Check continuity across relay terminals. Compare relay response times.
- **Resolution**: Replace relay, re-run safety function test.

Overcurrent or Overvoltage Events

- **Symptom**: SAF-350 or SAF-410 alarms triggered, breaker trips.
- **Diagnosis**: Inspect load wiring, verify transformer tap settings, check lightning arrestors.
- **Resolution**: Reduce load demand, replace damaged cabling, confirm surge protection is functional.

Preventive Maintenance for Safety

To avoid unnecessary trips and ensure compliance, preventive checks should be part of the maintenance schedule.

Monthly:

- Test all Emergency Stop switches.
- Review last 30 days of safety event logs.

Quarterly:

- Inspect wiring insulation with a megohmmeter.
- Verify relay coil resistance and contact response.

Annually:

- Perform a full Safety Integrity Level (SIL) validation test.
- Calibrate trip thresholds for overcurrent and overvoltage protection.
- Audit compliance records against ISO and IEC requirements.

ℹ Keep signed records of all preventive safety checks. Auditors may request proof of testing as part of compliance validation.

Compliance Logging & Reporting

All safety systems produce secure audit logs that must be:

- **Stored** for a minimum of two years (local regulations may require longer).
- **Backed up** to offsite or cloud storage.
- **Protected** from unauthorized modification.

```
[2025-09-12 08:42:15] SAF-350 Overcurrent event, Bus 3, Current = 128%
[2025-09-12 08:42:15] Load shedding initiated, Priority Load = HVAC
[2025-09-12 08:42:17] Operator acknowledged alarm
```

Example log excerpt

Regulatory Considerations

- **ISO 13849 (Safety of Machinery)**: Requires documented proof of tested safety functions.
- **IEC 61508 (Functional Safety)**: Governs safety lifecycle, from design to decommissioning.
- **OSHA / Local Electrical Codes**: National standards may mandate additional checks.

Failure to comply may result in:

- Invalidation of warranty and insurance.
- Regulatory fines or sanctions.
- Increased liability in case of incident.

⚠ Never suppress safety alarms in software. Compliance standards require hardware-level verification and response.

Escalation for Safety Issues

If a safety-related event cannot be explained by routine causes:

1. **Collect logs** for the previous 48 hours.
2. **Document operator actions** at the time of the event.
3. **Photograph** relay wiring, breakers, and E-Stop switches.

4. **Escalate** to SmartGrid™ technical support immediately.

Vendor support may request a **Safety Incident Report** including:

- Event timeline.
- Error codes.
- Photos or diagrams.
- Copies of compliance logs.

7. Diagnostic Tools & Logs

The SmartGrid™ Control Suite provides a range of diagnostic features that allow operators and engineers to collect evidence, isolate causes, and validate corrective actions. These tools are essential in ensuring that issues are properly documented and resolved.

System Logs

Logs are the first resource when diagnosing problems. They capture both real-time events and historical information.

Log Categories:

- **Event Logs**: Record alarms, warnings, and state changes.
- **Optimization Logs**: Track algorithm decisions, such as peak shaving or load shedding.
- **Communication Logs**: Record packet transmission, failures, and SCADA link status.
- **Safety Logs**: Document E-stop activations, relay trips, and overcurrent events.

```
/var/log/smartgrid/
   event.log
   optimization.log
   comm.log
   safety.log
```

Default Location

Retention Policy:

- Default: 7 days, rolling archive.
- Configurable via `sg_config logrotate`.

```
[2025-09-14 18:02:14] INFO: Controller 02 initialized successfully
[2025-09-14 18:02:20] WARN: SCADA link delay exceeded 150ms
[2025-09-14 18:02:22] ERROR: SAF-350 Overcurrent on Bus 1
[2025-09-14 18:02:23] ACTION: Load shedding initiated, Priority Load = HVAC
```

Sample Event Log Entry

Always correlate logs with SCADA timestamps. This helps identify whether issues are internal to SmartGrid™ or external in the supervisory system.

Diagnostic Console

SmartGrid™ includes a built-in command-line interface (CLI) for on-site diagnostics.

Command	Function	Example Output
`sg_status`	Displays system health	Controllers online: 4/4; SCADA link: Active
`sg_diag`	Runs hardware diagnostics	PCU3: Relay test failed; PCU4: OK
`sg_netcheck`	Tests connectivity to SCADA servers	Ping SCADA_IP: OK, Latency: 22ms
`sg_fwcheck`	Checks firmware consistency	PCU1–PCU4 running v2.4.1

Key Commands

```
sg_diag
[PCU1] Relay test: OK
[PCU2] Relay test: OK
[PCU3] Relay test: FAILED
[PCU4] Relay test: OK
Summary: 1 module requires service
```

Example Diagnostic Run

Run sg_diag before and after major maintenance. This creates a baseline to compare against future issues.

Network & SCADA Diagnostics

Communication issues are often network-related. Use `sg_netcheck` to verify paths.

```
sg_netcheck --scada 192.168.20.10
PING SCADA Server: Success
Latency: 22 ms
Packet Loss: 0%
```

Example

If packet loss >2%, check:

- Ethernet cabling integrity.
- Switch port configuration.
- Firewall rules.

Log Analysis Best Practices

- **Correlate Events**: Align multiple logs to reconstruct event sequences.
- **Look for Patterns**: Repeated errors often indicate systemic faults (e.g., firmware bugs).
- **Distinguish Cause vs. Effect**: A SCADA timeout may be an effect of a relay failure, not the root cause.
- **Automate Parsing**: Use log parsing tools (`grep` , `awk` , or vendor-provided analyzers).

When escalating to support, compress and send the entire /var/log/smartgrid/ directory rather than selective entries. Context matters.

8. Escalation & Support

Even with robust diagnostic tools, some issues require escalation to vendor technical support. Clear, complete communication shortens resolution time and ensures safe operation.

When to Escalate

Escalation is appropriate when:

- Documented troubleshooting steps fail to resolve the issue.
- Safety interlocks trigger repeatedly without cause.
- Optimization algorithms misbehave despite correct parameterization.
- Firmware or hardware inconsistencies are detected.

Preparing an Escalation Package

Before contacting support, prepare a **complete escalation package**:

1. **System Identification**
   - Serial numbers of all controllers.
   - Firmware versions (from `sg_fwcheck`).
2. **Error Evidence**
   - Logs from the last 24–48 hours.
   - SCADA screenshots showing anomalies.
   - Alarm codes and timestamps.
3. **Troubleshooting Actions**
   - List all corrective steps attempted.
   - Indicate whether the issue is reproducible.
4. **Environmental Context**
   - Site type (microgrid, industrial plant, renewable farm).
   - Ambient temperature, humidity, and other site conditions.

Contacting Support

Support Channels:

- **Web Portal**: [Support Portal URL]
- **Email**: support@smartgrid.example
- **Phone**: +1 800-555-1234 (24/7 hotline for critical issues)

Expected Response Times:

- Critical (safety or outage): < 2 hours.
- High (system instability): < 8 hours.
- Medium (optimization issues): < 2 business days.
- Low (general inquiries): < 5 business days.

ℹ Support cases with complete logs and documentation are typically resolved 30–40% faster than incomplete submissions.

Escalation Workflow

1. **Local Troubleshooting Attempt**
   - Apply documented fixes from this guide.
   - Record actions and outcomes.
2. **Internal Review**
   - Have a second engineer verify findings.
   - Ensure issue is not configuration-related.
3. **Escalation Submission**
   - Submit escalation package via portal/email.
   - Call hotline for critical cases.
4. **Vendor Engagement**
   - Support provides case ID.
   - Remote diagnostic session may be initiated.
   - Replacement hardware shipped if required.

Support Case Study

Scenario: A renewable plant reports repeated SAF-350 overcurrent alarms with no visible load increase.

- **Local Actions Taken**: Checked breakers, wiring, and SCADA configuration. No anomalies found.

- **Escalation Package Submitted**: Logs, SCADA screenshots, relay test results.
- **Vendor Response**: Identified firmware bug causing false overcurrent detection under specific harmonic conditions.
- **Resolution**: Firmware patch issued; plant resumed stable operation.

Post-Escalation Practices

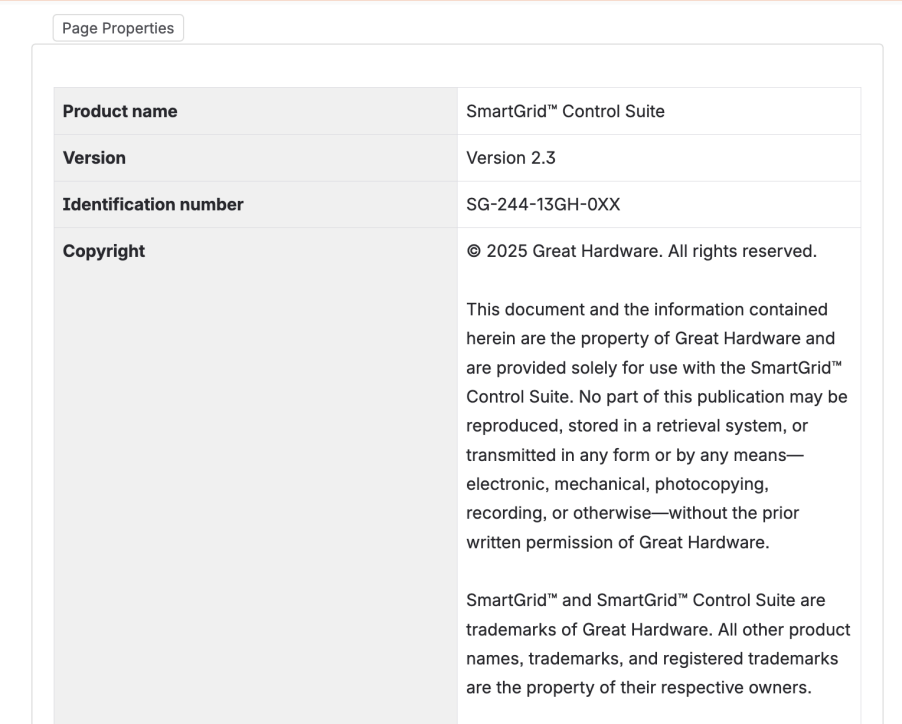
- **Update Documentation**: Add new knowledge to local troubleshooting guide.
- **Review with Staff**: Share lessons learned across the team.
- **Close the Loop**: Confirm system stability after vendor fix.

Consider holding quarterly “incident reviews” where all escalations are analyzed for patterns. This helps identify recurring issues across multiple sites.

This page is not part of the template file and won't affect your exports

This content was exported from Confluence using Scroll PDF Exporter

- To get the most of this Scroll PDF Exporter template: set up your brand and your logo and brand colors will be used automatically.
- Want to have more control over how your Confluence content is exported? Take a look at Scroll Exporter Extensions. With these macros you can insert page breaks, ignore content from your export, and more directly in your Confluence content.
    - This template leverages the macro 'Scroll title' to add styled captions to tables and code blocks.
- This template uses custom placeholders that are set by the content/page properties from the Confluence page template with the keys 'Product name', 'Version', 'Identification number' and 'Copyright'. Image attached below.
- Have suggestions on how to improve our templates or a use case we have not covered? Contact us at support@k15t.com



Page Properties

Product name	SmartGrid™ Control Suite
Version	Version 2.3
Identification number	SG-244-13GH-0XX
Copyright	© 2025 Great Hardware. All rights reserved. This document and the information contained herein are the property of Great Hardware and are provided solely for use with the SmartGrid™ Control Suite. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the prior written permission of Great Hardware. SmartGrid™ and SmartGrid™ Control Suite are trademarks of Great Hardware. All other product names, trademarks, and registered trademarks are the property of their respective owners.