Manufacturer's CLS Product Information

This form is available in a Microsoft Word version from the ENA's website.

G100/2 - Form B - Compliance Verification Report for Customer Export or Import Limitation Schemes

This form shall be used by the **Manufacturer** to demonstrate and declare compliance with the requirements of EREC G100. The form can be used in a variety of ways as detailed below:

1. For **Fully Type Tested** status

   The **Manufacturer** can use this form to obtain **Fully Type Tested** status for a **CLS** by registering this completed form with the Energy Networks Association (ENA) Type Test Register.

2. To obtain **Type Tested** status for a product

   The **Manufacturer** can use this form to obtain **Type Tested** status for one or more **Components** which are used in a **CLS** by registering this form with the relevant parts completed with the Energy Networks Association (ENA) Type Test Register.

3. One-off Installation

   The **Installer** can use this form to confirm that the **CLS** has been tested to satisfy the requirements of this EREC G100. This form shall be submitted to the **DNO** before commissioning.

A combination of (2) and (3) can be used as required, together with Form C where compliance of the **CLS** is to be demonstrated on site.

Note:

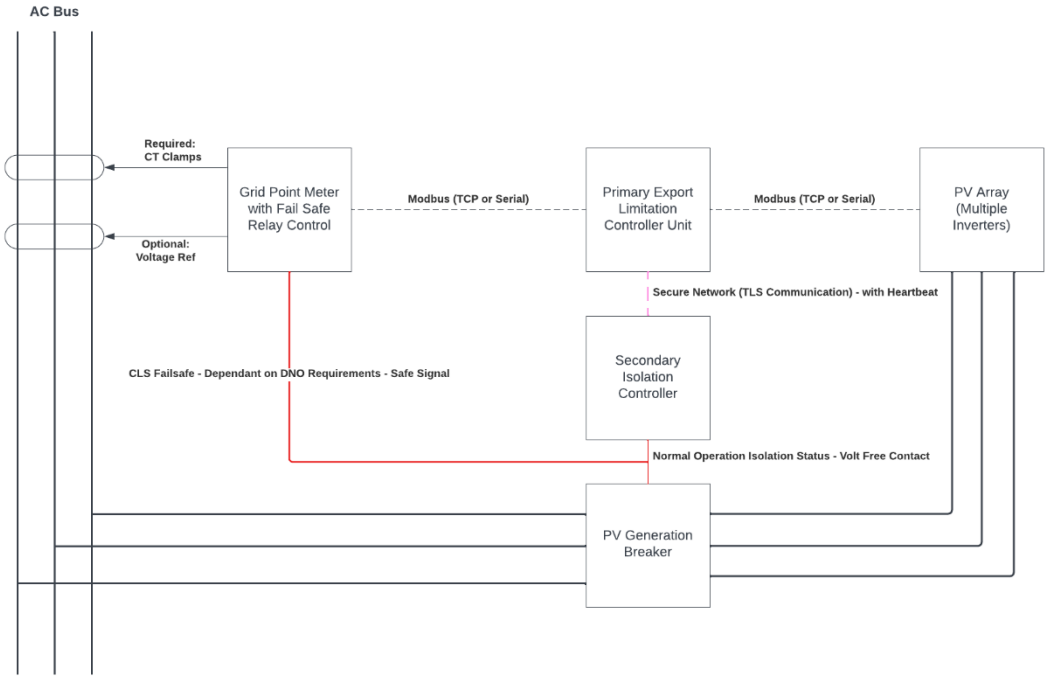
If the **CLS** is **Fully Type Tested** and registered with the Energy Networks Association (ENA) Type Test Register, Form C shall include the **Manufacturer**'s reference number (the Type Test Register system reference), and this form does not need to be submitted.

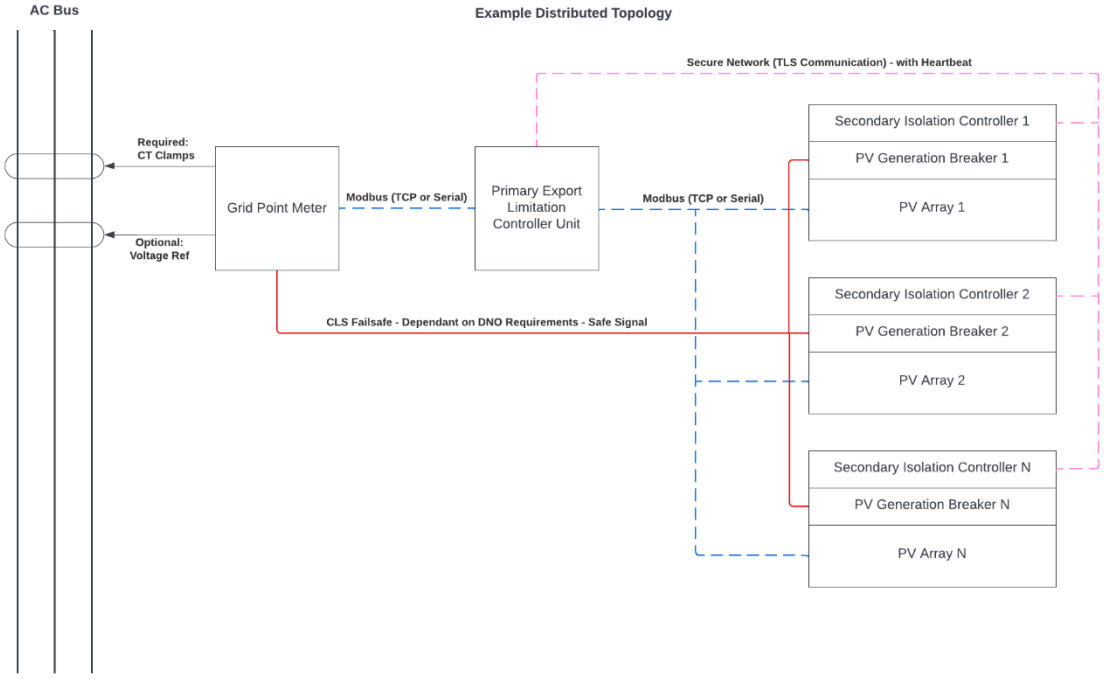
Where the **CLS** is not registered with the ENA Type Test Register or is not **Fully Type Tested** this form (all or in parts as applicable) shall be completed and provided to the **DNO**, to confirm that the **CLS** has been tested to satisfy all or part of the requirements of this EREC G100.

CLS Designation		Hark Distributed Export Limitation System	
Manufacturer name		Hark Systems	
Address		5A, Platform New Station St, Leeds, LS1 4JB	
Tel	0113 868 0805	Web site	https://harksys.com/
Email	Damon.roberts@harksys.com		
Installer's name			
Address			

Tel		Web site	
Email			

Export/Import capabilities			
Export	**Y** / N	Import	Y / **N**
Description of Operation			
EREC G100 section **Error! Reference source not found.** requires a description of the **CLS**, and schematic diagram, to be provided to the **Customer**. Please provide that description and the diagram here.			
The Hark Distributed Export Limitation System (HDEL) provides a flexible, configurable, and robust solution to complying with G100 requirements, independent of site layout or complexity. Hark specialises in vendor agnostic energy control solutions including solar inverter monitoring and control, through the use of proven, standardised hardware, and in-house software.			





The HDEL architecture allows for smart control of downstream generation active power, ensuring the current flow at the point of connection (PoC) never exceeds the limits set by the DNO. By providing rule-based control of equipment, fault conditions can be handled safely without wholesale disconnection of the entire sites generation, or the site itself. By aiming to curtail generation prior to limits being reached, the HDEL will allow customers to maximise the value, and net-zero impact of their assets.

Voltage and Current will be monitored at the PoC; performance metrics, as well as any occasional excursions are logged locally on secure, non-volatile storage. These logs are retained indefinitely if required, allowing analysis of long-term system performance, even if no instances of State 2 or 3 have been triggered.

The HDEL provides a significant amount of redundancy to the overall system, through the dual connection to individual system components, as well as failsafe relays. Where possible, the system will attempt to directly reduce outputs at the inverter level, co-ordinated by the Primary controller, whilst utilising distributed Secondary controllers to enable local control and tripping in the case of any communication failure.

If State 2 or 3 operation is triggered, the system will ensure all applicable devices are disconnected/turned down until the site begins to operate within the required parameters, with State 3 triggering the lockouts required as per G100-2023-2-2.

The majority of the parameters within the HDEL with regards to timings, turn down/off priorities, and limits are configurable by the installer, ensuring any edge cases as required by the DNO or site itself are possible.

The Primary Controller is configured to communicate with all generation assets via Modbus (TCP or Serial), the Primary Controller is responsible for regulation of active power across the distributed set of generation assets.

At each generation asset there is a Secondary Safety Controller which is also connected to the Primary Controller via secure TCP/IP communication which encrypted via TLS for security and encryption in flight. Should the Primary Controller lose communication with the Secondary the system can be configured to isolate or command the generators to zero or a configuration in line with the DNO requirement.

The system is bi-directional and should the Secondary Controller lose communication with the Primary the Secondary will locally isolate the generator to mitigate the potential of unknown generation state and operation within the solution.

Should the Primary lose communication with any of the generators then the Primary can command the Secondary Isolation Controller to ensure the system is safely isolated and there is no chance of generation from the specific generator associated with Secondary Isolation Controller.

Should the Primary or Secondary Controllers fail the output safe signal to the PV breakers will become unavailable and the breakers will open thus ensuring any failure of the system results in isolation of the generators within a user defined time which is configured in the controllers.

The configuration is limited to user access only and therefore cannot be changed without knowing the engineering passcodes.

Communications Media

Document the provisions made for the use of various communication media, and both the inherent characteristics and the design steps made to ensure security and reliability.

The system architecture consists of a Primary monitoring and control device, and a number of Secondary control devices. The primary monitors the PoC and sends commands to the Secondary devices located at each inverter. Depending on the site layout, a dedicated CAT5 or Fibre Modbus TCP or Serial network will be implemented, ensuring reliable communications. In the case of either the Primary or Secondary detecting a communications or hardware failure, the relevant generation devices will enter a failsafe state until communications have been restored.

Local monitoring and administration will only be possible through approved user accounts, who are connected to the dedicated HDEL network or VLAN, reducing any possible attack surface significantly.

No cloud connectivity will be used anywhere within the solution thus limiting the scope of attack via remote vectors.

Cyber Security

Confirm that the **Manufacturer** or **Installer** of the **CLS** has provided a statement describing how the **CLS** has been designed to comply with cyber security requirements, as detailed in section **Error! Reference source not found.**.
Hark Systems has been certified as ISO27001 ISMS compliant across all our software and hardware development activities, including those of the HDEL. The development utilises a secure development software lifecycle which is maintained by the CISO at Hark. The certificate number is available to customers upon request which is validated by BSI (British Standards Institute) who externally audit the companies processes and systems each year. Internal audits by external security companies are performed each month on the entire organization in the specific office where this software is currently developed. The HDEL similarly complies with **TSI EN 303 645**. Default passwords are randomised, all TCP connections where possible support TLS 1.3, software images are generated with the latest code and updated packages just prior to shipment to customers. The dedicated network for the system reduces the attack surface to only include those who have obtained system credentials and have physical access to the network. All customer networking is advised to be segregated on the Export Limitation network via physical separation where possible or logical separation via virtualisation of the LANs. This also adds a layer of segregation and reduces the scope for attackers to jump adjacent non-operational networks into the system. The configuration system for the Primary Export Limitation Controller and Secondary Configurations are protected by user authentication and also certain permissions within the software itself. Should the device be tampered with in such a way that disables its ability to perform its actions there are certain mitigations that would cause the Secondary Safety Isolation relays to command breakers to open. Passwords are encrypted and salted within strong encryption methods in line with the NIST (National Institute of Security and Technology). Hark already operates a vulnerability submission system which has been tested across a number of products. Local monitoring and administration is enabled by default, enabling approved users to examine system telemetry, manage user data, and validate installer settings. Any system level configuration changes require support from the 3rd party installer, or Hark Systems to be implemented, ensuring the G100 control scheme, and therefore MEL/MILs cannot be circumvented.
Power Quality Requirements
Where the **CLS** includes the power electronics that controls generation or loads (as opposed to the power electronics being included in **Devices** that are subject to their own power quality compliance requirements) please submit the harmonic and disturbance information here as required by EREC G5 and EREC P28.
The HDEL is not designed to directly control any load or generation devices and contains no power electronics. Rather it communicates with devices that already include the requisite power electronics and monitoring to do so, and as such will not impact the harmonic or power quality performance of a site.

Fail Safe
CLS internal failure: please submit here the description of the internal **Fail Safe** design and operation. Please also document how it has been demonstrated, including the non-volatile recording of times and numbers of state 2 operations, and confirm the overall response of the **CLS** to this internal failure.
The HDEL architecture provides several fail-safes to ensure the MEL is not breached. Depending on the nature of the failure, different scenarios may produce different failsafe responses. For example, if a single Secondary device loses connectivity with the Primary, only the attached generation device will be set to zero output, or disconnected from the system. If the Primary controller detects a failure within its own hardware, the grid meter, or other hardware it may be monitoring, the whole site may be tripped. By

minimising the number of components and external interconnections between devices, designing a robust failsafe system control scheme is easily achievable for the installer, even in a complex site.

A watchdog will be implemented on each controlled that ensure software and hardware integrity is maintained at all times. If the watchdog conditions are breached, the system will be power cycled, triggering an S3 lockout, and automatically tripping all connected isolation relays.

The system can automatically recover from communication failures, without triggering a state 3 lockout.

Communication and power supply failures between **Components** and **Devices**. Please document here compliance with EREC G100 section 5.5.

Component/Device number/description	**Communication failure test**	**Power supply failure test**
Primary –> Generation Device Connection	Secondary Isolation Relay associated with the Generation device is opened immediately. On re-established communication with the system, there is a user defined delay set of 15 minutes before the generation assets will be commanded via breakers and active power settings to generate, assuming there is capacity to do so.	Secondary Isolation Relays lose communication with the Primary and the Secondary Isolation device opens the breakers for all generation assets within 15 seconds. As the primary is not online the system is in State 3 but offline.
Primary –> Secondary Connections	Primary registers State 3 and commands all generation assets to stop generating within 15 seconds.	Secondary Isolation Relays lose communication with the Primary and the Secondary Isolation device opens the breakers for all generation assets within 15 seconds. As the primary is not online the system is in State 3 but offline.
Secondary –> Primary Connection	The Secondary goes into Isolation mode which opens the breakers connected to the Secondary System within 15-seconds.	The safety signal turns off immediately as this is supported by the power supply of the Secondary.
Primary –> Meter Connection	All secondary downstream devices trip in <5 seconds and S3 operation is triggered.	All secondary downstream devices trip in <5 seconds and S3 operation is triggered.

Operational Tests

In accordance with EREC G100 section 5.6 undertake the tests A and B to confirm correct operation in state 1 and state 2, that transition into state 3 occurs as required, and that behaviour in state 3 is also as required.

Test A

Nominal Export Limit (for type tests this will be at maximum, minimum and one intermediate setting) in Amp:	100
Nominal Import Limit (for type tests this will be at maximum, minimum and one intermediate setting) in Amp:	N/A

No	Starting level	Step value	**CLS** registers change in level?	**CLS** and/or **Component** and/or **Device** initiates correct response of ≥ 5%?	Duration of step in test	Correct state 1/ state 2 operation
1	95	105% of EL	Yes	Yes	58	Yes. S2 Logged and excursion count incremented.
2	95	110% of EL	Yes	Yes	58	Yes. S2 Logged and excursion count incremented.
3	95	120% of EL	Yes	Yes	58	Yes. S2 Logged and excursion count incremented.
4	95	105% of IL	N/A	N/A	N/A	N/A
5	95	110% of IL	N/A	N/A	N/A	N/A
6	95	120% of IL	N/A	N/A	N/A	N/A

Test B

Nominal Export Limit:	100
Nominal Import Limit	N/A

No	Starting level	Step value	**CLS** registers change in level?	**CLS** and/or **Component** and/or **Device** initiates correct	Duration of step in test	Correct state 3 operation

				response of ≥ 5%?		
7	95	120% of EL	Yes	Yes	62	Yes. S2 entered and logged, excursion counted incremented, and then trip logged at 60s. S3 operation enabled, and control locked for 4 hours.
8	95	120% of IL	N/A	N/A	N/A	N/A

State 3 Reset

These tests are to demonstrate compliance with section EREC G100 4.5.2

Please document how the reset from state 3 to state 1 has been demonstrated. Please include how the reset is achieved.

Please confirm that for **CLSs** to be installed in **Domestic installations** three (3) resets causes lockout or that for non-domestic installations lockout can only be reset after four hours. Please explain how lockout is reset.

The Primary device is used for managing, overriding, and resetting lockouts, however, the UI will be accessible from any connection point to the network. The software on the device provides the logic for lockout conditions, which are configured at the point of installation. Reset can be completed through connecting to the device network only, ensuring an on-site presence has confirmed any fault has been corrected.

In the case of a Domestic Installation, three resets will be allowed before a lockout condition occurs, after which the system will require intervention from an installer on site to restore functionality to the system. The lockout will be reset through the web UI when an approved user is logged in.

In the case of a Non-Domestic Installation, once a lockout condition is triggered, an installer, authorised user, or Hark employee will be required to restore the system, once the 4-hour lockout condition has passed. Lockout timing and causation information will be available via the UI. The lockout will be reset through the web UI when an approved user is logged in.

If S3 operation has been triggered by communication failures, as opposed to excursions above the limits, the system will attempt to restore functionality automatically without user intervention, only removing faulted devices from the network.