

Manufacturer's declaration

SunSynk Ltd.

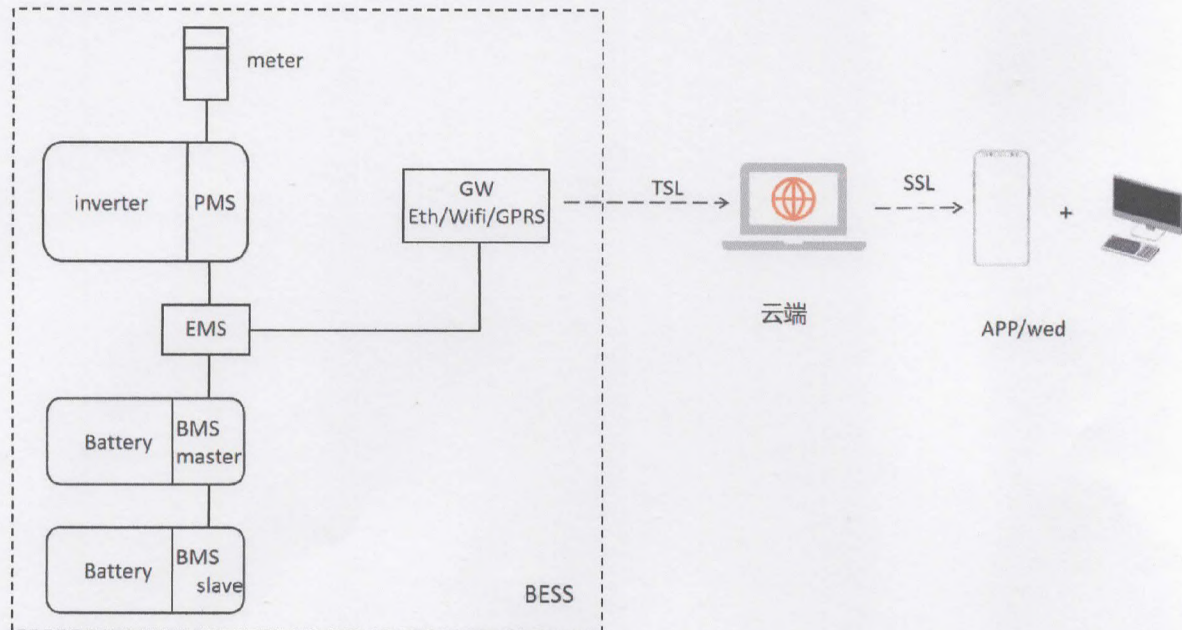
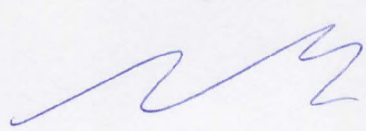
Flat A, 3/F Wai Yip Industrial Building, 171 Wai Yip Street, Kwun Tong, Hong Kong

The undersigned Keith Gough, as Chief Technical Officer (CTO) of the Company SunSynk Ltd.

On behalf of the same Company declares the following:

The inverter in accordance with the requirements of G98-Amd. 6 (2021-09) standard Sec.s 9.7.1, 9.7.2, and G99-Amd. 8 (2021-09) standard Sec.s 9.1.7, 9.1.8 regarding "Cyber Security"

The SunSynk Ltd. Battery Energy Storage Systems (BESS) include a system of internal and external logic communications as summarized in the following scheme:

where the main components involved and their main functions are explained in the following table:

<i>acronym/ name</i>	<i>meaning</i>	<i>function</i>	<i>location</i>
PMS	Power Management System	monitoring and management of power fluxes through the inverter, execution of EMS's commands or local logic functions depending on grid parameters values <i>Note: The PMS performs operational safety functions aimed at prevent physical damage/harm, typically by interrupting currents and/or opening contacts on some inverter ports when voltage, current or temperature limits are violated; no safety operation performed by PMS can be compromised/skipped by commands/signals originating outside the inverter.</i>	inverter
BMS	Battery Management System	monitoring of cells's status, execution of PMS's commands within safety conditions <i>Note: The BMS performs operational safety functions aimed at prevent physical damage/harm, typically by interrupting currents and/or opening contacts on some battery or BMS ports when voltage, current or temperature limits are violated; no safety operation performed by BMS can be compromised/skipped by commands/signals originating outside the BMS and batteries.</i>	battery
EMS	Energy Management System	monitoring of all field's measures, calculus of power and currents for every component of the system, reception of external commands, transmission of commands to PMS. <i>Note: No operational safety function aimed at preventing physical damage/harm is performed by the EMS; no operation performed by EMS can force the operational safety functions performed by BMS, PMS and electrical protections.</i>	Monitor Board
GW	Gate-Way	transmission of data to cloud server, reception of commands/settings from external stakeholder	Stick Logger
Meter	External Power Meter	meter at AC port of third party generator/inverter, for power measures	Meter

- 1) All communications between internal components of the BESS, and between EMS and supplied External Power Meter(s), take place via appropriate serial lines (RS485, CanBus) and are not directly connected to any device or system outside the BESS.
- 2) The only communication port between the BESS and the outside is constituted by the Gate-Way layer (GW) on the machine; the communication between BESS and the outside world can take place via an Ethernet line, WiFi or GPRS router according to the customer's request.
The BESS is a not-constrained customer IoT device according to the definitions in ETSI EN 303 645 sec. 3.1.
- 3) The direct recipients/senders of communications with the BESS is the in-cloud server –the communication is made secure by the use of TSL (Transport Layer Security) technology on GW, and by the use of SSL (Secure Sockets Layer) technology on Final User's device side and web-tools side;
- 4) The cyber-security assessment of the BESS was performed according to the ETSI EN 303 645 standard, and it is reported according to the Table B.1 form of the same standard:

EN 303 645 v2.1.1 (2020-06) Table B.1: Implementation of provisions for consumer IoT security			
Clause number and title			
Reference	Status	Support	Detail
5.1 No universal default passwords			
Provision 5.1-1	M C (1)	N/A	Device don not permit final user's login
Provision 5.1-2	M C (2)	N/A	
Provision 5.1-3	M	N/A	
Provision 5.1-4	M C (8)	N/A	
Provision 5.1-5	M C (5)	N/A	
5.2 Implement a means to manage reports of vulnerabilities			
Provision 5.2-1	M	Y	
Provision 5.2-2	R	Y	
Provision 5.2-3	R	Y	
5.3 Keep software updated			
Provision 5.3-1	R	Y	
Provision 5.3-2	M C (5)	Y	
Provision 5.3-3	M C (12)	Y	
Provision 5.3-4	R C (12)	Y	The manufacturer manages the updates of the systems by means of remote automatisms, selectively by type of machine or by activating special functions at the request of the user
Provision 5.3-5	R C (12)	N	see note at 5.3-4
Provision 5.3-6	R C (9, 12)	N	see note at 5.3-4

EN 303 645 v2.1.1 (2020-06) Table B.1: Implementation of provisions for consumer IoT security			
Clause number and title			
Reference	Status	Support	Detail
Provision 5.3-7	M C (12)	Y	
Provision 5.3-8	M C (12)	N	see note at 5.3-4
Provision 5.3-9	R C (12)	N	
Provision 5.3-10	M (11, 12)	Y	
Provision 5.3-11	R C (12)	N	
Provision 5.3-12	R C (12)	N	
Provision 5.3-13	M	Y	
Provision 5.3-14	R C (3, 4)	N/A	not constrained device
Provision 5.3-15	R C (3, 4)	N/A	not constrained device
Provision 5.3-16	M	Y	
5.4 Securely store sensitive security parameters			
Provision 5.4-1	M	Y	
Provision 5.4-2	M C (10)	Y	
Provision 5.4-3	M	N/A	hard-coded identity not used in source code
Provision 5.4-4	M	Y	
5.5 Communicate securely			
Provision 5.5-1	M	Y	
Provision 5.5-2	R	Y	
Provision 5.5-3	R	Y	
Provision 5.5-4	R	N	
Provision 5.5-5	M	Y	
Provision 5.5-6	R	Y	
Provision 5.5-7	M	Y	
Provision 5.5-8	M	Y	
5.6 Minimize exposed attack surfaces			
Provision 5.6-1	M	Y	
Provision 5.6-2	M	Y	
Provision 5.6-3	R	Y	
Provision 5.6-4	M C (13)	N/A	no debug interface accessible
Provision 5.6-5	R	Y	
Provision 5.6-6	R	Y	
Provision 5.6-7	R	Y	
Provision 5.6-8	R	N	
Provision 5.6-9	R	Y	
5.7 Ensure software integrity			
Provision 5.7-1	R	N	
Provision 5.7-2	R	N	
5.8 Ensure that personal data is secure			
Provision 5.8-1	R	N/A	no personal data transit through BESS hw/sw
Provision 5.8-2	M	Y	applicable to server/cloud services and to the customer App for mobile devices
Provision 5.8-3	M	Y	
5.9 Make systems resilient to outages			
Provision 5.9-1	R	Y	
Provision 5.9-2	R	Y	
Provision 5.9-3	R	Y	
5.10 Examine system telemetry data			
Provision 5.10-1	R C (6)	N	



EN 303 645 v2.1.1 (2020-06) Table B.1: Implementation of provisions for consumer IoT security			
Clause number and title			
Reference	Status	Support	Detail
5.11 Make it easy for users to delete user data			
Provision 5.11-1	M	N/A	
Provision 5.11-2	R	N/A	
Provision 5.11-3	R	N/A	
Provision 5.11-4	R	N/A	
5.12 Make installation and maintenance of devices easy			
Provision 5.12-1	R	Y	
Provision 5.12-2	R	Y	
Provision 5.12-3	R	Y	
5.13 Validate input data			
Provision 5.13-1	M	Y	
6 Data protection provisions for consumer IoT			
Provision 6.1	M	N/A	no personal data transit through BESS hw/sw
Provision 6.2	M C (7)	N/A	
Provision 6.3	M	N/A	
Provision 6.4	R C (6)	N/A	
Provision 6.5	M C (6)	N/A	
Conditions:			
1) passwords are used; 2) pre-installed passwords are used; 3) software components are not updateable; 4) the device is constrained; 5) the device is not constrained; 6) telemetry data being collected; 7) personal data is processed on the basis of consumers' consent; 8) the device allowing user authentication; 9) the device supports automatic updates and/or update notifications; 10) a hard-coded unique per device identity is used for security purposes; 11) updates are delivered over a network interface; 12) an update mechanism is implemented; 13) a debug interface is physically accessible.			
Status' Column:			
M	Mandatory provision		
R	Recommended provision		
M C	Mandatory and conditional provision		
R C	Recommended and conditional provision		
Support' Column:			
Y	Implemented		
N	Not implemented		
N/A	Not applicable		

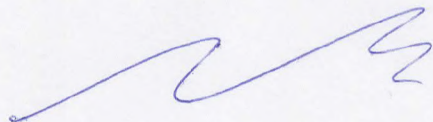
Keith Gough

CEO

On behalf of SunSynk Ltd.

December 3, 2021

Place: Hong Kong

A handwritten signature in blue ink, consisting of a series of fluid, connected strokes.