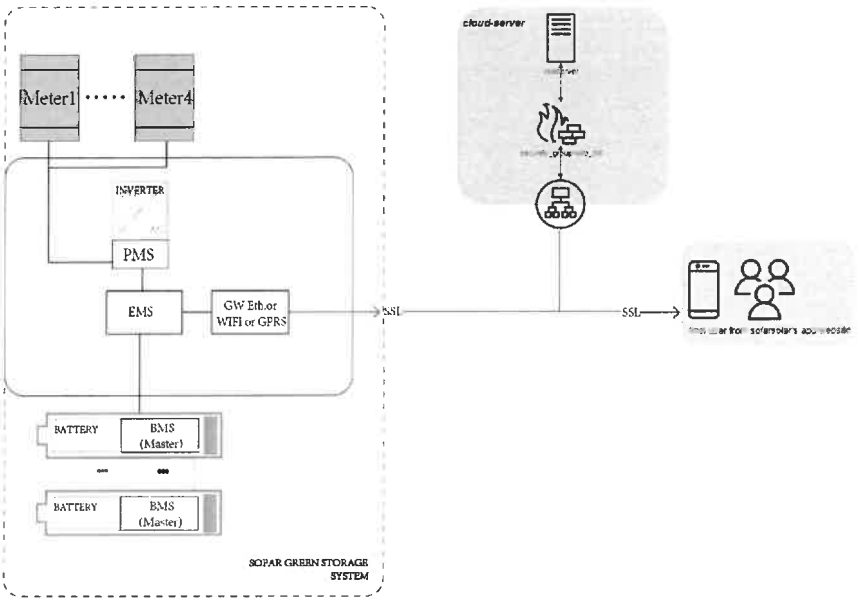
Shenzhen SOFARSOLAR Co.,Ltd.
11/F., Gaoxinqi Technology Building, No.67 Area, Xingdong Community,
Xin' an Sub-district, Bao' an District, Shenzhen City,China

Star Chen, born on 02 May 1989 in China, resident in China, as Head of Product Management of the Company Sofar Solar, based in Shenzhen China, on behalf of the same Company declares the following:

1) The Sofar Storage Battery Electrical 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:

acronym/ name	*meaning*	*function*	*location*
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. 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/skypped by commands/signals originating outside the inverter.	inverter

BMS	Battery Management System	monitoring of cells's status, execution of EMS's commands within safety conditions. 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/skypped by commands/signals originating outside the BMS and batteries.	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. 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.	monitor board
GW	Gate-Way	transmission of data to cloud server, reception of commands/settings from external stakeholder.	Collector
Meter	External Power Meter(s) (one to four)	*included in the supply*: meter at the PCC, and possible meter at AC port of third party generator/inverter, for power measures	PCC; third party inverter

2） 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,SCI) and are not directly connected to any device or system outside the BESS.

3） The only communication port between the device and the outside is constituted by the Gate-Way layer of a logic board on the machine, the communication between BESS and the outside world can take place via Bluetooth, WiFi or GPRS router to the customer's request.

4） The direct recipients/senders of communications with the BESS is the in-cloud server of Sofar Green Storage - the communication is made secure by the use of TSL(Transport Layer Security) technology on collector, and by the use of SSL(Secure Sockets Layer) technology on Final User's device side and Installer/Sofar service web-tools side.

5） All communications between the in-cloud server and the subjects/parties are cyber-protected by SSL technology.

6）The cyber-security assessment of the Sofar Green Storage 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 do 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	
Provision 5.3-5	R C (12)	N	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 5.3-6	R C (9, 12)	N	
Provision 5.3-7	M C (12)	Y	
Provision 5.3-8	M C (12)	Y	
Provision 5.3-9	R C (12)	N	See note at 5.3-5
Provision 5.3-10	M (11, 12)	Y	
Provision 5.3-11	R C (12)	Y	
Provision 5.3-12	R C (12)	N	The device failed to notify the user
Provision 5.3-13	M	Y	
Provision 5.3-14	R C (3,	Y	

	4)		
Provision 5.3-15	R C (3, 4)	N	
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	N	No unique key parameters are provided for the device
5.5 Communicate securely			
Provision 5.5-1	M	Y	
Provision 5.5-2	R	N	
Provision 5.5-3	R	N	
Provision 5.5-4	R	Y	
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	The device don't have the access control mechanism
Provision 5.6-9	R	Y	
5.7 Ensure software integrity			
Provision 5.7-1	R	N	The device don't have the hardware root of trust
Provision 5.7-2	R	N	The device don't have the ability to be in administration mode
5.8 Ensure that personal data is secure			
Provision 5.8-1	R	N/A	No personal data transit through the device
Provision 5.8-2	M	Y	
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)	Y	
5.11 Make it easy for users to delete user data			
Provision 5.11-1	M	N/A	No user/personal data are stored in the device
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 user/personal data are stored in the device
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

Date: 2022-06-08

Name: Star Chen

Title: Director of Product Management

Signature: Star Chen

Manufacture Seal