DISCOVER ENERGY SYSTEMS

885-0142 AES CAB BCU Modbus

BCU Modbus TCP Communication Protocol and Register Map

Document title	885-0142 AES CAB BCU Modbus Communication Protocol
Document number	885-0142
Revision	C
Date	July 2026
Applies to	Discover Energy Systems AES CAB high-voltage LFP energy storage cabinet
Interface	Modbus TCP between the cabinet BCU (BMS) and EMS / MGC / PCS
Reference protocol	Great Power, BMS and EMS Communication Protocol - Modbus TCP - BMS Slave for II, V1.5 (2025-04-16)
Audience	Controls integrators programming third-party controllers (e.g., ComAp) and EMS platforms

Revision History

Rev	Date	Description
A	2025-11	Initial release.
B	2026-02	General release.
C	2026-07	Register map realigned to the battery OEM protocol V1.5: cabinet-level data blocks (1001-1100, 1101-1200) and battery pack information block (50501-52100) removed (reserved in V1.5); pack status block re-addressed to 4501-4535 with charge/discharge complete flags, SBMU fault-location registers, and fire/MSD alarms at 4532-4535; cell-temperature offset formula corrected to 250 registers per pack; alarm parameters truncated at 50064; battery control values updated (61001 emergency stop); TMS and dehumidifier appendices added; alarm-code bit tables corrected; control and BMS operating logic section added.

DISCOVER ENERGY SYSTEMS

Table of Contents

DISCOVER ENERGY SYSTEMS

1. Introduction

This document defines the Modbus TCP communication interface between the Battery Control Unit (BCU) of the Discover Energy Systems AES High-Voltage Energy Storage Cabinet and an Energy Management System (EMS), Microgrid Controller (MGC), or Power Conversion System (PCS). It specifies the frame format, supported function codes, the complete register map, and the control logic required to monitor and control the battery system.

The register map in this document is aligned with the battery OEM protocol BMS and EMS Communication Protocol - Modbus TCP - BMS Slave for II, V1.5.

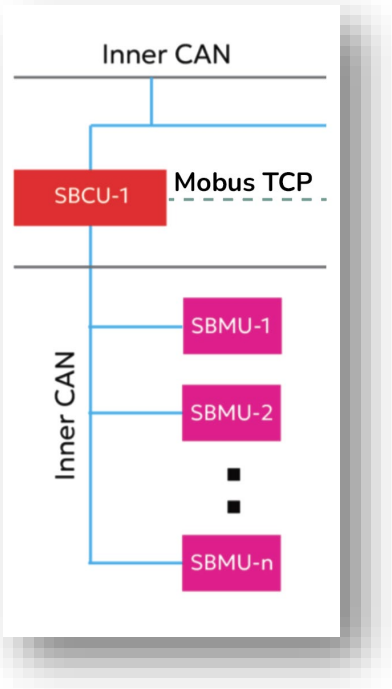
1.1 Audience

This document is intended for the use of engineers both internal and external to Discover Energy who intend to interface with the High Voltage Energy Storage Cabinet through the Modbus protocol. It is expected that the audience has a working knowledge of the Modbus standards for communication. If you are inexperienced in this topic, Discover recommends that you seek help from experienced personnel.

1.2 Glossary

Term	Description
BMS	Battery management system (SBAU + SBCU + SBMU hierarchy)
C&I	Commercial and industrial
EMS	Energy management system
MBAP	Modbus application protocol header
MGC	Microgrid controller
MSD	Manual service disconnect
PCS	Power conversion system
PDU	Protocol data unit
SBAU	Smart Battery Array Unit: aggregates multiple cabinets (clusters) in array installations
SBCU	Smart Battery Control Unit: supervises one battery cluster (cabinet)
SBMU	Smart Battery Management Unit: monitors cell voltages and temperatures within a pack
SOC / SOH / SOE	State of charge / state of health / state of energy
TMS	Thermal management system (liquid cooling unit)

1.3 System Topology



EMS/MGC to SBCU: Modbus TCP/IP (via RJ45 Ethernet)

SBCU to SBMU: CANbus

SBMU to cells: voltage and temperature monitoring

Auxiliary equipment (liquid cooler / TMS, dehumidifier, fire suppression, flood sensors, emergency stop) connects to the SBCU through dedicated CAN, RS-485, and dry-contact interfaces, and its status is exposed through the Modbus registers in this document.

Cluster/Pack Definition

A cluster represents one battery rack (cabinet), managed by one SBCU and composed of multiple SBMUs and battery cells (packs). The terms pack and cluster are used interchangeably in this document.

Each SBCU communicates with the EMS/MGC via Modbus TCP/IP (RJ45 Ethernet). Cabinets are individually controlled and monitored by the EMS via Modbus. The SBCU acts as the Modbus TCP/IP server; the EMS/MGC communicates as the Modbus TCP/IP client. In multi-cabinet array installations, an SBAU aggregates up to 32 clusters and presents them to the EMS on the same register map using the per-pack offset formulas defined in the appendices.

2. Communication and Network Details

2.1 Network Settings

Parameter	Value
Reference standard	GB/Z 19582.1-2004, Specification for Industrial Automation Networks Based on Modbus Protocol, Part III
Architecture	TCP/IP communication link, client/server. The BMS is the Modbus server; the EMS is the Modbus client
BMS IP address	192.168.1.101 (default). Configurable via the BMS Interface Software or registers 50329-50336 (restart required)
EMS IP address	192.168.1.10 recommended
Port	2404 (BMS as server)
Data format	Big-endian: the high byte is sent first. UINT32 values occupy two consecutive registers, high word first
Polling	EMS must send a 0x03 read request at intervals not exceeding 5 seconds
Communication timeout	BMS declares a timeout fault if no 0x03 request is received within 20 seconds. Detection is disabled by default (register 50337); timeout period configurable at register 50338 (default 60 s). Enable after field testing

For custom network configurations, use the BMS Interface Software to adjust the BMS IP address and port number. Connect a computer to the BMS via the designated communication port, then use the software to modify the IP address and port number to match your site's network requirements (e.g., static IP assignments, specific subnets, or firewall rules). If you do not have access to the BMS Interface Software or require detailed configuration instructions, contact Discover Energy Systems' Technical Support for the necessary tools and guidance.

2.2 Modbus Frame Format

The BCU uses a default Modbus TCP Unit ID of 0x01 (decimal value of 1). For standard Modbus TCP deployments the Unit ID is not used for device routing and should be set to 0x01 unless otherwise required by the client implementation. Where multiple BMS slaves share a link, addresses are allocated as Slave 1 = 0x01, Slave 2 = 0x02, Slave 3 = 0x03; the broadcast address 0x00 is not used.

Modbus communication acts as a client/server protocol. The client always initiates a Modbus communication. The server nodes do not send data to the client or any other server nodes unless they receive a request from a client.

MBAP Header	MBAP Header	MBAP Header	MBAP Header	PDU	PDU
Transaction identifier	Protocol identifier	Data length	Unit identifier / address	Function code	Data
2 bytes	2 bytes	2 bytes	1 byte	1 byte	N bytes

The MBAP header is defined as follows:

Segment Name	Length	Description	Value
Transaction identifier	2 bytes	Generated by the client and copied by the server; used for transaction processing pairing. Generally set to 0 by default.	0
Protocol identifier	2 bytes	Modbus protocol = 0	0
Data length	2 bytes	The number of bytes that follow, generated by the client and regenerated by the server in response.	Max 250
Unit identifier	1 byte	Defines the device linked to the destination node. Generated by the client and copied by the server when responding.	-

2.3 Modbus Function Codes Used

No.	Function Code	Description	Comments
1	0x03	Read the binary contents of holding registers in the server.	Primary polling command
2	0x06	Write a value into a single holding register.	Writable registers only (see appendix notes)
3	0x10	Write values into a sequence of consecutive holding registers.	Writable registers only (see appendix notes)

Function Code 0x03

Read the binary contents of holding registers in the server. Data length = 2 x number of data registers to read.

Client request:

Transaction ID	Protocol ID	Data Length	Unit ID / Addr	Function Code	Field 1	Field 2
0x00 0x00	0x00 0x00	2 bytes	0x01	0x03	Start address (2 bytes)	Number of registers (2 bytes)

Server normal response:

Transaction ID	Protocol ID	Data Length	Unit ID / Addr	Function Code	Field 1	Field 2
0x00 0x00	0x00 0x00	2 bytes	0x01	0x03	Byte count (1 byte)	Register data (N bytes)

Server exception response:

Transaction ID	Protocol ID	Data Length	Unit ID / Addr	Function Code	Field 1	Field 2
0x00 0x00	0x00 0x00	2 bytes	0x01	0x83 (0x03 + 0x80)	Error code (1 byte)	-

Function Code 0x06

Write a single holding register.

Client request:

Transaction ID	Protocol ID	Data Length	Unit ID / Addr	Function Code	Field 1	Field 2
0x00 0x00	0x00 0x00	2 bytes	0x01	0x06	Register address (2 bytes)	Register value (2 bytes)

Server normal response:

Transaction ID	Protocol ID	Data Length	Unit ID / Addr	Function Code	Field 1	Field 2
0x00 0x00	0x00 0x00	2 bytes	0x01	0x06	Register address (2 bytes)	Register value (2 bytes)

Server exception response:

Transaction ID	Protocol ID	Data Length	Unit ID / Addr	Function Code	Field 1	Field 2
0x00 0x00	0x00 0x00	2 bytes	0x01	0x86 (0x06 + 0x80)	Error code (1 byte)	-

Function Code 0x10

Write multiple consecutive holding registers.

Client request:

Transaction ID	Protocol ID	Data Length	Unit ID / Addr	Function Code	Register Address	Number of Registers	Byte Count	Data
0x00 0x00	0x00 0x00	2 bytes	0x01	0x10	2 bytes	2 bytes	1 byte	N bytes

Server normal response:

Transaction ID	Protocol ID	Data Length	Unit ID / Addr	Function Code	Field 1	Field 2
0x00 0x00	0x00 0x00	2 bytes	0x01	0x10	Register address (2 bytes)	Number of registers (2 bytes)

Server exception response:

Transaction ID	Protocol ID	Data Length	Unit ID / Addr	Function Code	Field 1	Field 2
0x00 0x00	0x00 0x00	2 bytes	0x01	0x90 (0x10 + 0x80)	Error code (1 byte)	-

2.4 Error Codes

No.	Name	Description
1	Code_one	0x01, invalid function code
2	Code_two	0x02, invalid request address
3	Code_three	0x03, invalid number of registers
4	Code_four	0x04, failed to write register data

An exception response returns the request function code + 0x80 followed by the error code.

3. Key Functional Interfaces

3.1 Status and Relay Monitoring

Pack status and relay states are read via function code 0x03.

Parameter	Address	Description
Pack operating status	4501	Bits: Initialization, Ready, Discharging, Charging, Alarm, Fault
Level I / II / III alarm codes	4504-4509	32-bit alarm codes; see Appendix 13
Maintenance alarm codes	4510-4513	32-bit alarm codes; see Appendices 14 and 15
Fire and MSD alarms	4532-4535	Per-pack fire and manual-service-disconnect alarms
Relay status feedback	60101+	Main positive/negative, pre-charge, breaker, fan, charge, discharge, dry contact

3.2 Common Battery Pack Data

Key operating data is read from the pack statistics block starting at register 1301 (Pack 1):

Metric	Address (Pack 1)	Unit
Total voltage	1301	0.1 V
Total current	1302	0.1 A (offset +32000)

Metric	Address (Pack 1)	Unit
SOC	1303	0.1 %
SOH	1304	0.1 %
Max cell voltage	1309	mV
Min cell voltage	1312	mV
Max cell temperature	1315	deg C (offset +40)
Min cell temperature	1318	deg C (offset +40)
Charge / discharge current limits	1323 / 1324	0.1 A

3.3 Monitoring Pack-Level Data

Pack statistics addressing per the protocol:

Offset address P = 1300 + 100 x n

n: pack index (0 for Pack 1, up to 31 for Pack 32). Each pack occupies 100 UINT16 registers. Example mapping:

Pack	Start Address (P+1)
1	1301
2	1401
3	1501
...	...
32	4401

3.4 Alarm and Protection Registers

Type	Registers
Level I-III alarm codes (active alarms)	4504-4509
Maintenance alarm codes (active alarms)	4510-4513
PACK fire / MSD alarms	4532-4535
Alarm threshold parameters	50001-50064

4. Control Interface and BMS Operating Logic

The EMS controls the battery system through the control registers at 61001-61007 (Appendix 9). The following behavior is defined by the OEM BMS control logic and must be implemented by the control's integrator.

4.1 Power-Up (High-Voltage Enable) Sequence

1. The BMS does not enable high voltage by default. The EMS must command power-up by writing 1 to register 61001.

2. Registers 61006 and 61007 select which packs are enabled for power-up; each bit represents one pack (e.g., 61006 = 0x0003 enables Packs 1 and 2).

3. Before closing relays, the BMS verifies that no Level 3 or maintenance fault is present, that relay feedback is normal, that total-voltage acquisition is valid, and that the circuit breakers of ready packs are closed. The pre-charge relay closes first, then the main positive relay of the lowest-voltage pack. Packs within the allowed voltage difference are connected; packs of lower voltage are charged with maintenance current until all enabled packs are connected.

4. If the pack-to-pack voltage difference exceeds the threshold, a high voltage-difference fault is raised, and the power-up sequence is aborted.

5. When all enabled packs are connected, the system enters the operating state (register 4501, Bit 1/2/3).

4.2 Power-Down Sequence

1. The EMS commands power-off by writing 2 to register 61001 (3 = emergency stop).

2. The BMS responds by limiting the charge/discharge current limits (registers 1323/1324) to 0. The EMS/PCS must reduce the working current to 0. When the BMS detects zero current it opens the main relays; if the PCS current does not decrease to 0, the BMS forcibly opens the relays after 5 seconds.

4.3 Protective Disconnection

On a Level 3 alarm, maintenance alarm, or external linkage alarm (fire detection, flood/water-immersion detection), the BMS requests a current limit of 0 and then disconnects the affected pack relays (or all packs for a system-level fault). Thermal-runaway detection additionally closes the K1 dry contact for external tripping. The EMS/PCS must always honor the charge and discharge current limits reported in registers 1323/1324.

4.4 Alarm Severity Levels

Level	Meaning	Expected Response
Level 1	Alarm (informational)	No human intervention required; BMS may derate
Level 2	Alarm	No human intervention required; BMS derates further
Level 3	Fault / protection	Affects safety; BMS executes protective disconnection. Some faults self-recover, others require maintenance. Fault reset can be enabled via register 61003
Maintenance	Equipment fault	Service required; see Appendices 14 and 15 for fault identification

The alarm-code registers are provided to the EMS for display and diagnostics. Threshold parameters for Level 1/2/3 alarms are held in registers 50001-50064 (Appendix 5). Firmware

updates of the SBAU/SBCU are performed over the CAN service port with the OEM upgrade tool; they are not performed over Modbus.

5. Data Address Map

NOTE. *The Start Address and End Address are included in the address range. Address numbers are in decimal format. Areas not listed are reserved and must not be written.*

Start Address	End Address	Data Storage Instructions	Reference
1	1300	Reserved	-
1301	4500	Battery pack statistics, 100 registers per pack. Supports up to 32 packs: 100 x 32 = 3200 UINT16. For the actual data size, refer to the specific plan.	Appendix 1. Battery Pack Statistics
4501	5000	Battery pack status information (4501-4535 used)	Appendix 2. Battery Pack Status
5001	10000	Reserved	-
10001	30000	Max 500 cell voltage data per pack. Max 32 packs: 500 x 32 = 16000 cell voltages.	Appendix 3. Battery Pack Cell Voltage Details
30001	38000	Max 250 cell temperature data per pack. Max 32 packs: 250 x 32 = 8000 cell temperatures.	Appendix 4. Battery Pack Cell Temperature Details
38001	50000	Reserved	-
50001	50300	Alarm parameters (50001-50064 used)	Appendix 5. Alarm Parameter Information
50301	50400	System parameters (50301-50338 used)	Appendix 6. System Operating Parameters
50401	50410	Time information (50401-50406 used)	Appendix 7. Time Information
50411	60100	Reserved	-
60101	60420	Relay status feedback, 10 registers per pack, maximum 32 packs: 10 x 32 = 320	Appendix 8. Relay Status Feedback
61001	61100	Battery cabinet control data (61001-61007 used)	Appendix 9. Battery Cabinet Control
62001	62100	TMS (liquid cooling) status	Appendix 10. TMS Status
62101	62200	TMS (liquid cooling) analog data	Appendix 11. TMS Data
62201	62300	Dehumidifier status (62201-62214 used)	Appendix 12. Dehumidifier Status

DISCOVER ENERGY SYSTEMS

Appendix 1. Battery Pack Statistics

Offset address P = 1300 + 100 x n (n represents the pack index, 0 <= n < 32; n = 0 represents the first pack). Pack 1 data begins at register 1301, Pack 2 at 1401, and Pack 32 at 4401.

NOTE. *The following data can only be accessed by the read function code 0x03.*

Register Address	Data Type	Data Description	Data / Units	Comments
P+1	UINT16	Total pack voltage	0.1 V	
P+2	UINT16	Total pack current	0.1 A	Offset +32000. Actual current (0.1 A) = raw value - 32000
P+3	UINT16	Pack SOC	0.1 %	
P+4	UINT16	Pack SOH	0.1 %	
P+5	UINT16	Pack insulation resistance, positive	kΩ	
P+6	UINT16	Pack insulation resistance, negative	kΩ	
P+7	UINT16	Maximum cell voltage - BMU number	-	
P+8	UINT16	Maximum cell voltage - cell serial number in module	-	
P+9	UINT16	Maximum cell voltage value	mV	
P+10	UINT16	Minimum cell voltage - BMU number	-	
P+11	UINT16	Minimum cell voltage - cell serial number in module	-	
P+12	UINT16	Minimum cell voltage value	mV	
P+13	UINT16	Maximum cell temperature - BMU number	-	
P+14	UINT16	Maximum cell temperature - cell serial number in module	-	
P+15	UINT16	Maximum cell temperature value	°C	Offset +40. Actual °C = raw value - 40
P+16	UINT16	Minimum cell temperature - BMU number	-	

Register Address	Data Type	Data Description	Data / Units	Comments
P+17	UINT16	Minimum cell temperature - cell serial number in module	-	
P+18	UINT16	Minimum cell temperature value	°C	Offset +40. Actual °C = raw value - 40
P+19	UINT16	Maximum cell voltage difference	mV	
P+20	UINT16	Average cell voltage	mV	
P+21	UINT16	Maximum temperature difference	°C	
P+22	UINT16	Average temperature	°C	Offset +40. Actual °C = raw value - 40
P+23	UINT16	Charge current limit	0.1 A	
P+24	UINT16	Discharge current limit	0.1 A	
P+25	UINT16	Pack charge/discharge cycle count	-	
P+26	UINT16	Single charge energy	0.1 kWh	
P+27	UINT16	Single discharge energy	0.1 kWh	
P+28, P+29	UINT32	Cumulative pack charge energy	0.1 kWh	High word first
P+30, P+31	UINT32	Cumulative pack discharge energy	0.1 kWh	High word first
P+32, P+33	UINT32	Pack available (chargeable) energy	0.1 kWh	Unit not stated in OEM V1.5; consistent with adjacent energy registers
P+34, P+35	UINT32	Pack available (dischargeable) energy	0.1 kWh	Unit not stated in OEM V1.5; consistent with adjacent energy registers
P+36	UINT16	SBCU software version	-	
P+37	UINT16	SBCU hardware version	-	
P+38	UINT16	SBMU software version	-	
P+39	UINT16	SBMU hardware version	-	

Appendix 2. Battery Pack Status

Registers 4501-4535. This block reports the status of the battery cluster served by the SBCU.

NOTE. *The following data can only be accessed by the read function code 0x03.*

Register Address	Data Type	Data Description	Data / Units	Comments
4501	UINT16	Pack operating status	Bit 0: Initialization; Bit 1: Ready (relays closed, not charging or discharging); Bit 2: Discharging; Bit 3: Charging; Bit 4: Alarm; Bit 5: Fault; other bits have no meaning	EMS/PCS must verify status: operation is permitted only when Bit 1, 2, 3, or 4 is set
4502	UINT16	Charging complete flag	Bit 0: 0 = charging not complete; 1 = charging complete	Reserved
4503	UINT16	Discharging complete flag	Bit 0: 0 = discharging not complete; 1 = discharging complete	Reserved
4504	UINT16	Level I alarm code - high 16 bits	See Appendix 13	
4505	UINT16	Level I alarm code - low 16 bits	See Appendix 13	
4506	UINT16	Level II alarm code - high 16 bits	See Appendix 13	
4507	UINT16	Level II alarm code - low 16 bits	See Appendix 13	
4508	UINT16	Level III alarm code - high 16 bits	See Appendix 13	
4509	UINT16	Level III alarm code - low 16 bits	See Appendix 13	
4510	UINT16	Maintenance alarm code 1 - high 16 bits	See Appendix 14	
4511	UINT16	Maintenance alarm code 1 - low 16 bits	See Appendix 14	
4512	UINT16	Maintenance alarm code 2 - high 16 bits	See Appendix 15	
4513	UINT16	Maintenance alarm code 2 - low 16 bits	See Appendix 15	

Register Address	Data Type	Data Description	Data / Units	Comments
4514, 4515	UINT32	SBMU communication failure address	Bit 0 = BMU 1 has this fault; Bit 1 = BMU 2; ... Bit 31 = BMU 32	
4516, 4517	UINT32	SBMU hardware fault address	Bit mapping as above	
4518, 4519	UINT32	SBMU wiring (disconnection) fault address	Bit mapping as above	
4520, 4521	UINT32	SBMU temperature-sensor disconnection fault address	Bit mapping as above	
4522, 4523	UINT32	SBMU balancing fault address	Bit mapping as above	
4524, 4525	UINT32	SBMU reserved fault register 1	-	Reserved
4526, 4527	UINT32	SBMU reserved fault register 2	-	Reserved
4528, 4529	UINT32	SBMU reserved fault register 3	-	Reserved
4530, 4531	UINT32	SBMU reserved fault register 4	-	Reserved
4532	UINT16	PACK fire alarms 1–8	See Appendix 16	Bits 8–15 reserved
4533	UINT16	Reserved (empty)	-	Listed as EMPTY in OEM protocol V1.5
4534	UINT16	PACK MSD alarms 1–8	See Appendix 17	Bits 8–15 reserved
4535	UINT16	Reserved (empty)	-	Listed as EMPTY in OEM protocol V1.5

Appendix 3. Battery Pack Cell Voltage Details

Offset address P = 10000 + 500 x n (n represents the pack index, 0 <= n < 32; n = 0 represents the first pack). Up to 500 cell voltages per pack.

NOTE. *The following data can only be accessed by the read function code 0x03.*

Register Address	Data Type	Data Description	Data / Units	Comments
P+1	UINT16	Cell voltage 1	mV	
P+2	UINT16	Cell voltage 2	mV	
P+3	UINT16	Cell voltage 3	mV	
...	UINT16	...	mV	
P+m	UINT16	Cell voltage m	mV	m represents the maximum number of cell voltages in the pack (m <= 500)

Appendix 4. Battery Pack Cell Temperature Details

Offset address P = 30000 + 250 x n (n represents the pack index, 0 <= n < 32; n = 0 represents the first pack). Up to 250 cell temperatures per pack.

NOTE. *The following data can only be accessed by the read function code 0x03.*

Register Address	Data Type	Data Description	Data / Units	Comments
P+1	UINT16	Cell temperature 1	deg C	Sent by BMS = actual temperature +40
P+2	UINT16	Cell temperature 2	deg C	Sent by BMS = actual temperature +40
P+3	UINT16	Cell temperature 3	deg C	Sent by BMS = actual temperature +40
...	UINT16	...	deg C	
P+m	UINT16	Cell temperature m	deg C	m represents the maximum number of cell temperatures in the pack (m <= 250)

Appendix 5. Alarm Parameter Information

Registers 50001-50064. Each monitored quantity has Level 1/2/3 alarm thresholds and a return (hysteresis) value.

NOTE. *The following data can be accessed by the read function code 0x03 and the write function codes 0x06/0x10. The OEM protocol V1.5 annex note marks this block as read-only; confirm write access against the installed firmware before depending on it.*

Register Address	Data Type	Data Description	Data / Units	Comments
50001	UINT16	Cell voltage high - Level 1 alarm value	mV	Default: 3550 mV
50002	UINT16	Cell voltage high - Level 2 alarm value	mV	Default: 3600 mV
50003	UINT16	Cell voltage high - Level 3 alarm value	mV	Default: 3650 mV
50004	UINT16	Cell voltage high - alarm return (hysteresis) value	mV	Default: 100 mV
50005	UINT16	Cell voltage low - Level 1 alarm value	mV	Default: 2900 mV
50006	UINT16	Cell voltage low - Level 2 alarm value	mV	Default: 2800 mV
50007	UINT16	Cell voltage low - Level 3 alarm value	mV	Default: 2600 mV
50008	UINT16	Cell voltage low - alarm return (hysteresis) value	mV	
50009	UINT16	Cell voltage difference high - Level 1 alarm value	mV	
50010	UINT16	Cell voltage difference high - Level 2 alarm value	mV	
50011	UINT16	Cell voltage difference high - Level 3 alarm value	mV	
50012	UINT16	Cell voltage difference high - alarm return (hysteresis) value	mV	
50013	UINT16	Total voltage high - Level 1 alarm value	0.1 V	
50014	UINT16	Total voltage high - Level 2 alarm value	0.1 V	
50015	UINT16	Total voltage high - Level 3 alarm value	0.1 V	

Register Address	Data Type	Data Description	Data / Units	Comments
50016	UINT16	Total voltage high - alarm return (hysteresis) value	0.1 V	
50017	UINT16	Total voltage low - Level 1 alarm value	0.1 V	
50018	UINT16	Total voltage low - Level 2 alarm value	0.1 V	
50019	UINT16	Total voltage low - Level 3 alarm value	0.1 V	
50020	UINT16	Total voltage low - alarm return (hysteresis) value	0.1 V	
50021	UINT16	Discharge current high - Level 1 alarm value	0.1 A	
50022	UINT16	Discharge current high - Level 2 alarm value	0.1 A	
50023	UINT16	Discharge current high - Level 3 alarm value	0.1 A	
50024	UINT16	Discharge current high - alarm return (hysteresis) value	0.1 A	
50025	UINT16	Charge current high - Level 1 alarm value	0.1 A	
50026	UINT16	Charge current high - Level 2 alarm value	0.1 A	
50027	UINT16	Charge current high - Level 3 alarm value	0.1 A	
50028	UINT16	Charge current high - alarm return (hysteresis) value	0.1 A	
50029	UINT16	Insulation low - Level 1 alarm value	kΩ	
50030	UINT16	Insulation low - Level 2 alarm value	kΩ	
50031	UINT16	Insulation low - Level 3 alarm value	kΩ	
50032	UINT16	Insulation low - alarm return (hysteresis) value	kΩ	
50033	UINT16	Charging temperature high - Level 1 alarm value	°C, +40	Real data +40 °C when sent by BMS

Register Address	Data Type	Data Description	Data / Units	Comments
50034	UINT16	Charging temperature high - Level 2 alarm value	°C, +40	Real data +40 °C when sent by BMS
50035	UINT16	Charging temperature high - Level 3 alarm value	°C, +40	Real data +40 °C when sent by BMS
50036	UINT16	Charging temperature high - alarm return (hysteresis) value	°C	
50037	UINT16	Charging temperature low - Level 1 alarm value	°C, +40	Real data +40 °C when sent by BMS
50038	UINT16	Charging temperature low - Level 2 alarm value	°C, +40	Real data +40 °C when sent by BMS
50039	UINT16	Charging temperature low - Level 3 alarm value	°C, +40	Real data +40 °C when sent by BMS
50040	UINT16	Charging temperature low - alarm return (hysteresis) value	°C	
50041	UINT16	Discharge temperature high - Level 1 alarm value	°C, +40	Real data +40 °C when sent by BMS
50042	UINT16	Discharge temperature high - Level 2 alarm value	°C, +40	Real data +40 °C when sent by BMS
50043	UINT16	Discharge temperature high - Level 3 alarm value	°C, +40	Real data +40 °C when sent by BMS
50044	UINT16	Discharge temperature high - alarm return (hysteresis) value	°C	
50045	UINT16	Discharge temperature low - Level 1 alarm value	°C, +40	Real data +40 °C when sent by BMS
50046	UINT16	Discharge temperature low - Level 2 alarm value	°C, +40	Real data +40 °C when sent by BMS
50047	UINT16	Discharge temperature low - Level 3 alarm value	°C, +40	Real data +40 °C when sent by BMS
50048	UINT16	Discharge temperature low - alarm return (hysteresis) value	°C	
50049	UINT16	Temperature difference high - Level 1 alarm value	°C	
50050	UINT16	Temperature difference high - Level 2 alarm value	°C	
50051	UINT16	Temperature difference high - Level 3 alarm value	°C	

Register Address	Data Type	Data Description	Data / Units	Comments
50052	UINT16	Temperature difference high - alarm return (hysteresis) value	°C	
50053	UINT16	SOC low - Level 1 alarm value	0.1 %	
50054	UINT16	SOC low - Level 2 alarm value	0.1 %	
50055	UINT16	SOC low - Level 3 alarm value	0.1 %	
50056	UINT16	SOC low - alarm return (hysteresis) value	0.1 %	
50057	UINT16	SOC high - Level 1 alarm value	0.1 %	
50058	UINT16	SOC high - Level 2 alarm value	0.1 %	
50059	UINT16	SOC high - Level 3 alarm value	0.1 %	
50060	UINT16	SOC high - alarm return (hysteresis) value	0.1 %	
50061	UINT16	Pack voltage difference high (cumulative) - Level 1 alarm value	0.1 V	Cumulative differential voltage
50062	UINT16	Pack voltage difference high (cumulative) - Level 2 alarm value	0.1 V	Cumulative differential voltage
50063	UINT16	Pack voltage difference high (cumulative) - Level 3 alarm value	0.1 V	Cumulative differential voltage
50064	UINT16	Pack voltage difference high (cumulative) - alarm return (hysteresis) value	0.1 V	Cumulative differential voltage

Appendix 6. System Operating Parameters

Registers 50301-50338.

NOTE. *The following data can be accessed by the read function code 0x03 and the write function codes 0x06/0x10. The OEM protocol V1.5 annex note marks this block as read-only; confirm write access against the installed firmware before depending on it.*

Register Address	Data Type	Data Description	Data / Units	Comments
50301	UINT16	Passive equalization start - voltage difference	mV	
50302	UINT16	Passive equalization start - minimum cell voltage	mV	
50303	UINT16	Fan on temperature	°C, +40	Real data +40 °C when sent by BMS
50304	UINT16	Fan off temperature	°C, +40	Real data +40 °C when sent by BMS
50305	UINT16	Fan cell voltage	mV	
50306	UINT16	Maximum allowable current, single-pack charging	0.1 A	
50307	UINT16	Minimum allowable current, single-pack charging	0.1 A	
50308	UINT16	Charge current reduction - cell voltage	mV	
50309	UINT16	Charge stop - cell voltage	mV	
50310	UINT16	Maximum allowable current, single-pack discharge	0.1 A	
50311	UINT16	Minimum allowable current, single-pack discharge	0.1 A	
50312	UINT16	Discharge current reduction - cell voltage	mV	
50313	UINT16	Discharge stop - cell voltage	mV	
50314	UINT16	Pre-charge voltage	0.1 V	
50315	UINT16	Pack cumulative total-voltage-difference alarm value	0.1 V	
50316	UINT16	Cooling set temperature	°C	
50317	UINT16	Cooling start temperature	°C	
50318	UINT16	Cooling stop temperature	°C	
50319	UINT16	Heating set temperature	°C	
50320	UINT16	Heating start temperature	°C	

Register Address	Data Type	Data Description	Data / Units	Comments
50321	UINT16	Heating stop temperature	°C	
50322	UINT16	Self-circulation minimum temperature	°C	
50323	UINT16	Self-circulation maximum temperature	°C	
50324	UINT16	Self-circulation start temperature difference	°C	
50325	UINT16	Self-circulation stop temperature difference	°C	
50326	UINT16	Dehumidifier - humidity start value	%	
50327	UINT16	Dehumidifier - humidity stop value	%	
50328	UINT16	Dehumidifier - heating start value	°C	
50329	UINT16	IP_Addr1_1	-	IP address changes take effect after restart
50330	UINT16	IP_Addr1_2	-	
50331	UINT16	IP_Addr1_3	-	
50332	UINT16	IP_Addr1_4	-	
50333	UINT16	IP_Addr2_1	-	
50334	UINT16	IP_Addr2_2	-	
50335	UINT16	IP_Addr2_3	-	
50336	UINT16	IP_Addr2_4	-	
50337	UINT16	EMS communication fault enable	-	Disabled by default; enable after commissioning
50338	UINT16	EMS communication timeout period	s	Default: 60 seconds

Appendix 7. Time Information

Registers 50401-50406.

NOTE. *The following data can be accessed by the read function code 0x03 and the write function codes 0x06/0x10.*

Register Address	Data Type	Data Description	Data / Units	Comments
50401	UINT16	Year	-	
50402	UINT16	Month	1–12	
50403	UINT16	Day	1–31	
50404	UINT16	Hour	0–23	
50405	UINT16	Minute	0–59	
50406	UINT16	Second	0–59	

Appendix 8. Relay Status Feedback

Offset address P = 60100 + 10 x n (n represents the pack index, 0 <= n < 32; n = 0 represents the first pack). Pack 1 relay status begins at register 60101.

NOTE. *The following data can only be accessed by the read function code 0x03.*

Register Address	Data Type	Data Description	Data / Units	Comments
P+1	UINT16	Main positive relay status	0 = open; 1 = closed	
P+2	UINT16	Main negative relay status	0 = open; 1 = closed	
P+3	UINT16	Main pre-charge relay status	0 = open; 1 = closed	
P+4	UINT16	Breaker relay status	0 = open; 1 = closed	
P+5	UINT16	Fan relay status	0 = open; 1 = closed	
P+6	UINT16	Charge relay status	0 = open; 1 = closed	
P+7	UINT16	Discharge relay status	0 = open; 1 = closed	
P+8	UINT16	Dry contact status K1	0 = open; 1 = closed	

Appendix 9. Battery Cabinet Control

Registers 61001-61007.

NOTE. *The BMS does not enable high voltage by default. The following data can be accessed by the read function code 0x03 and the write function code 0x06.*

Register Address	Data Type	Data Description	Data / Units	Comments
61001	UINT16	Enable high voltage (pack power on/off)	0 = no action; 1 = enable high voltage (power on); 2 = disconnect pack relays (power off / lower voltage); 3 = emergency stop; other values have no meaning	EMS sends the enable signal to the BMS. The BMS does not enable high voltage by default
61002	UINT16	Insulation detection control	0 = no action; 1 = turn off insulation detection; 2 = turn on insulation detection, do not check insulation after power-up; 3 = insulation detection on, polls to detect insulation after power-up; other values have no meaning	
61003	UINT16	Fault reset enable	0 = disable fault reset; 1 = enable fault reset; other values have no meaning	
61004	UINT16	Set cluster ID	-	
61005	UINT16	PCS fan control	0 = N/A; 1 = N/A	Not applicable for the AES cabinet
61006	UINT16	Pack power-up enable 1–16	Each bit enables power-up of one pack: 0 = disabled, 1 = enabled. Bit 0 = Pack 1, Bit 1 = Pack 2, ... up to 16 bits	Referenced by the OEM power-on/power-off control logic; not listed in protocol V1.5 Annex 10
61007	UINT16	Pack power-up enable 17–32	Each bit enables power-up of one pack: 0 = disabled, 1 = enabled. Bit 0 = Pack 17, Bit 1 = Pack 18, ... up to 16 bits	Referenced by the OEM power-on/power-off control logic; not listed in protocol V1.5 Annex 10

Appendix 10. TMS Status

Registers 62001-62006. Validity depends on the project-specific thermal configuration.

NOTE. *The following data depends on the configuration of the project and can only be accessed by the read function code 0x03.*

Register Address	Data Type	Data Description	Data / Units	Comments
62001	UINT16	TMS operating status	0 = off; 1 = cooling mode; 2 = heating mode; 3 = self-circulation mode	
62002	UINT16	TMS K1 high-voltage relay status	0 = open; 1 = closed	
62003	UINT16	TMS K2 high-voltage relay status	0 = open; 1 = closed	
62004	UINT16	TMS preheat (warm-up) mode feedback	0 = exit preheat mode; 1 = enter preheat mode	
62005	UINT16	TMS fault code	0 = no fault. Multiple fault types are transmitted cyclically	
62006	UINT16	TMS fault level	0 = invalid; 1 = Level 1 fault	

Appendix 11. TMS Data

Registers 62101-62105.

NOTE. *The following data depends on the configuration of the project and can only be accessed by the read function code 0x03.*

Register Address	Data Type	Data Description	Data / Units	Comments
62101	UINT16	TMS outlet (supply) water temperature	°C	Resolution 1 °C/bit; offset +40 (actual = raw - 40); range -40 to 210 °C
62102	UINT16	TMS return water temperature	°C	As above
62103	UINT16	TMS ambient temperature	°C	As above
62104	UINT16	TMS inlet pressure	bar	Resolution 0.1 bar/bit; offset 0; range 0 to 25.0 bar
62105	UINT16	TMS outlet pressure	bar	Resolution 0.1 bar/bit; offset 0; range 0 to 25.0 bar

Appendix 12. Dehumidifier Status

Registers 62201-62214. Validity depends on the project-specific configuration.

NOTE. *The following data can only be accessed by the read function code 0x03.*

Register Address	Data Type	Data Description	Data / Units	Comments
62201	UINT16	Current temperature	°C, +40	Real data +40 °C when sent by BMS
62202	UINT16	Current humidity	%RH	
62203	UINT16	Humidity start value	%RH	
62204	UINT16	Humidity stop value	%RH	
62205	UINT16	Heating start value	°C, +40	Real data +40 °C when sent by BMS
62206	UINT16	Temperature alarm value	°C, +40	Real data +40 °C when sent by BMS
62207	UINT16	Humidity alarm value	%RH	
62208	UINT16	Heating state	-	
62209	UINT16	Dehumidifier operating status	-	
62210	UINT16	Dehumidifier manual/automatic switch	-	
62211	UINT16	Manual humidification output	-	
62212	UINT16	Manual heating output	-	
62213	UINT16	Over-temperature alert	-	
62214	UINT16	Over-humidity alert	-	

Appendix 13. Level I, II, and III Alarm Codes

One shared code table applies to the Level I, II, and III alarm code registers (4504-4509). Each level's code is a 32-bit value split across a high and a low 16-bit register: the low register carries Bits 0-15 and the high register carries Bits 16-31. For each bit, 1 = alarm active and 0 = no alarm.

Low 16-bit register (4505 / 4507 / 4509):

Alarm Name	Bit	Alarm Code
High discharge temperature	Bit 0	0x0001
Low discharge temperature	Bit 1	0x0002

Alarm Name	Bit	Alarm Code
High cell voltage	Bit 2	0x0004
Low cell voltage	Bit 3	0x0008
High cell voltage difference	Bit 4	0x0010
Low SOC	Bit 5	0x0020
High SOC	Bit 6	0x0040
High pole (terminal) temperature	Bit 7	0x0080
High charging current	Bit 8	0x0100
High discharge current	Bit 9	0x0200
High temperature difference	Bit 10	0x0400
Low insulation	Bit 11	0x0800
High total voltage	Bit 12	0x1000
Low total voltage	Bit 13	0x2000
High charging temperature	Bit 14	0x4000
Low charging temperature	Bit 15	0x8000

High 16-bit register (4504 / 4506 / 4508):

Alarm Name	Bit	Alarm Code
Rapid temperature rise	Bit 16 (high register Bit 0)	0x00010000
High single-pack total voltage	Bit 17 (high register Bit 1)	0x00020000

Appendix 14. Maintenance Alarm Code 1

32-bit value across registers 4510 (high 16 bits) and 4511 (low 16 bits). For each bit, 1 = alarm active and 0 = no alarm.

Alarm Name	Bit	Alarm Code
SBMU hardware failure	Bit 0	0x00000001
Battery wiring failure	Bit 1	0x00000002
SBMU communication failure	Bit 2	0x00000004
Temperature wiring failure	Bit 3	0x00000008
Main negative relay failure	Bit 4	0x00000010
Main positive relay failure	Bit 5	0x00000020
Pre-charge fault	Bit 6	0x00000040
Fuse failure	Bit 7	0x00000080

Alarm Name	Bit	Alarm Code
Emergency stop	Bit 8	0x00000100
Current loop failure	Bit 9	0x00000200
Total voltage acquisition invalid	Bit 10	0x00000400
Cell voltage abnormally high	Bit 11	0x00000800
Cell voltage extremely high	Bit 12	0x00001000
Cell voltage extremely low	Bit 13	0x00002000
Temperature extremely high	Bit 14	0x00004000
Relay forced control	Bit 15	0x00008000
Reserved (empty)	Bit 16	0x00010000
Communication error with SBAU	Bit 17	0x00020000
Communication error with EMS	Bit 18	0x00040000
EMS/PCS forced (hard) control	Bit 19	0x00080000
Communication error with PCS	Bit 20	0x00100000
Communication error with display	Bit 21	0x00200000
Fan failure	Bit 22	0x00400000
Insufficient packs in position	Bit 23	0x00800000
EMS - emergency stop	Bit 24	0x01000000
EMS - lower high voltage	Bit 25	0x02000000
Initialization blocked	Bit 26	0x04000000
Maintenance charging	Bit 27	0x08000000
High-voltage box temperature acquisition failure	Bit 28	0x10000000
Passive balancing failure	Bit 29	0x20000000
Active balancing failure	Bit 30	0x40000000
SBCU-QF circuit breaker failure	Bit 31	0x80000000

Appendix 15. Maintenance Alarm Code 2

32-bit value across registers 4512 (high 16 bits) and 4513 (low 16 bits). Bits 11-31 are reserved.

Alarm Name	Bit	Alarm Code
Loop current alarm	Bit 0	0x00000001
Incorrect operation mode setting	Bit 1	0x00000002
BMU thermistor failure	Bit 2	0x00000004
Main negative fuse failure	Bit 3	0x00000008

Alarm Name	Bit	Alarm Code
Main positive fuse failure	Bit 4	0x00000010
Smoke sensor failure	Bit 5	0x00000020
Temperature sensor failure	Bit 6	0x00000040
Fire-suppression equipment malfunction	Bit 7	0x00000080
Flood sensor failure	Bit 8	0x00000100
Travel (limit) switch	Bit 9	0x00000200
SPD (surge protection) failure	Bit 10	0x00000400

Appendix 16. Pack Fire Alarms

Register 4532 carries fire alarms for packs 1-8 (Bit 0 = Pack 1). Bits 8-15 and register 4533 are reserved in protocol V1.5.

Alarm Name	Bit	Alarm Code
PACK1 fire alarm	Bit 0	0x0001
PACK2 fire alarm	Bit 1	0x0002
PACK3 fire alarm	Bit 2	0x0004
PACK4 fire alarm	Bit 3	0x0008
PACK5 fire alarm	Bit 4	0x0010
PACK6 fire alarm	Bit 5	0x0020
PACK7 fire alarm	Bit 6	0x0040
PACK8 fire alarm	Bit 7	0x0080

Appendix 17. Pack MSD Alarms

Register 4534 carries MSD (manual service disconnect) alarms for packs 1-8 (Bit 0 = Pack 1). Bits 8-15 and register 4535 are reserved in protocol V1.5.

Alarm Name	Bit	Alarm Code
PACK1 MSD alarm	Bit 0	0x0001
PACK2 MSD alarm	Bit 1	0x0002
PACK3 MSD alarm	Bit 2	0x0004
PACK4 MSD alarm	Bit 3	0x0008
PACK5 MSD alarm	Bit 4	0x0010
PACK6 MSD alarm	Bit 5	0x0020
PACK7 MSD alarm	Bit 6	0x0040
PACK8 MSD alarm	Bit 7	0x0080

DISCOVER
ENERGY SYSTEMS

13711 International Pl Unit 320,
Richmond, BC, V6V 2Z8, Canada
+ 1.604.242.0350
info@discoverenergysys.com
discoverenergysys.com