

Modbus register map

The authoritative Modbus reference for the CPU. Modbus (RS485/UART) is the primary service, configuration and telemetry interface. The same address map is reused for register access over CAN.

This page describes the PLC profile of firmware **30.08** (FIRMWARE_REVISION = 0x1e08), with MAX_MODULES = 34, a 140-byte UART buffer and at most 64 registers per request. It is implemented in `modbus.c` (MODBUS_userMemoryMap()), which maps a register address directly onto a byte offset into one of the three global structs. **This is the key fact:** the register map *is* the in-memory layout of DATALAYER / COMMAND / CONFIGLAYER (firmware architecture), so the struct definitions in `data.h` are the ground truth for exact offsets.

Conventions

- All registers are **16-bit**. Multi-register values (`uint32/int32`) occupy two consecutive registers.
- Standard Modbus holding-register access (read/write). Writes into a section trigger a side-effect handler (e.g. config writes persist to EEPROM; command writes drive outputs).
- Signedness and scale are **per field** — see each table’s unit column. The fixed-point scales themselves (0.1 mV, 0.1 A, centiKelvin, SOC ×100, ...) are defined once in the canonical units and scaling table.
- Multi-register 32-bit values use the first register as the low word (LSW), followed by the high word (MSW).

Modbus RTU profile

Property	Value
UART	115200 bit/s, asynchronous, 8 data bits
Default slave address	1
Functions	0x03 Read Holding Registers, 0x10 Write Multiple Registers
Maximum request	64 registers
Register byte order	Big-endian on the wire
CRC	Standard Modbus CRC16, low byte first

Address sections

Base	Length	Struct	Access	Purpose
1000	29 valid, stride 50 / module	DATALAYER.module[n]	R (mostly)	Per-module data. Module 1 starts at 1000; module 34 at 2650.
3000	48	DATALAYER (from warning)	R (+ a few W)	Pack data and fault flags, 3000–3047.
3500	8	COMMAND	R/W	Host→BMS commands and test triggers, 3500–3507.
4000	81	CONFIGLAYER	R/W	Persistent configuration, 4000–4080. A write saves EEPROM.
5000/5001/5002	1	—	R/W	Identity & actions (see below).
7777	1	unlockCode	R/W	Unlock code register (gates protected config).

Section bases are the MODBUS_*_START defines in `config.h`.

Section 3000 — pack data (read)

Offset 0 is `DATALAYER.warning`; register address is `3000 + fieldOffset`. The table below is byte-accurate for firmware 30.08:

Reg	Field	Type	Unit / meaning
3000	warning	bitfield	Pack warning flags (safety).
3001	error	bitfield	Pack error flags.
3002	errorCPU	bitfield	Internal CPU faults (<code>error_system_t</code>).
3003	current	int16	Pack current, 0.1 A.
3004	voltage	uint16	Pack voltage, 0.01 V.
3005	speed	uint16	Vehicle speed, 0.01 km/h; legacy.
3006	SOC	uint16	State of charge $\times 100$ (5000 = 50 %).
3007	cellMin	uint16	Min cell voltage, 0.1 mV.
3008	cellMax	uint16	Max cell voltage, 0.1 mV.
3009	motorTemp	uint16	Motor temperature, centiKelvin; unused in storage firmware.
3010	ampAhCounter	int16	Coulomb counter, 0.01 Ah. Write here triggers Ah-counter reset.
3011	trip	uint16	Trip distance, legacy; not accumulated in this firmware.
3012	throttleOverride	uint16	Throttle/power override, 0–255; 255 = fully limited.
3013	tempMin	uint16	Min temp, centiKelvin.
3014	tempMax	uint16	Max temp, centiKelvin (drives high-temperature derating/faults).
3015	avgTemp	uint16	Average temp, centiKelvin (drives cold-charge derating).
3016	balTempMax	uint16	Maximum balancing-resistor temperature, centiKelvin.
3017–3021	AI_volt[0..4]	uint16 $\times 5$	CPU analog inputs, 0.1 mV. Input 1 is the central current sensor; input 3 is switch NTC; input 4 is precharge feedback.
3022	numModules	uint16	Modules detected from config.
3023	numCells	uint16	Total configured cells.
3024	pecCounter	uint16	PEC error counter.
3025	pecPercent	uint16	PEC health %.
3026–3027	ampAsPosCounter	uint32, LSW/MSW	Positive current integral, 0.01 As.
3028–3029	ampAsNegCounter	uint32, LSW/MSW	Negative current integral, 0.01 As.
3030	outputs	bitfield	Internal output state, bits 0–5 outputs, bits 6–7 bistable states.
3031–3032	ampAsLastCounter	int32, LSW/MSW	Last current-integrator state used for SOC, 0.01 As.
3033	currentLimitChg	uint16	Current Charge Current Limit (CCL), 0.1 A.
3034	currentLimitDchg	uint16	Current Discharge Current Limit (DCL), 0.1 A.
3035	voltageLimitChg	uint16	Current Charge Voltage Limit (CVL), 0.01 V.
3036	voltageLimitDchg	uint16	Current discharge-voltage limit, 0.01 V.
3037	switchTemp	uint16	Contact/switch NTC, centiKelvin.
3038	minCellVoltageDynamic	uint16	Dynamic minimum-cell limit, mV/cell.
3039	cellMinMod, cellMinIdx	uint8 $\times 2$	Low byte module, high byte cell of minimum voltage; indexes start at 1.
3040	cellMaxMod, cellMaxIdx	uint8 $\times 2$	Low byte module, high byte cell of maximum voltage.
3041	cellTMinMod, cellTMinIdx	uint8 $\times 2$	Low byte module, high byte sensor of minimum temperature.
3042	cellTMaxMod, cellTMaxIdx	uint8 $\times 2$	Low byte module, high byte sensor of maximum temperature.
3043–3045	socAvg[0..2]	uint16 $\times 3$	Internal three-sample SOC averaging buffer, SOC $\times 100$.
3046	errorLast	bitfield	Error flags from the previous safety cycle.

Reg	Field	Type	Unit / meaning
3047	pecBlockCount	uint16	Reserved PEC block counter; currently not updated.

Registers 3000, 3001 and 3046 use the same bit layout:

Bit	Field	Meaning
0	cellVoltHigh	High cell voltage.
1	cellVoltLow	Low cell voltage.
2	cellTempHigh	High cell temperature.
3	cellTempLow	Low cell temperature; forced clear in 30.08.
4	currentOver	Overcurrent.
5	currentUnder	Current below configured condition.
6	voltDiff	SOC/extreme-cell mismatch warning or error.
7	isolation	Isolation fault.
8	communication	Module communication fault.
9	socLow	Low SOC.
10	motorTempOver	Motor over-temperature; legacy.
11	switchTempOver	Contactor/switch over-temperature.
14	tempCalc	Temperature calculation fault.
15	contactor	Contactor fault.

Register 3002 (`errorCPU`) uses:

Bit	Field	Meaning
0	contactor	Contactor control fault.
1	precharge	Precharge fault.
2	systemFail	General system fault.
3	eeepromFail	EEPROM fault.
4	bootFail	Boot fault.
5	sdCardFail	SD/FatFs fault; not set when FatFs is disabled.
6	configFail	Invalid configuration was detected/corrected.
7	tempCalcMotorFail	Motor-temperature calculation fault; legacy.
8	tempCalcNTCFail	NTC calculation fault.
9	turnedOffTimeout	Turned off by no-current timeout.
10	CANconfig	Invalid CAN configuration.

Section 3500 — commands (read/write)

Offset 0 = `COMMAND.main`. Writes here run `OUTPUTS_modbusControl()`.

Reg	Field	Meaning
3500	main	Bit 0 <code>turnOn</code> (contactor request), bit 1 <code>victronOn</code> . CAN-set 3500 is timeout-protected (<code>API_can3500timeout</code>).
3501	test	Test bits: bit 0 balancing 1, 1 balancing 2, 2 output cycle, 3 outputs off, 4 beeper, 5 charger on, 6 charger off, 7 overdischarge, 8 overcharge, 9 overtemperature, 10 undertemperature, 11 vent.
3502	outputsOn	Force-on mask for outputs/relays.
3503	outputsOff	Force-off mask.
3504	beeperTime	Beeper duration/mode.
3505	flags	Status flags (<code>battAlmostFullFlag</code> , ...).
3506	feedback	DI/DO feedback (inputs & output states).
3507	moduleTestCommand	0=off; 1..34 force module ON; 101..134 force OFF; 200 calibrate all configured modules; 201..234 calibrate one.

The manual ON/OFF override expires after approximately one second. Current-sensor calibration switches the selected module off, waits five seconds, samples and saves its 6-bit offset into 4002–4015, switches the module back on for one second and exits. A short beep marks the start of each calibration step.

Section 4000 — configuration (read/write, persisted)

Offset 0 = `CONFIGLAYER.numModulesConf`. A write persists via `DATA_saveConfiglayer()`. These offsets are **authoritative** — the `config_t` struct annotates them directly. Registers **4079–4080 require the unlock code** (write `MODBUS_SECRET_CODE` = 1234 to reg 7777 first).

Reg	Field	Type	Meaning
4000	<code>numModulesConf</code>	uint16	Number of configured modules.
4001	<code>moduleConfig</code>	uint16	Module topology (1 = 8+1+8+1 gapped).
4002–4015	<code>moduleCurrentOffsetPacked</code>	packed	Per-module current-sensor offsets: signed 6-bit, 2 mV/step, −64..+62 mV.
4016	<code>moduleCurrentOffsetPacked[14]</code>	uint16	Spare in the current packed-offset format.
4017	<code>tempHighLimit</code>	uint16	High-temperature derating start [°C]. +5 warn, +10 error. <i>Width widened & meaning changed in 30.08 — was uint8 hard cutoff.</i>
4018	<code>currentSensor</code>	uint16	0=off, 1=CPU ADC, 2=module sensors.
4019	<code>currentSensorOffset</code>	uint16	CPU ADC current offset [mV].
4020	<code>currentSensorSlope</code>	int16	Current-sensor sensitivity, 0.01 mV/A; e.g. 660 = 6.60 mV/A.
4021	<code>capacity</code>	uint16	Pack capacity [Ah].
4022	<code>wheelCircumference</code>	uint16	[mm] (vehicle).
4023	<code>numPoles</code>	uint16	Poles × ratio / 100 (speed calc).
4024	<code>driftConfig</code>	bitfield	SOC OCV drift tuning, packed as 4-bit nibbles: bits 0–3 <code>internalBattR</code> , bits 4–7 <code>driftSpeed</code> , bits 8–11 <code>topBottomSpeedup</code> , bits 12–15 reserved. Default/recommended 0x0513 = 1299 (R=3, <code>driftSpeed</code> =1, <code>topBottomSpeedup</code> =5). See SOC drift FAQ.
4025	<code>cpuRefVolt</code>	uint16	ADC reference [mV].
4026	<code>cpuRefOhms</code>	uint16	Reference resistance [ohm].
4027	<code>ktyType</code>	uint16	KTY sensor type (0 = NTC).
4028	<code>ntcBeta</code>	uint16	NTC beta.
4029	<code>maxCellVoltage</code>	uint16	Over-voltage error threshold [mV].
4030	<code>minCellVoltage</code>	uint16	Under-voltage error threshold [mV].
4031	<code>balancingTreshold</code>	uint16	Min cell voltage to allow balancing [mV].

Reg	Field	Type	Meaning
4032	balancingDelta	uint16	Max allowed cell spread [mV].
4033	warningMargin	uint16	Warning offset from error thresholds [mV].
4034	shutdownTimeout	uint16	Shutdown timeout after error.
4035	outputMode	bitfield	Output/contactor mode (<code>outputmode_t</code>).
4036	keyswitchMode	bitfield	DI key-switch/power-limit mode (<code>inputmode_t</code>).
4037	outputFlags	bitfield	<code>outputflags_t</code> — bit 2 <code>lowVoltageDynamicLimit</code> , bit 10 <code>ventSyncMode</code> , bit 15 <code>bmsSuspended</code> , bit 0 <code>prechargeFb</code> , bit 1 <code>ignitionOffLowVoltWarning</code> .
4038	soundConfig	uint16	Beeper enable/config.
4039	canConfig	uint16	CAN address/baud selector (see CAN).
4040	maxMotorTemperature	uint16	Motor temp limit.
4041	watchdogNoComm	uint16	No-comm reboot/limp watchdog [s].
4042	throttleOverrideMode	uint16	Throttle/power override when DI1 limiting is active, 0–255.
4043	prechargeResistorDivider	uint16	Precharge feedback divider.
4044	timeoutTurnOffNoAmps	uint16	Automatic HV off after low/no current [s]; 65535 disables it.
4045	chargeEndVoltage	uint16	Per-cell charge target [mV].
4046	maxChargeCurrent	uint16	CCL ceiling [0.1 A].
4047	dischargeEndVoltage	uint16	Per-cell discharge floor [mV].
4048	maxDischargeCurrent	uint16	DCL ceiling [0.1 A].
4049	socHighLimit / socLowLimit	uint8×2	SOC high/low limits (packed).
4050	maxSwitchTemperature	uint16	Contactor NTC limit [centiKelvin].
4051–4061	SoC_OCV_table[11]	uint16×11	OCV→SOC lookup.
4062	proportional	uint16	Width of the linear CCL taper below 4045, 0.1 mV/cell.
4063	socHL	uint8×2	Low byte high SOC threshold, high byte low SOC threshold; default 0x0A5A = 90/10 %.
4064	parallelPack	uint16	Parallel-string count (CVL divisor).
4065	cvlUpdatePeriodSec	uint16	Dynamic CVL trim period [s].
4066	cvlTrimStepMvPerCell	uint16	CVL trim step [mV/cell].
4067	cvlMaxTrimMvPerCell	uint16	CVL max trim [mV/cell].
4068	chargeSocRampEndPct	uint16	SOC above which charge unrestricted.
4069	chargeSocMinCurrentPct	uint16	Charge floor % at low SOC / hot / cold.
4070	chargeTempRampEndDegC	uint16	Cold-charge ramp end [°C above 0].
4071	chargeTempMinCurrentPct	uint16	Cold-charge floor %.
4072–4075	totalEnergyIn / totalEnergyOut	uint32×2	Energy totals [100 Wh].
4076	socSaved	uint16	SOC persisted across restart, SOC ×100.
4077–4078	totalDistance	uint32, LSW/MSW	Total distance [m]; legacy.
4079	runtimeCounter	uint16	Runtime in 2-hour increments; write requires unlock .
4080	serialNumber	uint16	CPU serial number; write requires unlock .

Packed module-current offsets, 4002–4016

Each module occupies a signed two’s-complement 6-bit value. One step is 2 mV:

```

bit_index = 6 * (module - 1)
register   = 4002 + floor(bit_index / 16)
shift     = bit_index % 16
offset_mV = sign_extend_6bit(raw) * 2

```

A value can cross a register boundary. Registers 4002–4015 contain all 36 calibration values; register 4016 remains spare.

Output mode, 4035

Bit	Meaning
0	DO0 main contactor.
1	DO0+DO1 bistable discharge relay.
2	DO3+DO4 bistable charge relay.
3	DO2 on low-voltage warning.
4	DO5 on high-voltage warning.
5	DO3 on low-voltage error.
6	DO4 on high-voltage error.
7	Invert NO/NC behavior of bits 3–6.
8	DO2 on high-voltage warning with hysteresis.
9	DO0+DO1 combined charge/discharge bistable relay.
10	DO5 low-voltage/SOC hysteresis using 4049.
11	DO3 controlled by low SOC threshold 4063.
12	DO1 pulsed SOC indication.
13	DO4 controlled by high SOC threshold 4063.
14	Charge bistable relay on DO1+DO2.
15	DO3+DO4 two-color SOC indication.

Input mode, 4036

Bits 0–1 select the DI0 keyswitch mode: 0 = Modbus/CAN command only, 1 = automatically on after boot, 2 = follow DI0, 3 = long-press toggle. Bits 2–3 (**di1keyswitch**) are defined but not evaluated in 30.08. Bit 4 enables DI1 power limiting using register 4042.

Output flags, 4037

Bit	Meaning
0	Check precharge feedback.
1	Turn ignition off on low-voltage warning.
2	Enable current-dependent dynamic low-voltage limit.
10	Drive LTC GPIO9 vent as synchronization heartbeat.
15	BMS suspended.

Section 1000 — per-module data (read)

For one-based module number n , base address $B = 1000 + (n - 1) \times 50$. Only offsets 0–28 map onto `module_t`; offsets 29–49 are an address gap and firmware returns Modbus exception 2 (Illegal Data Address). The structure contains: `V_Cell[18]`, `T_Cell[6]`, `amps`, `ampsFiltered`, `ampsRaw`, `Vref`, `balancing[3]`, `pecErrorCount`, `commFailCycles`, `dataStale`, `cfg`. Per-module PEC error count and staleness are visible here (`commFailCycles`, `dataStale` were added in 30.08). Current Node-RED flows read the first 28 registers from each module window (`maxModuleRegs = 28`, `moduleRegStride = 50`).

Reg	Field	Type	Unit / meaning
B+0 .. B+17	<code>V_Cell[0] .. V_Cell[17]</code>	<code>uint16</code> ×18	Cell voltage, 0.1 mV. In 30.x these are 18 physical positions. With the 8-1-8-1 layout, disabled/gap positions are still present in the register window.
B+18	<code>T_Cell[0]</code> , <code>T_Cell[1]</code>	<code>int8</code> ×2 packed	Module temperatures, °C.
B+19	<code>T_Cell[2]</code> , <code>T_Cell[3]</code>	<code>int8</code> ×2 packed	Module temperatures, °C.
B+20	<code>T_Cell[4]</code> , <code>T_Cell[5]</code>	<code>int8</code> ×2 packed	Module temperatures, °C.
B+21	<code>amps</code>	<code>int16</code>	Module current, 0.1 A.
B+22	<code>ampsFiltered</code>	<code>int16</code>	Filtered module current, 0.1 A.
B+23	<code>ampsRaw</code>	<code>uint16</code>	Raw current-sensor voltage, 0.1 mV.
B+24	<code>Vref</code>	<code>uint16</code>	LTC reference voltage, 0.1 mV.
B+25	<code>balancing[0..1]</code>	<code>uint8</code> ×2 packed	Balancing mask bits 0..15.
B+26	<code>balancing[2]</code> , <code>pecErrorCount</code>	<code>uint8</code> ×2 packed	Balancing mask bits 16..17 and per-module PEC error count.
B+27	<code>commFailCycles</code> , <code>dataStale</code>	<code>uint8</code> ×2 packed	Consecutive failed cell-read cycles and stale-data flag (1 = measurements too old to trust).
B+28	<code>cfg</code>	byte/packed	Low byte: bit 0 <code>hvon</code> , bit 1 <code>vent</code> ; high byte reserved.
B+29 .. B+49	invalid address gap	—	Not backed by <code>module_t</code> ; returns Illegal Data Address.

Legacy note: older 22.x firmware exposed a 12-cell module layout. The 30.x firmware widened the per-module cell voltage block to 18 cell positions, so integrations that assumed only 12 contiguous cell voltage registers must be updated.

Special registers

Reg	Behavior
5000	Read returns <code>FIRMWARE_REVISION</code> (0x1e08 = 30.08).
5001	Write 43690 (0xAAAA) to reboot, 28730 (0x703A) for factory config, or 7658 (0x1DEA) for Bluetooth-name change mode.
5002	Read returns <code>HARDWARE_REVISION</code> .
7777	<code>unlockCode</code> . Write 1234 (<code>MODBUS_SECRET_CODE</code>) to enable writes to 4079–4080.

Migration from the old global-data map

RAM optimization removed historical raw-AI, trip/debug and other fields. The operating-limit registers therefore moved:

Old address	30.08 address	Value
3051	3033	CCL

Old address	30.08 address	Value
3052	3034	DCL
3053	3035	CVL
3054	3036	Discharge voltage limit
3055	3037	Switch NTC
3056	3038	Dynamic minimum-cell limit

Addresses 3048 and above are not part of the 30.08 global-data section and return Illegal Data Address rather than exposing memory beyond DATALAYER.

Maintaining this page

Recalculate the byte offsets whenever `data_t`, `commands_t`, `config_t` or `module_t` changes. Do not rely on historical inline `//30xx` comments. See development conventions.

See also

- Firmware architecture — the structs behind the map.
- CAN bus — telemetry frames and register access over CAN.
- Safety, Current limiting — meaning of the flag and limit registers.