TÜVRheinland®
Precisely Right.

Automation - Functional Safety

Report on the evaluation of the Battery Management System from TD HiTech Energy Inc.

Report-No.: 968/FSP 1912.00/19
Date: 2019-07-12

**Report on the evaluation of the
Battery Management System from
TD HiTech Energy Inc.**

Report-No.:	968/FSP 1912.00/19
Date:	2019-07-12
Number of pages (excl. appendices):	11
Product / Project:	Battery Management System (BMS) MPSS-01 series BMS, including product types: HT1204DD, HT1205AC, HT1203AA, HT1204DA
Customer / Manufacturer:	TD HiTech Energy Inc. 6F, No. 21, Sui-Lih Road, HSINCHU CITY 30059, TAIWAN, R.O.C.
Customer-Order-No. / Date:	114081580 dated 2018-09-04
Certification Body:	TÜV Rheinland Industrie Service GmbH Automation - Functional Safety (A-FS) Am Grauen Stein 51105 Köln / Germany TÜV Rheinland (China) Ltd. Unit 707, AVIC Bldg.No.10B, Central Road East 3rd Ring Road, Chaoyang District Beijing 100022 P.R. China
TÜV-Offer-No. / Date:	12108435 dated 2018-08-31
TÜV-Order-No. / Date:	114081580 dated 2018-09-04
Assessor/Expert:	Yunxi Zhang (responsible for project) Elvis Wei
Duration:	September 2018 - July 2019

The results are exclusively related to the product/project.

This report must not be copied **in an abridged version** without the written permission of the Certification Body.

Contents **Page**

1. Scope

Within the scope of this assessment the MPSS-01 series Battery Management System (Types: HT1204DD, HT1205AC, HT1203AA and HT1204DA) from TD HiTech Energy Inc. shall be approved against the requirements for SIL 1 according to IEC 61508, SIL CL 1 according to IEC 62061, as well as requirements for Cat. 2 / PL c according to ISO 13849-1.

This test report contains the essential safety engineering aspects, that were assessed during the inspection and identifies the various test steps that were performed to provide evidence that the test object complies with the safety-relevant requirements of the product specification and the relevant standards.

2. Standards forming the basis for the requirements

[N1] **EN 15194:2017 (in extracts)**
Cycles - Electrically power assisted cycles - EPAC Bicycles

[N2] **ISO 13849-1:2015**
Safety of machinery - Safety-related parts of control systems
Parts 1: General principles for design

[N3] **IEC 62061:2015**
Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

[N4] **IEC 61508:2010, parts 1-7**
Functional safety of electrical/electronic/programmable electronic safety-related systems

3. Identification of the product / project under assessment

3.1. Description of the product / project

The MPSS-01 series Battery Management System (Tyeps: HT1204DD, HT1205AC, HT1203AA and HT1204DA) have the safety functions as following (see [D4]):

- Charge over-voltage protection
- Charge, pre-charge and discharge over-current protection
- Charge and discharge over-temperature protection
- Discharge under-voltage protection
- Short circuit protection

The safe state of the device is to switch-off all the charge and discharge MOSFETs and/or break the current fuse.

The MPSS-01 series Battery Management System (Tyeps: HT1204DD, HT1205AC, HT1203AA and HT1204DA) can only be used with the battery package which contains lithium-ion battery cell types INR18650-35E3 or ICR18650-26J from SAMSUNG SDI Co., Ltd.

Both the external battery package and charger are out of the scope of this assessment.

The MPSS-01 series Battery Management system consists of BMU control board and power board:

- BMU control board: It consists of wake up signal of MPSS-01 series Battery Management system, and a microcontroller which is responsible for the measurement of the battery cell voltage, temperature and charge/pre-charge/discharge current and also the non-safety related communication with external devices via CAN and SPI bus.
- Power board: It mainly consists of current-sense amplifier, MOSFETs and active current fuse. The MOSFETs can be switched on/off by the control signals from the BMU control board.

Below figure 1 shows the functional block diagram of MPSS-01 series Battery Management System (see [D4]).

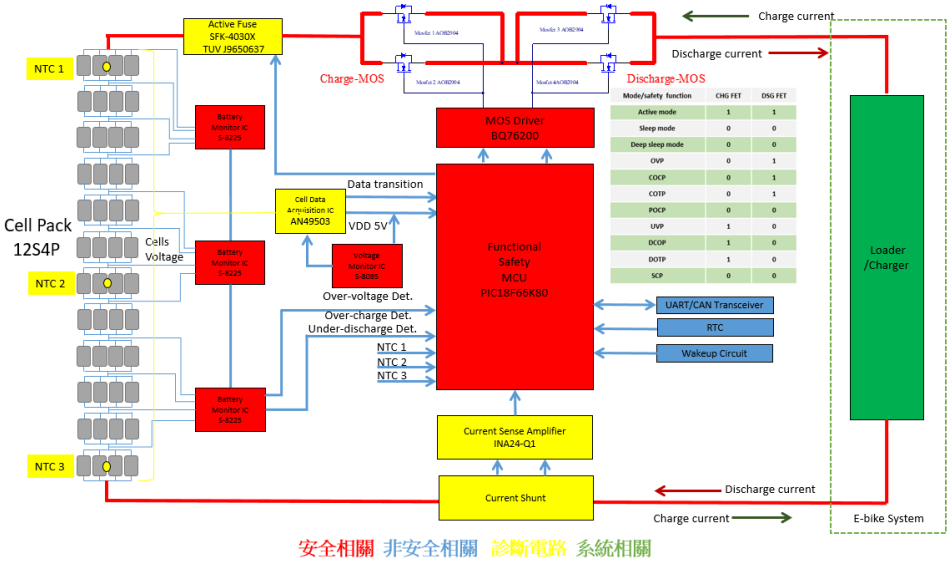

Figure 1: MPSS-01 series Battery Management System functional block diagram

The following MPSS-01 series Battery Management System product types and their revisions are covered by this assessment:

Product types	BMU control board		Power board	
	HW Rev.	SW Rev.	HW Rev.	SW Rev.
HT1204DD	V2	V0.1.9 (HT1204DD_V0.1.9_20190723.hex CRC16: 0xD155)	V2	-/-
HT1205AC	V2	V0.1.9 (HT1205AC_V0.1.9_20190723.hex CRC16: 0xDD71)	V2	-/-
HT1203AA	V2	V0.1.9 (HT1203AA_V0.1.9_20190723.hex CRC16: 0x4A41)	V2	-/-
HT1204DA	V2	V0.1.9 (HT1204DA_V0.1.9_20190723.hex CRC16: 0x5768)	V2	-/-

Table 1: Product type and revisions covered by the assessment

The MPSS-01 series Battery Management System (Types: HT1204DD, HT1205AC, HT1203AA and HT1204DA) adopts a Cat. 2 / 1oo1 and Cat. 3 / 1oo2 mixed safety architecture. The device is considered in general as type B subsystem according to 7.4.4.1.3, IEC61508-2. The device can work in high demand mode of operation.

3.2. Documents provided by the customer

The complete project documentation for design, development, testing and quality management as listed in [D1] were provided by the manufacturer.

Among other documents as detailed in [D1] the following superior documents have been taken into account during the assessment:

No.	Document	Rev.	Date
[D1]	Document list File: 001_DL_V1.0_2019-07-04.doc	1.0	2019-07-04

No.	Document	Rev.	Date
[D2]	Safety plan File: 002_Safety_Plan EE 2019-01-13.doc	1.0	2019-01-13
[D3]	Verification and validation plan File: 003_VVP_Plan_2019-01-13.doc	1.0	2019-01-13
[D4]	Safety requirements specifications and safety concept design File: 004_SRS-SC_MPSS-01_v10.0_2019-05-08.docx	10.0	2019-05-08
[D5]	FMEA reports of HT1203AA / HT1204DD / HT1204DA / HT1205AC File: 005_HT1203AA_FMEA_13849-20190628.xlsx 006_HT1204DD_FMEA_13849-20190628.xlsx 007_HT1204DA_FMEA_13849-20190628.xlsx 008_HT1205AC_FMEA_13849-20190628.xlsx	3.0	2019-06-28
[D6]	Circuit schematics File: 009_HT1203,HT1204,HT1205XX Schematic 0322.pdf	1.0	2019-03-22
[D7]	Software unit static analysis report File: 024_Static Analysis Report_20190610.docx	1.0	2019-06-10
[D8]	Software unit dynamic analysis report File: 025_Dynamic Analysis Report_20190610.docx	1.0	2019-06-10
[D9]	System integration and validation test results of HT1203AA / HT1204DD / HT1204DA / HT1205AC File: 017_HT1205AC EE test report 20190625.pdf 018_HT-190420-01 DQA-HT1203AA test report 20190420.doc 019_HT-190420-01 DQA-HT1204DA test report 20190421.doc 020_HT-190420-01 DQA-HT1204DD test report 20190419.doc 021_HT-190420-01 DQA-HT1205AC test report 20190421.doc 027_Test Report_UN38.3_Pack_HT1205AC_final.pdf	01 1.0 1.0 1.0 1.0 1.0	2019-04-30 2019-04-20 2019-04-21 2019-04-19 2019-04-21 2019-03-18
[D10]	Environmental test results of HT1203AA / HT1204DD / HT1204DA / HT1205AC File: 013_HT1203AA(Environmental related requirements)Test 20190509.doc 014_HT1204DA(Environmental related requirements)Test 20190509.doc 015_HT1204DD(Environmental related requirements)Test 20190509.doc 016_HT1205AC(Environmental related requirements)Test 20190509.doc	-/-	2019-05-09
[D11]	EMC test results File: 028_19-05-MAS-070-01(IEC 61326-3-1).pdf 029_19-05-MAS-070-02(EN15194).pdf 033_HT120X EMC test report.pdf	-/- -/- -/-	2019-06-20 2019-06-20 2019-05-02
[D12]	Requirement tracing matrix File: 011_Requirement tracing matrix_20190625.xlsx	1.0	2019-06-25

Table 2: Documents provided by the manufacturer

Besides the above listed documents, the manufacturer has provided the following user manuals:

No.	Document	Rev.	Date

No.	Document	Rev.	Date
[U1]	Safety manual File: 012_Safety manual_20190704.doc	4.0	2019-07-04

Table 3: User manual provided by the manufacturer

3.3. Documents compiled by TÜV Rheinland

The following table shows the main documents, complied by the Certification Body:

No.	Documents
[T1]	List of Open Points (LOP) File: 2019-07-09_LOP_Hitech.xlsx
[T2]	Fault-Insertion-Test report File: FIT report_TD Hitech_BMS_v1.4_2019-07-04.docx
[T3]	Evaluation plan File: EvaluationPlan_TD Hitech_BMS_2019-07-08.doc

Table 4: Documents prepared by TÜV Rheinland

Most of the test activities were based on the review of documents, which were provided by the manufacturer. In addition, practical tests have been performed by the Certification Body together with the design engineers during the fault insertion tests (see [T2] for details). The IDs of the used test samples are documented and can be found in the inspectors fault insertion test documents.

4. Test and test results

4.1. Evaluation procedure

The assessment activities were done according to an Evaluation Plan [T3] and mostly based on the review of documents which were provided by TD HiTech Energy Inc., as listed in [D1]. The following points have been assessed in accordance with [N1] - [N4]:

- Management of functional safety on project level / product level
- Documentation over the entire safety lifecycle
- Measures for fault avoidance (QM) over the entire safety lifecycle
- Safety structure
- Measure for detection and control faults in HW and SW
- Safety related parameters
- Embedded software
- Fault insertion tests and functional test
- Electrical safety
- Environmental (ENV) tests
- Electromagnetic compatibility (EMC) tests
- Inspection and review of the documentation for user

The following subchapters provide assessment results regarding the above listed topics.

4.2. Result of the assessment of individual objects

4.2.1. Assessment of management of functional safety

The assessment of Functional Safety Management of this MPSS-01 series Battery Management System project is mainly based on the review of documents Safety Plan and Verifivation & Validation Plan (see [D2] - [D3]) provided by customer. Open items have been discussed and clarfied together with the customer (see [T1]).

Result:

The Safety Plan and Verifivation & Validation Plan fulfill the requirements of [N3] - [N4].

4.2.2. Assessment of documentation over the entire safety lifecycle

The documentation plan, Safety Plan and Verfication & Validation Plan (see [D1] - [D3]) include the planned documentation over the entire safety life cycle. Open items have been discussed and clarfied together with the customer (see [T1]).

Result:

The assessment of the documentation of the MPSS-01 series Battery Management System project confirmed that the respective requirements of [N2] - [N4] are fulfilled.

4.2.3. Assessment of measures for fault avoidance (QM) over the entire safety lifecycle

The measures for fault avoidance of the MPSS-01 series Battery Management System project were part of the functional safety management assessment (see chapter 4.2.1 and 4.2.2). Open items have been discussed and clarified together with the customer (see [T1]).

Result:

The assessment has shown that the respective requirements of [N1] - [N4] are fulfilled.

4.2.4. Description and result of the inspection of the safety structure

The MPSS-01 series Battery Management System (types: HT1204DD, HT1205AC, HT1203AA and HT1204DA) adopts a Cat. 2 / 1oo1 and Cat. 3 / 1oo2 mixed safety structure:

- Battery cell voltage measurement subsystem adopts a Cat. 3 / 1oo2 safety structure, where each channel can respectively perform the battery cell over-voltage and under-voltage protection functions, and the measured battery cell voltage values are further compared within the CPU for diagnostic purpose.
- All other subsystems adopt a Cat. 2 / 1oo1 safety structure, where each function block e.g. power supply, CPU-core, CPU-RAM, CPU-ROM, temperature measurement circuitry, current measurement circuitry, etc., has continuously running diagnostic functions, which have at least a diagnostic coverage of DC > 60% (Low).

The inspection of the safety structure was performed essentially on documentation level. The major basis for the inspection was the safety requirement specification and the safety concept description (see [D4]). Besides this various other detailed documents were assessed as listed in [D1].

Result:

The assessment has shown that the respective requirements of [N2]- [N4] are fulfilled.

4.2.5. Assessment of the measures for detection and control of faults in HW and SW

The implemented measures to detect and control faults have been analyzed by the manufacturer and verified by the Certification Body, whether they are suitable and sufficient to detect faults, which have to be assumed according to table A.1 of [N4] part 2.

The used method was a Failure Mode and Effects Analyses (FMEA) on component level (see [D5] - [D6]), in order to show the completeness of diagnostics, which have been reviewed by the assessors (see [T1]).

These theoretical analysis (FMEA) have shown that any detected fault will lead to the safe state and the required diagnostic coverage for each single element is fulfilled.

Result:

It can be confirmed that the applied measures for detection and control of failures meet the requirements of [N1] - [N4].

4.2.6. Safety related parameters

The calculations of the safety relevant parameters were based on the resulting FMEA on component level (see [D5]) by the manufacturer, under considerations of the following assumptions:

- The components failure rates are based on values taken from manufacturers under a ambient temperature of 60℃.
- It is assumed that the failure rate of components remains constant over the period of use and the early phase of higher failure rates has been passed when system goes into operation.
- The failure modes of the components are taken from ISO 13849-2. For complex components a conservative distribution of 50 % safe and 50 % dangerous faults is used.
- All external elements such as external cabling were not considered within the failure rata calculation.
- Electronic devices used in non-safety related function are not included in failure rate calculation.

The following safety related parameters (see [D5]) were calculated by the manufacturer and has been reviewed by the assessors (see [T1]):

Safety architecture	Cat. 2 / 1oo1 and Cat. 3 / 1oo2 mixed
Hardware Fault Tolerance (HFT)	Cat. 2 / 1oo1 parts: HFT=0 Cat. 3 / 1oo2 parts: HFT=1
Hardware Safety Integrity Level (SIL)	SIL 1
Systematic Capability (SC)	SC 1
Performance Level (PL)	PL c
Device type	Type B
Safe Failure Fraction (SFF) of each element	Cat. 2 / 1oo1 parts: > 60% Cat. 3 / 1oo2 parts: > 0%
Safe failure rate λ_S	4.0E-06 (4000 FIT)
Detected dangerous failure rate λ_{DD}	4.0E-06 (4000 FIT)
Undetected dangerous failure rate λ_{DU}	4.13E-07 (413 FIT)
MTTFd	> 10 years
PFH	4.13E-07 (4.13% of SIL 1)

Table 5: Safety related parameters

Result:

The calculated safety related parameters fulfil the requirements for PL c and SIL 1.

4.2.7. Assessment of embedded software

The inspection of the embedded software is based on the measures for fault avoidance as specified for SC1 of [N4] part 2 and part 3. The following test steps were performed:

- Review of the manufacturer documentation (see chapter 4.2.2)
- Verification of measure for fault avoidance (see chapter 4.2.3)
- Analysis of the software design (see below)
- Inspection of the measures for fault control implemented in software (see chapter 4.2.5)
- Review of the performed software unit tests (see below)
- Review of the performed integration and validation tests (see below)

The inspection of the embedded software of the MPSS-01 series Battery Management System were mainly performed through reviews of the documentation provided by the manufacturer as listed in [D1]. Furthermore the requirement traceability document [D12] was also provided by manufacturer and reviewed by the assessors (see [T1]).

The software unit static- and dynamic tests (see [D7] - [D8]), and system integration and validation tests (see [D9]) were performed by the manufacturer. Partial verification of software design were performed on-site together with the manufacturer design and testing teams (see [T2]).

Result:

The results of the theoretical analysis of the software design as well as the performed tests showed that the software version specified in chapter 3.1 fulfill the requirements for SC1 as specified of [N4] part 2 and part 3.

Nevertheless it is recommended to improve the software off-line support tools qualification in a more systematic way. This weakness is accepted for the actual project.

4.2.8. Fault insertion tests and functional test

During the verification activities of the MPSS-01 series Battery Management System, the requirement specifications were not only checked in functional tests (positive tests) but also in negative tests (fault insertion tests).

The functional tests on the MPSS-01 series Battery Management System were carried out by the manufacturer, and the corresponding test results were documented in [D9], which have been reviewed by the assessors (see [T1]).

Particularly the implemented diagnostic measures have been verified through fault insertion tests. Some of these tests were carried out in co-operation with the assessors in the manufacturer's laboratories during the main approval (see [T2]).

Result:

The functional test results have been passed successfully and are accepted by the Certification Body.

The fault insertion tests confirmed the effectiveness of the realized measures to detect and control of faults. The respective requirements of [N1] - [N4] are fulfilled.

4.2.9. Electrical safety

The maximum charging voltage of the entire battery package must be less than 49.2 VDC as required in the safety manual [U1]. The MPSS-01 series Battery Management System has implemented corresponding control measures preventing it from spuriously entering charge or discharge mode (see [D4]). Furthermore the effectiveness of those implemented control measures have been verified during fault injection test (see [T2]). Therefore a safe insulation is ensured.

Result:

Respective electrical safety requirements are fulfilled.

4.2.10. Environmental (ENV) tests

The environmental tests were carried out based on the manufacturer specific test reuirements. All tests have been performed in the accredited test laboratory TD HiTech Energy Inc.. and The corresponding test results were documented in [D10], which has been reviewed by the assessors (see [T1]).

Result:

All tests have been passed and are accepted by the Certification Body based on the accreditation of the test lab TD HiTech Energy Inc..

4.2.11. Electromagnetic capability (EMC) tests

The EMC tests were carried out based on the requirements defined in standards EN 55014-1:2017, EN 55014-2:2015, EN 61000-3-2:2014, EN 61000-3-3:2013 and EN 15194:2017 for normal levels and IEC 61326-3-1:2017 for increased immunity levels. All tests have been performed in the accredited test laboratory Electronics Testing Center, Taiwan and Intertek Testing Services Taiwan Ltd.. The corresponding test results were documented in [D11], which has been reviewed by the assessors (see [T1]).

Result:

All tests have been passed and are accepted by the Certification Body based on the accreditation of the test labs Electronics Testing Center, Taiwan and Intertek Testing Services Taiwan Ltd..

4.2.12. Inspection and review of the documentation for the user

The safety manual (see [U1]) for the MPSS-01 series Battery Management System was provided by the manufacturer and have been reviewed by the assessors acc. to the applicable requirements of [N4] part 2 and part 3, Annex D. Open items have been discussed and clarified together with the manufacturer (see [T1]).

Result:

The safety manual covers all relevant aspects for a safe use of the product and is accepted by the Certification Body. All relevant information for identification and safe use is in its appropriate place.

5. Summary

The MPSS-01 series Battery Management System (Types: HT1204DD, HT1205AC, HT1203AA and HT1204DA), as specified in chapter 3.1, comply with the requirements of SIL 1 / SIL CL 1 according to IEC 61508 / IEC 62061 and Cat. 2 / PL c according to ISO 13849-1 and can be used in applications up to these safety levels.

The instructions of Safety Manual ([U1]) have to be considered before any usage in the safety related applications.

This assessment does not substitute the validation at application level.

Beijing, 2019-07-12
TIS/A-FS/Kst. 962 yz-nie

Report released after review:
Date: 2019-07-12

The assessors

M.-Eng. Yunxi Zhang	M.-Eng. Elvis Wei	Bin Zhao