



FMEA and HARA

SeaPower™

57-Ah Battery Documentation

1	SUMMARY OF DIAGNOSTIC COVERAGE	4
2	FAILURE MODES AND EFFECTS ANALYSIS (FMEA)	5
2.1	Scoring:	5
2.2	FMEA (Partial)	6
3	HAZARD ANALYSIS AND RISK ASSESSMENT (HARA)	7
4	TRACEABILITY MATRIX (FMEA TO HAZARD ANALYSIS)	8
5	FUNCTIONAL SAFETY GOALS AND INTEGRITY LEVELS	9
6	VALIDATION AND VERIFICATION STRATEGY	9
7	COMMON-MODE AND LATENT FAULT ASSESSMENT	9
8	DIAGNOSTIC DEGRADATION AND MAINTENANCE	9
9	RESIDUAL RISK AND ALARP JUSTIFICATION	10
9.1	Insulation Failure Without IMD	10
10	CONCLUSIONS	11
11	LEGAL NOTICES & CONTACT INFORMATION	12
11.1	Copyright and Trademarks	12
11.2	Disclaimer	12
11.3	Feedback / Support	12

Document Version History

Document Number: SeaPower-57Ah-D006

Version	Date	Author	Reviewer	Change
1.0	2025-08-02	P. Paranhos	C. Thiede	Initial Release

1 Summary of Diagnostic Coverage

Failure Mode	Detection Hardware	Firmware/Logic Diagnostic Path	Diag. Cove.	Failure Prob.	Commentary
Overcurrent	IVTS (BMS), SSR gate feedback, Hard Fuse	Current threshold checks, relay state crosscheck	≥97%	Medium to High	Fast response path with fallback; Hard fuse provides fail-safe
Overvoltage	Cell voltage sensors, Pack voltage sense	Multi-point voltage validation, charge control cutoff	≥98%	Medium	Monitors per-cell and total pack; OV fuse backup (~90%)
Overheating	Redundant thermal sensors (cell/SSR)	Sensor plausibility, thermal zone cross-verification	≥98%	Low to Medium	Redundant channels + active control; proven in FAT
Insulation Failure	None (no IMD used)	None (design-for-safety via potting/spacing only)	None	Low	Relies on potting and coating. Coating damage + conductive inserts pose undetected shock risk. Consider IMD in future revs.
SOC Fault / Drift	IVTS, Voltage Sensors	Coulomb count + voltage cross-estimation	≥97%	Medium	SOC validated by dual sensing; ±3% deviation flags fault
Short Circuit	IVTS + SSR feedback + fuse	Voltage drop profile; fast cutoff signature	~95%	Medium	Detected by current + voltage transient correlation
Communication Loss	RS485/USB/Watchdog	Heartbeat signal, fallback logic	≥90%	Low to Medium	Autonomous recovery logic tested in HAT
Relay Failure (SSRs)	SSR gate monitor, precharge circuit	Firmware precharge validation + current monitor	≥95%	Medium	Latent SSR issues revealed by state mismatch or timing faults
Fuse Failure	None (non-recoverable)	None — design assumes passive fail-safe	N/A	Very Low	Fuses are sized and verified via burn-in and spec qualification

2 Failure Modes and Effects Analysis (FMEA)

Note: Complete FMEA table covering cells, modules, BMS, and pack subsystems is attached in Appendix A. A summarized view of high and moderate risks is provided below:

2.1 Scoring:

Value	Severity (S):	Occurrence (O):	Detection (D):
1	No effect	Remote (<1 in 1M)	Always detected (automated)
4	Minor performance loss	Low (1 in 10k)	Likely detected by procedure
7	System degraded, unsafe	Moderate (1 in 100)	Low chance of detection
10	Catastrophic (injury/fire)	Frequent (>1 in 10)	Undetectable before failure

RPN Range	Risk Level	Color
1–100	Low	● Green
101–300	Moderate	● Yellow
301+	High	● Red

2.2 FMEA (Partial)

FMEA ID	Item	Failure Mode	Effect	S	O	D	RPN	Controls
FMEA-CELL-01	Cell	Internal short circuit	Thermal runaway, fire	10	2	2	40	Cell QA, cutoff, thermal sensors
FMEA-MOD-01	Cell Temp Sensor	Open/short	Overheat undetected	4	4	1	16	Redundant sensors, plausibility check
FMEA-MOD-02	Cell Voltage Sensor	Drift / calibration loss	Overvoltage	6	3	3	54	Voltage cross-check, fast cutoff
FMEA-MOD-03	Passive Balancing	Resistor open/short	Capacity loss, power loss	5	3	3	45	Unbalance detection in BMS
FMEA-BMS-01	Hard Fuse	No blow on overcurrent	Last line fails, damage	6	2	4	48	Verified spec, tested, backup by SSRs and BMS logic
FMEA-BMS-02	IVTS Sensor	Drift or comms failure	Incorrect thresholds	5	6	3	90	Crosschecked by firmware + redundant path
FMEA-BMS-03	Isolation Barrier	Breakdown, short circuit	HV barrier fault	6	2	3	36	Potting, PCB spacing, FAT inspection
FMEA-BMS-04	SSRs	Fail open or closed	No power or no isolation	7	4	2	56	Gate driver monitor, firmware fault detection
FMEA-BMS-06	RS485 Interface	Noise or break	Communication Fault	4	2	3	24	Auto-fallback mode, error-detection protocol
FMEA-PACK-01	Power Connector	Pin wear/damage (subsea)	High contact resistance/loss	6	3	3	54	Redundant pins, visual inspection, subsea-rated connector
FMEA-PACK-02	Frame Coating	Coating missing/damaged near insert	Shock hazard from conductive surface	7	3	3	63	Visual inspection, manufacturing QA, evaluate frame material change or coating redundancy

3 Hazard Analysis and Risk Assessment (HARA)

Hazard Type	S	O	Justification	Mitigation Measures	Initial Risk	Residual Risk
Overcurrent HAZ-OC-01	4	3	High fault current can cause fire	SSRs + BMS cutoff + hard fuse; precharge; 10ms shutdown	12	3
Overvoltage HAZ-OV-01	4	3	Charging fault can cause fire	Cell/pack sensing; charge control; fuse; BMS disconnect logic	12	3
Overheating HAZ-THERM-01	4	3	Sensor drift may mask faults	Thermal limits; redundant sensors; over-temp shutdown	12	3
Isolation Fault HAZ-ISO-01	4	2	HV exposure from barrier failure	Galvanic design; potting; spacing rules; FAT verification	8	4
SOC Monitoring HAZ-SOC-01	3	2	Bad estimate = cell overuse	Redundant SoC calculation via voltage + coulomb count; sanity check	6	3
Short Circuit HAZ-SC-01	4	2	Arc/fire due to wiring/component	Pattern detection in IVTS + SSR shutdown + fuse	8	2
Isolation Fault HAZ-IF-01	4	3	Combined failure of connector integrity and front plate coating at insert interface may expose live HV.	Non-conductive frame; isolation quality control.	12	2

4 Traceability Matrix (FMEA to Hazard Analysis)

FMEA ID	Component	Failure Mode	Hazard Category	Hazard ID	Mitigation Strategy
FMEA-BMS-01	Hard Fuse	Does not blow on overcurrent	Overcurrent	HAZ-OC-01	SSR + BMS cutoff, fuse verification, system fault test
FMEA-BMS-02	IVTS Sensor	Drift / offset / loss of comms	SOC Monitoring Fault	HAZ-SOC-01	IVTS + voltage sensors, ±3% accuracy, diagnostics
FMEA-BMS-03	Isolation Barrier	Breakdown, short circuit	Isolation Fault	HAZ-ISO-01	Potting, PCB spacing, FAT inspection
FMEA-BMS-04	SSRs	Fail open or closed	Overcurrent	HAZ-OC-02	Gate monitor, watchdog, BMS fault logic
FMEA-BMS-05	USB Interface	Loss of debug access	Data Loss	HAZ-COM-01	Pre-shipment test, firmware fallback
FMEA-BMS-06	RS485 Interface	Noise or break	Communication Fault	HAZ-COM-02	Auto-fallback mode, error-detection protocol
FMEA-MOD-01	Cell Temp Sensor	Open/short	Overheating	HAZ-THERM-01	Redundant sensors, thermal shutdown logic
FMEA-MOD-02	Cell Voltage Sensor	Drift / calibration loss	Overvoltage	HAZ-OV-01	Voltage cross-check, fast cutoff
FMEA-PACK-01	Power Connector	Pin wear, mechanical damage	Isolation	HAZ-ISO-02	Redundant pins, non-conductive frame coating and potting, subsea-qualified connector, FAT, visual inspection

5 Functional Safety Goals and Integrity Levels

Safety Goal	SIL Target	Risk Justification
Prevent thermal runaway	SIL 2	Catastrophic event mitigated < 10 ms
Avoid high-voltage exposure	SIL 1	Potting and isolation; no live IMD
Ensure correct SOC management	SIL 1	Redundant estimation, fault detection

6 Validation and Verification Strategy

- **FAT/HAT testing:** Confirm safety logic behavior under real conditions
- **HIL checks:** Fault injection to test detection, shutdown, and logging
- **Field trial logging:** Long-term data confirms false-positive and missed detection thresholds
- **Coverage metrics:** 100% of major failure modes in FMEA exercised under lab conditions

7 Common-Mode and Latent Fault Assessment

Common-mode risks such as SSR command failure or loss of all temperature sensors have been mitigated with:

- Start-up test
- Gate driver feedback and precharge test logic
- Minimum 2 independent thermal sensors per risk-critical area
- Mechanical fuse backup on overcurrent protection. Latent faults are periodically tested via system diagnostic routines and watchdog resets.

8 Diagnostic Degradation and Maintenance

- Fault counters and degraded mode thresholds are stored in EEPROM for traceability
- Remote debug tools via USB/RS485 allow firmware access without opening the housing
- Preventive maintenance guidance includes connector inspection, FAT review, and annual health check

9 Residual Risk and ALARP Justification

Kraken Robotics has implemented a comprehensive set of hardware, firmware, and process-based safety measures to mitigate all identified high-severity hazards. The core battery design uses:

- Redundant sensing and protection circuits
- Fast fault detection and shutdown (<10 ms)
- Robust mechanical insulation via potting and subsea-rated materials

Despite these controls, a few residual risks remain that do not have active diagnostic coverage. These include:

9.1 Insulation Failure

The current 57 Ah battery design does **not include an integrated Insulation Monitoring Device (IMD)**. Instead, insulation integrity is achieved through a combination of robust design features:

- **Full potting of all high-voltage components,**
- **High-resistivity silicone barriers** around pouch cells ($\geq 1 \times 10^{15} \Omega \cdot \text{cm}$, >5 mm thickness),
- **A non-conductive coating for the frame,** and
- **A subsea connector** with insulation resistance exceeding **200 M Ω** .

Under normal conditions, this configuration provides multiple layers of electrical isolation, exceeding the requirements of IEC 62619 for a 311 Vdc battery system. However, analysis has identified a **localized failure mode** at the **front plate**, where the connector is mounted.

If the **surface coating around metal inserts** becomes compromised—due to machining, wear, or poor QA—and is **combined with connector damage**, a **conductive leakage path** could develop at the interface. This fault would require **both** the dielectric barrier around the insert to be breached and the connector insulation to fail. All other potential isolation failures would require **damage to the potting**, which is highly unlikely under normal mechanical and environmental conditions.

System-level insulation monitoring via a **central IMD on the high-voltage bus** is recommended.

10 Conclusions

Kraken Robotics has applied a robust FMEA and hazard assessment framework to ensure that the SeaPower™ Subsea Battery System is:

- Designed with **fail-safe architecture**,
- Supported by **redundant sensors and protections**,
- Capable of detecting and mitigating **critical hazards** within milliseconds.

11 Legal Notices & Contact Information

11.1 Copyright and Trademarks

© Copyright Kraken Robotics Inc. All Rights Reserved.

Kraken Robotics (Kraken), Kraken Power, Kraken Robotik, the Kraken Robotics logo, AquaPix, KATFISH, ThunderFish, SeaVision, Tentacle, SeaPower, and *Seeing with Sound* are trademarks or registered trademarks of **Kraken Robotics Inc.** These trademarks may not be reproduced or used without the express written permission of Kraken Robotics Inc.

All other product and brand names are trademarks of their respective owners.

All elements of this document are protected by Canadian and international copyright laws. No part of this documentation may be reproduced or distributed without the express written permission of Kraken Robotics Inc.

11.2 Disclaimer

- Kraken must be consulted regarding the proper **integration, calibration, and configuration** of any Kraken-designed system.
- This document is intended as **supplementary information only**. Any modifications to system integration or configuration must be discussed with Kraken Robotics.
- Failure to operate the product in a **safe and responsible manner** may result in injury, property damage, or product failure.
- It is essential to **read all documentation** pertaining to the product and follow all safety instructions and warnings prior to setup or use.
- Information in this document is provided “**as is**.” Kraken will not be responsible for damages arising from typographical errors, misinterpretation of documentation, or deviations from intended usage.
- Kraken reserves the right to revise this document at any time without obligation to notify users.
- In no event shall Kraken Robotics, its employees, or authorized agents be liable for any direct or indirect damages or losses arising from the use of this documentation.

11.3 Feedback / Support

To suggest improvements or report errors, please contact: documentation@krakenrobotics.com

For technical assistance and customer support: CustomerSupport@krakenrobotics.com

 www.krakenrobotics.com