/

ENGINEERING **RESEARCH REPORT · Engineering research report**

Fail-Safe Design and Fault-Injection Verification for Power-Battery-Pack Handling Tooling

Public-source research, engineering derivation, and verification methods for assisted handling and custom tooling in the automotive industry

Document Number AUREK-RC-AR-039
Version V1.0
Release date 2026-07-13
Issuing unit Jiangsu Aurek Intelligent Technology Co., Ltd.

Research and Verification Methods · Not Product Certification or Evidence of Customer Acceptance

Report structure

> Research Boundary Standards, papers, and vendor data in the main text are used to support the methodological framework; example calculations contain assumptions. Project applications must be supplemented with real workpiece, tooling, action curves, risk assessments and original test evidence.

> Research boundary — Document type: methodology research and verification plan. This report has not performed fault injection on any specific battery-pack tool and does not provide a certificate of conformity. Example loads and response requirements shall be confirmed by the project risk assessment, tests with actual loads, and customer technical specifications.

00 Executive Summary

Power-battery packs have high mass, complex center-of-gravity distributions, and sensitive housings and sealing surfaces, and may present risks associated with high-voltage connections, cooling interfaces, and damaged cells. If handling tooling loses air or electrical power, fails to lock completely, receives invalid sensor signals, or releases inadvertently, the consequences can include not only a dropped workpiece but also housing deformation, damage to insulation or cooling systems, and subsequent safety hazards. GB 38031-2025 took effect on 2026-07-01 and specifies safety requirements for traction batteries used in electric vehicles [1]. The standard addresses battery-product safety and does not directly replace mechanical-safety design of handling tooling, but it demonstrates that battery packs require rigorous prevention of mechanical damage and abnormal energy events.

This study proposes a fail-safe architecture based on priority for geometric support, control of hazardous release, diagnosability of single faults, and safe controlled set-down under abnormal conditions. The tooling shall not rely primarily on friction or continuous pneumatic pressure to retain a heavy load. Priority shall be given to a clear mechanical load path, self-retaining locks after closure, an interlock that permits release only after support is confirmed, and diverse-signal diagnostics for pressure, position, locking, and load state. Safety-related control functions may be designed in accordance with ISO 13849-1:2023 and validated by analysis and testing in accordance with ISO 13849-2:2012 [2][3]; the required performance level is determined by the project-specific risk assessment.

Core conclusion

- Heavy battery packs shall use geometric support and mechanically self-retaining features as the primary load path; a single pneumatic-pressure, vacuum, or friction function shall not be the sole drop-prevention measure.
- "Failsafe" does not mean continuing production after all failures, but maintaining load after failure, stopping dangerous actions, prohibiting release, and entering a diagnosable recovery state.
- Fault injection must cover stuck sensors, signal shorts/opens, stuck valves, ruptured pipes, pressure drops, communications outages, recipe mismatches and false release commands.
- The testing should follow the progressive principles from low energy to high energy, alternative loads to real battery packs, and single faults to reasonable combinations of faults.
- Verification evidence must be traceable to safety requirements, fault assumptions, test steps, original signals, judgment and rectification closed loops.

01 Research Scope and Safety Objectives

The study covers purpose-built handling tooling for battery modules, lower housings, battery trays, and complete power-battery packs during assembly, inspection, rework, and line-side transfer. The carrier may be a Pneumatic Industrial Manipulator, lifting device, robot, or purpose-built machine. This report focuses on the tooling and control interface; it excludes cell electrochemical design, BMS algorithm certification, and transport regulations.

The safety objectives fall into four categories: protect personnel from dropped-load and crushing hazards; prevent handling damage to the battery-pack housing, sealing surfaces, or interfaces beyond product limits; prevent a single tooling fault from directly causing hazardous release; and provide defined steps for transferring the load to safe support during an abnormal condition. ISO 12100 requires hazard identification and risk reduction throughout the machinery life cycle [4], while ISO/TR 20218-1 provides safety guidance for the design and integration of robot end effectors [5].

Safety Function	Trigger condition	target response	Evidence that must be retained
Clamping/supporting confirmation	Before pickup	Lifting is prohibited without confirmation	Position, pressure/force, locked status
load holding	Loss of air supply, loss of electrical power, valve failure	No dangerous release, stop movement	Maintain time, displacement, structural state
support-confirmed release	workpiece is in position and the attitude is allowed	Only allowed to unlock/unclamp	Destination-support signal, position, and command record
mismatch suppression	Battery model/tooling/recipe is inconsistent	No clamping or lifting allowed	ID, recipe version, interlocking log
Exception recovery	Any safety related failure	Enter the controlled set-down or maintenance state	Recovery steps and authorization records

02 Bearer architecture and fail-safe principles

02.1 Priority for Geometric Support

The battery pack has a large mass and usually has a structural allowable zone and a no-touch zone at the bottom. Prioritize the use of supporting arms, fork supports, load-bearing holes/side beam positioning, or mechanical grab points confirmed by the product side to allow gravity to be transmitted through a clear structural path. The cylinder or motor is mainly used for closing, positioning and locking, and should not lose all load immediately after the energy disappears.

If clamping friction force transmission must be used, verifiable data on the minimum friction coefficient, contact material, surface condition and clamping force should be obtained, and the effect of clamping on the housing, cooling plate, sealing surface and coating should be evaluated. For heavy-duty safety functions, geometric support is often more robust than simply increasing the clamping force.

02.2 Load Cases and Example Calculations

$$F_{eq} = m \cdot (g + a_z) + F_{shock}$$
$$F_{design} = S_L \cdot F_{eq}$$

Assume a battery pack mass of 650 kg and a maximum upward acceleration of 0.25g, with no additional impact load. The equivalent vertical load is approximately 7.97 kN. With the example safety factor $S_L=2.0$, the design vertical load is approximately 15.9 kN; four ideal, uniformly loaded support points carry approximately 4.0 kN per point on average. The actual design must also account for center-of-gravity offset, unequal support stiffness, manufacturing tolerances, inclination, braking, and failure of one support point. This example is neither a project load rating nor a recommended safety factor.

For eccentric centers of gravity, each fulcrum reaction should be calculated through static equilibrium or finite elements. The total load cannot be simply distributed evenly. If the battery pack has different lengths, masses or accessory configurations, the "maximum single point reaction force" rather than the "maximum total mass" should be used as one of the fulcrum design inputs.

02.3 Locking and releasing

After closing, the locking mechanism shall provide a verifiable mechanical state. If drive energy is lost, it shall retain the load or at least prevent hazardous release. Release requires confirmation that the workpiece is supported, the tooling is at a permitted position, motion has stopped, the personnel zone is safe, and the operating command is valid. Any sensor conflict shall lead to a conservative state rather than substitution of a software default for actual feedback.

03 Pneumatic, electrical and control safety architecture

ISO 4414:2010 applies to pneumatic systems and components on machinery and addresses significant hazards associated with their intended use [6]. For battery-pack tooling, the pneumatic design shall address line rupture, fitting disconnection, valve-spool seizure, supply-pressure fluctuation, residual energy, and maintenance isolation. Air receivers or pressure-retention devices can only delay loss of capacity; they do not automatically constitute safe load holding.

Recommended diagnostic layers include source pressure; both actuator chambers or other critical-circuit pressures; lock position; gripper-jaw/support-arm position; workpiece presence; supported state; load/weight plausibility; and control-communication health. Signals should be physically diverse wherever practicable so that two nominally redundant signals do not actually depend on the same mechanical target or cable.

```
Lift_Enable = Load_Present ∧ Clamp_Closed ∧ Lock_Confirmed ∧ Pressure_OK ∧ Recipe_Match
    Release_Enable = Supported ∧ Safe_Position ∧ Motion_Stopped ∧ Operator_Command ∧
                                    Diagnostics_OK
```

Logical expressions only describe functional relationships and are not equivalent to meeting a certain performance level. The structure, diagnostic coverage, common cause failures, software and verification of safety-related control systems should be implemented according to project selection standards [2][3].

04 Hazard Analysis and FMEA

failure mode	local causes	potential consequences	design control	Verification method
Sudden loss of the main air supply	The main pipe is cut off and the joints fall off	Clamping force decreases and load slips	Mechanical support, self-retaining lock, check valve, and monitoring	Gas outage fault injection
Single branch rupture	Worn hoses and damaged joints	Single gripper jaw failure, uneven load	Zone isolation, support-point redundancy, and pressure monitoring	Open drain at designated location
The valve core is stuck in the release position	Contamination, mechanical failure	Inadvertent unclamping	Release isolation, biconditional permission, mechanical retention	Simulated valve stuck
The lock is not fully in place	Tolerances, foreign matter, misalignment	Disconnection while carrying the load	Independent locking feedback, geometric anti-off	Semi-locked state test
Sensor stuck open	Line short circuit, software freeze	Not clamped but allowed to lift	Complementary signals and timing/plausibility diagnostics	Signal is forced to 1
Sensor stuck closed	Open circuit, target deviation	Unable to release or misjudgment of fault	Open-circuit diagnostics and maintenance state	Signal is forced to 0
Model recipe error	Barcode-reading, network, or operator error	Wrong stress point and interference	Mechanical error-proofing, ID consistency, version control	mismatch injection
Inadvertent release command	Human-machine interface or program error	Dropped suspended load	Support-confirmation interlock, restricted position, dual action	Issue release command while hanging in the air

failure mode	local causes	potential consequences	design control	Verification method
Communication interruption	Bus failure, PLC restart	Status unknown	Keep load, stop movement, prohibit release	Disconnect/restart injection
Abnormal load	Double bags, foreign objects, abnormal center of gravity	Overloading of structure or lifting gear	Reasonable weight, pick-up position to prevent double pick-up	Surrogate-load testing

FMEA shall be used together with a fault tree or safety-requirements matrix. For the load-drop top event, identify minimal cut sets such as “no geometric support + lock failure + erroneous release command” or “common-cause sensor failure + no software diagnosis.” If any single fault can trigger the top event, modify the structure first rather than merely lowering the occurrence rating.

05 Fault injection verification strategy

ISO 13849-2:2012 specifies procedures and conditions for verification of safety functions, implementation categories and performance levels through analysis and testing [3]. Fault injection is part of verification and is not a substitute for complete design review, component data, calculations, and software verification. A risk assessment, test area isolation, alternative load design, emergency support and recovery plans must be completed prior to testing.

05.1 Grading order

1. Model and Logic Level: Force inputs, acknowledge state machines and alarms in control simulation or offline logic.
2. Low Energy Bench Level: Use empty tooling or lightweight dummies to inject wire breaks, short circuits, valve and pressure failures.
3. Rated surrogate-load level: use a non-battery load with equivalent geometry and mass to verify retention, displacement, and structure.
4. Real battery pack level: Only interface and product protection items that cannot be covered by the first three levels are tested. The risks are controlled and authorized.
5. Field integration level: Confirm interlocking with manipulators, lifting devices, conveyor lines, tooling and safety systems.

05.2 Fault injection matrix

No.	Inject fault	inject moment	expected system state	key record

No.	Inject fault	inject moment	expected system state	key record
FI-01	Shut off the main air supply	Resting after lifting/moving	Keep the load, stop dangerous movements, and prohibit release	Pressure, displacement, stop time
FI-02	Rapid leakage in a single branch	The most unfavorable posture	Isolate the fault, issue an alarm, and maintain a condition that permits controlled set-down	Zone pressure, fulcrum reaction force
FI-03	Lock-position feedback stuck open	before closing	Lifting is not permitted	Input/output and alarm log
FI-04	Lock-position feedback stuck closed	half locked state	Plausibility diagnostic is triggered; lifting is not permitted	Position, pressure, signal contradictions
FI-05	Release-valve command stuck active	floating state	Physical or control layers prevent hazardous releases	Valve current, pressure, lock status
FI-06	False support-confirmation signal	Not in place	Double/diversity check rejects release	Support, position, load changes
FI-07	Controller restart/bus lost	In transit	The output enters the defined safe state and the load remains	Restart time, output status
FI-08	Incorrect battery model / recipe	Before pickup	The recipe is inconsistent and the action is prohibited	ID, recipe version, CRC/signature
FI-09	emergency stop	maximum reasonable speed	Stop without releasing the load	Peak acceleration, structure/load displacement
FI-10	Maintenance release misoperation	unsupported	Subject to permissions and mechanical conditions	Permissions, steps, lock status

Each test case shall define three outcomes: pass, fail, and engineering review required. Do not record only whether the load ultimately dropped; also check peak displacement, changes in lock state, alarm visibility, whether recovery requires bypassing a safety function, and whether the battery pack sustained hidden damage.

06 Acceptance indicators and evidence chain

Project metrics shall be derived from the risk assessment and technical agreement. Common categories include rated and worst-case loads, reaction at a single support point, permitted housing deformation, holding time, maximum slip, stopping acceleration, fault-detection time, alarm and reset, release permission, and maintenance isolation. This report gives no universal values for these metrics because battery packs, carriers, and personnel exposure conditions differ substantially.

evidence layer	Typical documents	Quality requirements
demand	Safety Requirements Specification, customer interfaces, product prohibited/restricted zones	Unique number, version and source
analysis	Load calculation, finite element, FMEA/FTA, PL evaluation	Assumptions are explicit and worst-case operating conditions are traceable
design	Drawings, BOM, pneumatic circuit/electrical diagram, software version	Consistent with analysis and reality
Verification	Test plan, original curves, photos, logs	Inject faults, time bases and criteria complete
Release Approval	Deviation list, rectification closed loop, signature and maintenance requirements	Unclosed issues have clear restrictions

The test signals should use a unified time base to allow analysis of cause and effect relationships between commands, valve actions, pressure changes, locking displacements and carrier stops. Simply saving an HMI screenshot is not sufficient to support fault response verification.

07 Safe Recovery, Maintenance, and Change Management

Abnormal recovery shall be defined during design. Typical steps include stopping the carrier, confirming load retention, establishing temporary support, isolating energy, clearing the fault, reconfirming lock engagement, low-speed set-down, and reset approval. Personnel shall not stand beneath the battery pack or rely on continuous manual support. If a mechanical lock must be released manually, the action shall be controlled by tooling, authorization, and confirmed support conditions.

Maintenance items include latch wear, arm deformation, fasteners, hose wear, valve contamination, sensor targets, cable kinks, contact pad material and calibration status. Any changes in battery pack mass, center of gravity, shell structure, allowed support points, tooling module, software recipe or carrier acceleration should trigger impact analysis and necessary revalidation.

08 Conclusion and applicable limitations

Fail-safe design of power-battery-pack handling tooling shall begin with the structural load path; pneumatic, electrical, and control systems then provide state confirmation, fault diagnostics, and controlled release. The safety objective is not to maintain cycle time after a fault, but to prevent hazardous release and bring the system to a safely recoverable state. Fault-injection verification shall correspond to the requirements, FMEA/FTA, control logic, and actual structure, forming an auditable evidence chain.

This report is an engineering research and verification plan. It is not evidence of product conformity to GB 38031, ISO 13849 performance-level certification, third-party inspection, or customer acceptance. Competent professionals shall design and approve each project in accordance with applicable regulations, standards, customer specifications, and actual risks.

References

1. GB 38031-2025 Safety requirements for power batteries for electric vehicles. https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=3AB693FAFF5D9716DF61C61D6FD2187A
2. ISO 13849-1:2023. Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design. https://www.iso.org/standard/73481.html
3. ISO 13849-2:2012. Safety of machinery - Safety-related parts of control systems - Part 2: Validation. https://www.iso.org/standard/53640.html
4. ISO 12100:2010. Safety of machinery - General principles for design - Risk assessment and risk reduction. https://www.iso.org/standard/51528.html
5. ISO/TR 20218-1:2018. Robotics - Safety design for industrial robot systems - Part 1: End-effectors. https://www.iso.org/standard/69488.html
6. ISO 4414:2010. Pneumatic fluid power - General rules and safety requirements for systems and their components. https://www.iso.org/standard/44790.html
7. ISO/TR 14121-2:2012. Safety of machinery - Risk assessment - Part 2: Practical guidance and examples of methods. https://www.iso.org/standard/57180.html
8. U.S. Department of Transportation / NHTSA. Safety Management of Automotive Rechargeable Energy Storage Systems. https://rosap.ntl.bts.gov/view/dot/38221/dot_38221_DS1.pdf
9. Held, M.; Bronnimann, R. Safe cell, safe battery? Battery fire investigation using FMEA, FTA and practical experiments. Microelectronics Reliability 64, 2016. https://doi.org/10.1016/j.microrel.2016.07.051