Inadvertent-Release Prevention for Custom Material-Handling Tooling and Methods for Confirming Load Seating

—Engineering Implementation Based on a Load State Machine and Multiple Safety Interlocks

Tooling safety is not only about holding the load; the tooling must also be prevented from releasing at the wrong time.

Published by Jiangsu AUREK Intelligent Technology Co., Ltd. · Engineering Research Center
Document Category Corporate Engineering Research White Paper
Version V1.1 (Optimized Release)
Published 2026/6

Release-state control: release is executed only in S6; all other states block the release path

S0 | S1 | S2 | S3 | S4 | S5 | S6 · Release Permitted | S7 · Complete

S8 · Abnormal-State Lockout
Any abnormality detected in any state causes a transition to this state; release is prohibited

Release Notice

This white paper addresses engineering design, design review, and acceptance validation for custom material-handling tooling. The thresholds and example parameters illustrate the method and do not constitute a universal performance commitment for every project or operating condition. Actual projects must be confirmed from the workpiece, operating conditions, risk assessment, and validation records accordingly.

Abstract

In a custom automated material-handling system, tooling performs critical workpiece gripping, lifting, transfer, positioning, and release functions. Tooling safety depends not only on holding the workpiece when required, but also on preventing release before safe conditions are met. When a workpiece is suspended, not stably seated, has not transferred its load, the operator presses a button unintentionally, or a pneumatic/vacuum condition is abnormal, unintended release can directly cause the load to fall or damage the equipment.

This white paper develops a load-state model for inadvertent-release prevention in custom material-handling tooling and proposes release-permission logic based on height confirmation, position confirmation, support-contact confirmation, and load-transfer confirmation. It combines this logic with pneumatic interlocks, vacuum retention, loss-of-air protection, two-button release, press-and-hold confirmation, abnormal-state lockout, and multisensor fusion to create an engineering control method in which release is blocked in every non-permitted state.

It also provides formula-variable definitions, design considerations for different tooling types, an FMEA risk analysis, test methods, acceptance items, and an engineering design checklist. Thresholds, test counts, and acceptance criteria must be established from project risk assessment and measured validation; the examples in this white paper illustrate the method and do not replace a project-level safety assessment.

Keywords

custom tooling; inadvertent-release prevention; load-seating confirmation; load transfer; pneumatic interlock; vacuum retention; loss-of-air protection; state machine; FMEA.

1. Introduction

1.1 Research Background

Custom material-handling tooling is widely used for machine loading/unloading, automotive-parts handling, battery-module transfer, sheet-metal handling, and heavy-load logistics applications. Unlike standard tooling, it is normally customized for workpiece geometry, mass, surface condition, handling cycle time, and equipment boundary conditions, so its structure, sensor configuration, and control logic vary substantially.

In engineering practice, tooling safety is often reduced to whether gripping, vacuum holding, or magnetic force is sufficient. The release phase is equally high-risk: if the load remains suspended, or if it contacts a support surface but load transfer is incomplete, release can turn a held workpiece into an unsupported workpiece. Confirmation of release conditions must therefore be a central part of tooling safety design.

1.2 Being Able to Hold the Load Does Not Mean the System Is Safe

Tooling safety comprises two independent requirements: first, the tooling must hold when required; second, it must not release unless safe release conditions are met. The first concerns gripping and holding capacity; the second concerns release permission and state control. Failure of either can cause loss of load control.

Key Point

Tooling safety requires more than holding the load: the tooling must be prevented from releasing at the wrong time. Release must be designed

as a safety action governed jointly by a state machine, sensor confirmation, a safety chain, and hardware interlocks—not as an ordinary action triggered by a single button

or software bit.

1.3 Scope and Boundaries

This white paper addresses inadvertent-release prevention and load-seating confirmation for custom material-handling tooling, focusing on mechanical grippers, vacuum tooling, electro-permanent-magnet tooling, and combinations of these types. It does not replace project safety assessment, equipment risk assessment, functional-safety calculation, or third-party certification. In a specific project, validation must account for workpiece-failure consequences, handling motions, personnel-accessible areas, control-system architecture, and applicable standards.

2. Inadvertent-Release Risk Definition and Control Objectives

2.1 Definition of Inadvertent Release

In this white paper, inadvertent release means any unclamping, depressurization, vacuum break, demagnetization, blow-off release, or other action that occurs before safe release conditions are met and reduces holding force. It differs from a failure to grip: a gripping failure means the load cannot be acquired; inadvertent release means the load is released when it should remain held.

The control objectives are: no release while suspended, no release before stable seating, and no release in an abnormal state. To achieve these objectives, the system must simultaneously confirm load state, release permission, operator intent, and safety-chain status.

2.2 Inadvertent-Release Risk Categories

Table 2-1. Inadvertent-Release Risk Categories and Principal Controls

No.	Risk Type	Typical Condition	Principal Controls
R1	**Release While Suspended**	**The load remains suspended and the release valve or unclamping mechanism receives a release request**	State-machine blocking, seating/transfer confirmation, pneumatic or electrical release interlock
R2	**Release Before Stable Seating**	The load contacts a support surface, but support is insufficient or its weight has not yet transferred	Contact-force confirmation, load-transfer confirmation, and stabilization-time criterion
R3	**Unintentional Release**	**Single-button mispress, HMI error, or maintenance error**	**Two-button control, press-and-hold confirmation, access control, and operation log**
R4	**Unclamping After Loss of Air**	**Air supply interrupted or pressure below threshold, reducing gripping force**	**Normally closed/self-locking mechanism, check valve, pressure-holding valve, air receiver, and pressure switch**
R5	**Vacuum-Loss Release**	Vacuum leakage, suction-cup failure, or interruption of the air supply causes the vacuum level to decrease	Vacuum reservoir, vacuum switch, check valve, independent circuit, and pressure-loss lockout
R6	**Sensor Mis-classification**	Height, position, contact, or load sensors are contaminated or drifting, or affected by impact	Multisource fusion, 2oo3 voting, self-diagnostics, and abnormal-state lockout

2.3 Top-Event Logic

Using unexpected loss of load support as top event T, the principal causal paths can be expressed as follows:

$$T = E_{air} \vee E_{unstable} \vee E_{pressure} \vee E_{control}$$

where Eair is release while suspended, Eunstable is release before stable seating, and Epressure is a reduction in holding force caused by abnormal pneumatic pressure or vacuum conditions. Econtrol is a control malfunction or human error. This formula illustrates the risk analysis; an actual project must further decompose it into specific components, signals, and operating modes.

Because the top event normally has an OR-gate relationship, any critical failure path can cause a hazardous outcome, so safeguards cannot rely on one measure. A sound engineering approach combines state constraints, sensor confirmation, hardware interlocks, and fail-safe protection.

3. Load-State Model

3.1 Need for a State Model

Inadvertent release often occurs when the control system does not accurately distinguish load states. If the release valve responds only to a pressed button or a true release bit and does not confirm seating, stability, or completed load transfer, release can occur at any stage. The load-state model constrains release to a controlled action that can execute only in a permitted release state.

3.2 State Definitions

Table 3-1. Load-State Definitions and Release Constraints

State	Name	Meaning	Release Constraint
S0	Unloaded	Tooling is not holding a workpiece	No load-release action; unintended operation must still be prevented
S1	Grip Confirmed	Tooling is gripping/vacuum-holding/magnetically holding the workpiece but has not lifted it	Release prohibited except during a controlled pickup/placement or maintenance procedure
S2	Lift	Workpiece leaves the pickup surface and begins lifting	Release prohibited
S3	Transfer	Workpiece moves with the tooling in a suspended or tooling-held state	Release prohibited
S4	Approach to Seating	Workpiece descends near the target support area	Release prohibited
S5	Load Transfer	Workpiece contacts the support surface and its load transfers from the tooling to that surface	Release prohibited until transfer is complete and stable
S6	Release Permitted	Seating, support, load transfer, and safety-chain conditions are all satisfied	Only normal state in which release is permitted
S7	Release Complete	Tooling has released the workpiece and the support structure carries the load	Release is complete; proceed to the exit or reset sequence
S8	Abnormal-State Lockout	Pressure loss, abnormal vacuum, inconsistent sensors, emergency stop, or logic fault detected	Release prohibited; reset only after holding the load or completing a controlled safe response reset

3.3 State-Transition Principles

$$State(t+1) = f\ (\ State(t), Sensor(t), Logic(t), Safety(t)\ )$$

where State(t) is the current state, Sensor(t) is the sensor-signal set, Logic(t) is the state-machine and release-permission logic, and Safety(t) is the safety-chain signal set, including emergency stop, safety gate, safety PLC, or safety relay.

Normal operation proceeds S0→S1→S2→S3→S4→S5→S6→S7. If any state detects abnormal pressure or vacuum, sensor conflict, communication fault, emergency stop, or an open safety chain, the system must transition to S8 abnormal-state lockout. State advancement requires sufficient sensor evidence; if the evidence is insufficient, remain in the current state or transition to a safe state.

4. Release-Permission Logic and Control Architecture

4.1 Multicondition AND Logic

Safe release is based on multicondition AND logic: height, position, contact, load transfer, operator request, safety-chain status, and absence of faults must all be satisfied. No single sensor, button, or software variable may independently trigger release.

4.2 Four-Factor Release Permission

$$R = H_s \wedge L_s \wedge P_s \wedge O_s$$

where R is release permission; Hs is height confirmation; Ls is horizontal-position/orientation confirmation; Ps is support-contact confirmation; and Os is load-transfer confirmation. Release permission is established only when all four conditions are true.

This criterion emphasizes that none of the conditions is interchangeable: height confirmation cannot replace load-transfer confirmation, position confirmation cannot replace support contact, and an operator request cannot replace safety confirmation.

4.3 Final Release-Command Synthesis

$$\text{Release} = \text{Operator\_Request} \wedge R \wedge \text{Safety\_OK} \wedge \text{No\_Fault}$$

where Operator_Request is the release request after inadvertent-operation safeguards have been applied; Safety_OK indicates that the safety chain is valid; and No_Fault means that no abnormal-state lockout, sensor fault, insufficient pressure, insufficient vacuum, unauthorized maintenance bypass, or similar condition is present.

In an engineering implementation, Release should not directly drive the release valve. Instead, it should indirectly enable the valve through a safety output, pilot permission, or hardware-interlock chain. This arrangement makes it difficult for a single logic fault in a supervisory controller or standard PLC to bypass the hardware-level release constraints.

4.4 Dual Channels and Diversity

$$R = R_{sensor} \wedge R_{logic}$$

where Rsensor is the decision from the physical sensing channel and Rlogic is the decision from the state-machine and control-logic channel. To the greatest extent practicable, the two channels should use different physical principles to reduce the risk of common-cause failure.

For example, the sensing channel may comprise a height sensor, support-side weighing modules, and a pressure/vacuum switch; the logic channel may comprise the state machine, action sequence, time windows, and safety-chain status. If the two channels disagree, the system must inhibit release and provide diagnostic information.

4.5 Separation of Software and Hardware Responsibilities

Software is suited to state-machine execution, signal fusion, diagnostics, and logging; hardware interlocks are suited to providing the last line of defense so that release remains impossible even if software issues an erroneous release request. The release action should be divided into four stages—software permission, hardware enable, valve actuation, and actuation-feedback confirmation—with diagnostic coverage provided for each stage.

5 Load-Seating and Load-Transfer Confirmation

5.1 Height Confirmation

$$\Delta H = | H - H_{set} | \leqslant E_H$$

where H is the measured height, Hset the seating-height setpoint, ΔH the height deviation, and EH the allowable height error. EH may be established from positioning accuracy, support-structure characteristics, and sensor repeatability; it should not be treated as a universal fixed value.

Height confirmation establishes only that the load is near the target height; by itself, it does not prove that the support surface is carrying the load.

5.2 Position and Orientation Confirmation

$$| X - X_0 | \leqslant E_X \quad , \quad | Y - Y_0 | \leqslant E_Y \quad , \quad | \theta - \theta_0 | \leqslant E_\theta$$

where X, Y, and θ are the measured horizontal position and orientation angle; X0, Y0, and θ0 are the target position and orientation; and EX, EY, and Eθ are the allowable errors. Where necessary, the Z-axis position, positioning-pin engagement, or pallet-bay status should also be confirmed.

Position confirmation ensures that the load is within the effective support area, avoiding partial overhang, eccentric loading, or overturning even though the load has made contact.

5.3 Support-Contact Confirmation

$$F_c \geqslant F_{min}$$

where Fc is the contact force or valid contact signal detected on the support side, and Fmin is the minimum valid contact threshold. Fmin must exceed sensor noise, vibration, dynamic disturbance, and no-load drift and must be established through unloaded and loaded tests.

5.4 Load-Transfer Confirmation (Core Criterion)

The essence of seating confirmation is not whether the height is low enough, but whether the workpiece weight has transferred to the support structure. Load-transfer confirmation directly supports the safety objective that release will not cause a fall.

$$W = m\,(g + a_z)$$

$$W = F_g + F_s$$

Os = 1 when Fs / W ≥ η for a duration ≥ τ

where W is the design load, m is the workpiece mass, g is gravitational acceleration, and az is the vertical design acceleration to be considered during seating or handling (for static cal- culations, az may be taken as 0; dynamic load must be included where impact, rapid descent, or emergency stopping occurs); Fg is the load still carried by the tooling, and Fs is the load carried by the support surface. As the load settles, Fs increases and Fg decreases. Os is the load-transfer confirmation result; η is the load-transfer-ratio threshold (0.85–0.95 is often used as an engineering starting point and must be validated); and τ is the stability-confirmation time used to filter transient impact or vibration.

For long workpieces or those with multiple support points, total support force alone may be insufficient. Load distribution across the support points and overturning risk must also be checked. For example, conditions such as “Fsi ≥ Fsi,min at every critical support point” and “support moments |Mx| and |My| do not exceed their limits” may be added.

5.5 Multisource Fusion and Confidence

Load transfer may be corroborated by support-side weighing modules, tooling-side pressure/force sensors, changes in lift-axis current, changes in suction-cup vacuum, or contact switches used in combination. Critical decisions should include at least two types of sensing based on different physical principles.

$$\text{Vote} = 2\text{oo}3$$

$$C = \Sigma\,(w_i \cdot S_i) \quad , \quad \Sigma\, w_i = 1 \quad , \quad C \geqslant C_{th}$$

Here, 2oo3 means two-out-of-three voting: a conclusion is accepted only when at least two of three independent decision signals confirm it. This can tolerate one intermittent sensor failure, but does not replace sensor diagnostics or project risk assessment. Si is the normalized result of sensor or decision channel i; wi is its weight; C is the combined confidence; and Cth is the confidence threshold. The weights and threshold must be established by testing, and their basis documented.

5.6 Combined Seating Criterion

$$\text{Placement\_OK} = \text{Height\_OK} \wedge \text{Position\_OK} \wedge \text{Contact\_OK} \wedge \text{Transfer\_OK}$$

This expression requires height, position, contact, and load transfer all to be satisfied. Transfer_OK is an indispensable condition; if transfer evidence is insufficient, release must be denied rather than compensated for by height confirmation or a button request.

6 Pneumatic, Vacuum, and Failure-Protection Design

6.1 Interlock Layers

Inadvertent-release prevention should use defense in depth across three layers: mechanical, electrical/safety-control, and pneumatic/vacuum circuits. The mechanical layer provides self-locking or travel limitation; the electrical layer provides state determination and safety outputs; and the pneumatic/vacuum layer blocks unauthorized release actions in the actuation circuit.

6.2 Pneumatic Release Interlock

$$R \land Safety\_OK \land No\_Fault \rightarrow Pilot\_Enable \rightarrow Release\_Valve\_Enable$$

> This logic means that the release-valve pilot or enable circuit may actuate only when complete release permission is present, the safety chain is valid, and no fault exists. The interlock conditions must not be reduced to Position_OK, because position confirmation does not establish that the load has transferred.

A valve-manifold design that maintains clamping or blocks release after loss of electrical power or air is recommended. If standard PLC and safety outputs coexist, the release valve's energy path should be controlled by a safety output or safety relay; the standard output should serve only as an operator request or action command.

6.3 Loss-of-Air Protection and Pressure Retention

The purpose of loss-of-air protection is not to allow normal handling to continue, but to keep the load under control when the air supply is abnormal and place the system into a safe shutdown, controlled-descent, or abnormal-state-lockout sequence.

- ◇ Grippers should use a normally closed, self-locking, or mechanically wedged structure so that loss of air or power does not actively release the load.
- ◇ Install a check valve, pressure-holding valve, or locking valve on the clamping or vacuum chamber to reduce the rate of abnormal pressure loss.
- ◇ Where necessary, provide an air receiver or energy-storage unit, with clearly defined holding time, minimum pressure, and response strategy.
- ◇ The pressure switch should be an independent hardware input to the release-inhibit chain. If pressure falls below the threshold, release must be inhibited and an alarm generated.
- ◇ Pressure-retention capability must be validated through leakage, holding-time, and minimum-gripping-force tests; the mere presence of a valve does not establish that the safety requirement is met.

6.4 Vacuum Retention and Vacuum-Release Control

Vacuum tooling must address two risks: insufficient vacuum reducing holding force, and vacuum break or blow-off release being executed before the seating conditions are met. Vacuum-break, blow-off, and exhaust-valve actuation must, like mechanical unclamping, be governed by S6 release permission.

- ◇ Provide a vacuum switch or sensor to monitor whether the vacuum level meets the gripping-permission and handling-retention thresholds.
- ◇ Use a vacuum reservoir, check valves, and segmented circuits to reduce the effect of a single-point leak on all suction cups.

- ◇ Leak testing should cover static retention, handling acceleration, suction-cup aging, and variation in workpiece surface condition.
- ◇ The vacuum-break/blow-off release valve must be governed by Release permission. Unauthorized bypass in maintenance or commissioning mode is prohibited.
- ◇ Vacuum holding time, vacuum-decay rate, and alarm thresholds must be established for the project. If a criterion such as “no more than a 10% drop within 30 s” is used, it must be supported by test records.

6.5 Abnormal-State Lockout and Reset

Abnormal-state lockout S8 must include action inhibition, alarms, state logging, and controlled reset. Reset must not directly restore release capability; it must re- establish state confirmation, pressure/vacuum confirmation, sensor-consistency confirmation, and operator authorization.

7 Inadvertent-Release Prevention for Different Tooling Types

7.1 Mechanical-Gripper Tooling

Mechanical grippers retain a workpiece primarily through form fit, clamping force, and friction. For vertical handling that relies on frictional retention, gripping force may be checked using the following expression:

$$n \cdot \mu \cdot F_N \geqslant K \cdot m\,(g + a_z)$$

where n is the number of effective friction-contact surfaces, μ is the coefficient of friction under the worst-case condition, FN is the normal clamping force at each contact surface, and K is the safety factor; m, g, and az have the meanings defined above. If horizontal acceleration, eccentric loading, or impact is present, resistance to slipping and overturning must also be checked separately.

Key inadvertent-release-prevention measures include a normally closed/self-locking structure, closed-position and opening feedback, clamping-pressure monitoring, retention after loss of air, a release-valve interlock, and inhibition of unclamping in an abnormal state. For form-fit tooling, confirm insertion depth, positioning-pin engagement, and locking-element engagement—not merely that the cylinder has reached its end position.

7.2 Vacuum Tooling

$$F_{vac} = \Delta P \cdot A_{eff} \cdot \lambda$$

$$S = F_{available} / F_{required} \geqslant S_{min}$$

where Fvac is the available vacuum holding force, ΔP the vacuum pressure differential, Aeff the effective vacuum area, and λ a correction factor accounting for suction-cup compression, surface roughness, leakage, and orientation; S is the vacuum-holding safety margin; Favailable is the available holding force at the worst-case vacuum level and effective area; Frequired is the required force accounting for workpiece weight, acceleration, orientation, and disturbance; and Smin is established by the project risk assessment.

Key inadvertent-release-prevention measures include permitting lifting only after vacuum reaches the threshold, continuously monitoring the vacuum level during handling, and initiating a hold/alarm/safe-response sequence when vacuum is insufficient. Vacuum-break release may be executed only in the S6 Release Permitted state. For a multiple-suction-cup system, assess the residual holding capacity after failure of one cup, one branch, or one vacuum source.

7.3 Magnetic Tooling (Electro-Permanent Magnet)

Electro-permanent-magnet tooling uses electrical power to magnetize or demagnetize and normally retains magnetic force after power is removed. It is suitable for handling magnetizable materials. Its safety concerns include not only release after power loss, but also poor seating, changes in air gap, material variation, misinterpretation of residual magnetism, and unintended triggering of demagnetization.

$$F_{mag} \geq K \cdot m\,(g + a_z)$$

where F_{mag} is the effective magnetic holding force under worst-case air-gap, material, and seating conditions. Magnetic-force parameters must be confirmed through sample testing or valid supplier data; ideal holding-force values alone must not be used.

Key inadvertent-release-prevention measures include magnetization-complete feedback, confirmation of holding force or seating, governance of demagnetization by release permission, access control for maintenance demagnetization, and a load-response sequence following an abnormal power outage.

7.4 Comparison of Tooling Types

Table 7-1. Holding Principles, Failure Modes, and Inadvertent-Release-Prevention Priorities by Tooling Type

Tooling Type	Principal Holding Principle	Principal Failure Modes	Inadvertent-Release-Prevention Priorities
Mechanical Gripper	Clamping force, friction, and form fit locking	Unclamping after loss of air, insufficient clamping, slipping, and incomplete	Normally closed/self-locking design, pressure monitoring, opening feedback, and release- valve interlock
Vacuum Holding	Pressure differential across the suction cup and unsuitable surface condition	Leakage, suction-cup aging, unintended vacuum-break actuation,	Vacuum monitoring, vacuum reservoir, check valves, segmented cir- cuits, and vacuum-break permission
Electro-Permanent Magnet	Magnetic-circuit holding force and misinterpretation of residual magnetism	Poor seating, material variation, unintended demagnetization,	Magnetization/demagnetization state constraints, holding-force confirmation, and demagnetization access control
Combination Tooling	Multiple holding principles tion	Failure of one holding method or incorrect logic transi-	Define the primary/secondary holding relationship and maintain at least one effective means of holding during transitions.

8 Ergonomics and Protection Against Incorrect Operation

Ergonomic measures reduce the probability of inadvertent actuation and incorrect operation, but must not replace the state machine, sensor confirmation, or hardware interlocks. Even if the operator issues a release request, the system must deny release whenever release permission has not been established.

8.1 Two-Button and Press-and-Hold Confirmation

$$Button\_OK = B1 \wedge B2 \wedge (| tB1 - tB2 | \leq Tsync) \wedge (Tpress \geq Thold)$$

where B1 and B2 are two independent button signals, Tsync is the synchronization window, Tpress is the continuous press time, and Thold is the press-and-hold threshold. Tsync and Thold must be established from the work cycle time, ergonomics, and risk assessment.

Two-button and press-and-hold confirmation can reduce the probability of single-point inadvertent actuation. Where a specified safety level is required, however, input devices and a safety-control architecture of the corresponding safety level must be used; logic written only in a standard PLC is insufficient.

8.2 HMI Secondary Confirmation and Status Indication

The HMI may display states such as Release Prohibited, Approaching Seating, Load Transfer in Progress, Release Permitted, and Abnormal-State Lockout, and may provide secondary confirmation at critical workstations. HMI confirmation improves visibility and traceability; it must not bypass R, Safety_OK, or No_Fault.

8.3 Maintenance Mode and Access Control

Bypass operations such as maintenance release, manual vacuum break, and manual demagnetization must be constrained through access authorization, a key switch, low-speed/jog operation, area clearance, and operation logging. To the extent practicable, release in maintenance mode should retain load-support confirmation or confirmation of a temporary physical support, so that a maintenance bypass does not become a new inadvertent- release path.

9 FMEA Risk Analysis

The following table is an FMEA example for inadvertent-release prevention in custom material-handling tooling. The ratings illustrate the method only. For project implementation, reassess them using workpiece mass, personnel expo- sure, cycle time, failure history, diagnostic coverage, and actual test data.

Table 9-1. Failure Mode and Effects Analysis for Inadvertent-Release Prevention (Example)

Failure Mode	Principal Causes	Consequences	Example S/O/D/RPN	Controls	Validation Focus
Release While Suspended	State-machine fault, release-valve unintended actuation, or uncontrolled by- pass	Load fall, equipment damage, and risk to personnel	10/3/4/120	S1–S5 release inhibi- tion; safety interlock for the release valve; S6 as the only per- mitted state	Inject a release request while the load is suspended; confirm that the valve does not actuate and that an alarm is logged.
Release Before Stable Seating	Height confirmed but support insufficient; eccentric loading; transfer incomplete	Tipping, slip- ping, tooling or workpiece dam- age	9/4/4/144	Contact confirmation, load- transfer confirmation, stabilization time, and eccentric-load monitoring	Create boundary-seating, eccentric- loading, and partial-support con- ditions; confirm release is not per- mitted on the hazardous side.
Unclamping After Loss of Air	Main air supply inter- rupted, line leakage, or valve leak- age	Holding force decreases and the load becomes uncontrolled	10/2/5/100	Normally closed/self-locking design, check valve, pressure-holding valve, pressure switch, and air receiver	Shut off the air supply and measure holding time, minimum pressure, and gripping force.
Vacuum Pressure Loss	Suction-cup leakage, abnormal vacuum source, or surface contami- nation	Vacuum holding force decreases and the load falls	10/3/4/120	Vacuum reservoir, check valve, vacuum monitoring, segmented circuits, and pressure-loss lockout	Simulate different leakage rates; verify alarm, retention, and release inhibition.
Unintended Release Request	Single-button acci- dental press, HMI mis- tap, or incorrect maintenance operation	Unintended re- lease request enters the system	8/5/3/120	Two-button control, press-and-hold, secondary confirmation, and access control	Confirm single-button, short-duration, or unauthorized operations cannot trig- ger Release.
Sensor Misclassification	Contamination, drift, cable fail- ure, reflection, or vibration	System falsely concludes that seating or load transfer is complete	8/4/4/128	Multisource fusion, 2oo3 voting, self-diagnostics, and signal-consistency checks	Inject open-circuit, short-circuit, and drift faults; confirm entry into release-inhibit or abnormal-state lockout.
Software or Communication Fault	Program defect, communication delay, or incorrect variable write	Incorrect release permission or corrupted state	10/2/5/100	Safety PLC, watch- dog, dual-channel per- mission, and version management	Test communication interruption, watchdog timeout, and version-regression behavior.

For items with a high RPN or a severity of 9–10, hardware interlocks and test validation must be implemented first. Even after measures reduce the RPN, high-severity failures must still remain subject to periodic validation and maintenance inspections.

10 Test Methods and Acceptance Items

10.1 Validation Principles

Validation must focus on preventing inadvertent release, preventing unsafe false-positive decisions, and ensuring that abnormal conditions are diagnosable. A combination of boundary-condition testing, fault injection, repeatability testing, and records for traceability is recommended. Claims such as “100% suppression,” “zero inadvertent releases,” or “one hundred thousand fault-free cycles” may be published as project results only when supported by a complete test report, sample definition, and statistical basis.

10.2 Functional and Interlock Test Matrix

Table 10-1. Functional and Interlock Test Matrix

Test Category	Test Method	Expected Result	Acceptance Record
State Inhibition	In each of S1–S5, issue a release re- quest.	Release remains false and the release valve does not actu- ate; the system identifies the reason for inhibition.	Record state, request, valve output, and alarm information.
Permitted Release	When all S6 conditions are satisfied, issue a release request.	Release actions execute in sequence; after release is complete, the system transitions to S7.	Record Hs/Ls/Ps/Os, the safety chain, and actuation feedback.
Pneumatic Interlock	After disconnecting pilot permission or the safety output, issue a standard release command.	The release valve does not actuate and the pneumatic circuit remains blocked.	Record pilot pressure or valve-position feedback.
Safety Chain	Trigger the emergency stop, safety gate, or safety-relay deenergization.	Immediately inhibit release; maintain clamping where necessary or execute a safe response.	Record safety-chain inputs and state-machine transi- tions.
Abnormal Reset	Create a sensor conflict or insufficient-pressure condition, then reset.	Reset requires the diagnostic and permission conditions to be satisfied again; it must not directly initiate release.	Record the fault code, person performing the reset, and reset conditions.

10.3 Seating and Load-Transfer Tests

Table 10-2. Seating and Load-Transfer Tests

Item	Test Method	Suggested Acceptance Criterion
Height Confirmation	Test at the target height, boundary height, and out-of-tolerance height.	Set Height_OK only when height is within the threshold; when out of tolerance, deny release.
Position Confirmation	Create X/Y/orientation deviations, disengaged positioning pins, pallet offset, and similar conditions.	Position_OK is false when deviation exceeds the limit or positioning is not complete.
Contact Confirmation	Create firm contact, light contact, no contact, and sensor-noise con- ditions.	Deny release when contact force is below Fmin or the signal is not credible.
Load Transfer	Measure the transfer ratio using weighing, tooling-side force, or current trends.	Set Transfer_OK only after Fs/W reaches η and remains there for τ.
Eccentric Load / Multiple Supports	**Create one unsupported point, excessive one-sided loading, or an abnormal support point.**	**Even if total support force is sufficient, deny release when eccentric loading exceeds the limit.**
Unsafe False-Positive Decision	Count false permissions across all conditions that should be rejected.	Unsafe false permission must be 0; conservative rejections should be recorded and opti- mized.

10.4 Loss-of-Air, Pressure-Loss, and Holding Tests

Table 10-3. Loss-of-Air, Pressure-Loss, and Holding Tests

Item	Test Method	Data to Record	Acceptance Focus
Loss-of-Air Retention	At rated load, shut off the air supply.	Pressure curve, gripping force, holding time, and state transition	Holding time meets the needs of a safe response; unclamping does not occur.
Slow Leakage	Introduce a small leak and monitor continu- ously.	Pressure/vacuum decay rate, alarm time, and lock- out time	Alarm thresholds are appropriate and the trend is diagnosable.
Rapid Pressure Loss	Disconnect the main air supply or vacuum source.	Valve position, pressure, load state, and alarms	The system enters hold/lockout and does not permit release.
Restore Air Supply	After the abnormal condition, restore the air supply and attempt operation.	Whether reset is required and whether the state must be recon- firmed	Restoration must not automatically release the load or clear the fault.

10.5 Human-Factor Incorrect-Operation Tests

Table 10-4. Human-Factor Incorrect-Operation Tests

Test Item	Test Method	Expected Result
Single Button	Press only B1 or B2.	Release remains false.
Buttons Not Pressed Synchronously	Press the two buttons more than Tsync apart.	Release remains false.
Short Press	Press duration is less than Thold.	Release remains false.
Unauthorized Maintenance Release	An unauthorized user attempts manual release or vacuum break.	Deny and log the operation.
Release-Permitted Indication	The operator executes release in S6.	State indication is clear and the action sequence is correct.

10.6 Documentation and Acceptance Outputs

- Risk-assessment and FMEA records;
- calculations for gripping force, vacuum holding force, or magnetic holding force;
- release-permission logic diagram, state-machine diagram, and safety I/O list;
- pneumatic, vacuum, and electrical schematics with interlock descriptions;
- test records, fault-injection records, and abnormal-reset records;
- maintenance-inspection items and a periodic pressure-retention/leakage validation plan;
- operating instructions and maintenance-mode access-control instructions.

11 Engineering Design Checklist

Table 11-1. Engineering Design Checklist for Inadvertent-Release Prevention in Custom Material-Handling Tooling

Category	Checklist Item	Acceptance Criterion
Holding Capacity	Gripping/vacuum/magnetic-force calculation	Use worst-case parameters; clearly state the safety factor and its basis.
Holding Capacity	Dynamic-load considerations	Account for additional loads caused by lifting, lowering, emergency stopping, swinging, or impact.
Seating Confirmation	Height and position confirmation	Threshold basis is clear and boundary tests pass.
Seating Confirmation	Support-contact confirmation	Contact signal exceeds noise and drift; failures are diagnosable.
Load Transfer	Transfer-ratio confirmation	Fs/W reaches the project threshold η and remains there for τ; eccentric loading on multiple supports is controlled.
Release Logic	Four-factor permission	R = Hs ∧ Ls ∧ Ps ∧ Os; no single condition may substitute for another.
Release Logic	Final command synthesis	Operator_Request, R, Safety_OK, and No_Fault are all true simultaneously.
Pneumatic Interlock	Pilot permission	The complete permission chain enables the release valve; loss of power or air results in release inhibition.
Loss-of-Air Protection	Pressure retention and holding	After the air supply is shut off, holding time meets safe-response needs and is documented by test records.
Vacuum System	Vacuum monitoring and release prevention	Vacuum switches/sensors, vacuum reservoir, check valves, and leak tests are complete.
Ergonomics	Two-button / press-and-hold / access control	A single-point inadvertent actuation, short press, or unauthorized operation cannot trigger release.
Abnormality Response	Abnormal-state lockout and reset	S8 lockout, fault codes, controlled reset, and operation records are complete.
Validation Documentation	Testing and traceability	Test methods, sample size, acceptance criteria, raw records, and documented issue closure are complete.

12 Engineering Conclusions

The safety design of custom material-handling tooling must address both holding the load and preventing release at the wrong time. The former concerns holding capacity; the latter concerns release permission and state safety.

Release actions must be constrained by the load state machine and executed only in the S6 Release Permitted state. In S1–S5, S8, and other non-permitted states, the release path must be blocked at both the software and hardware levels.

Seating confirmation must not rely on height or position alone. Height, position, support contact, and load transfer must all be established; of these, load-transfer confirmation most directly addresses the safety objective of preventing a fall after release.

Pneumatic interlocks, vacuum retention, loss-of-air holding, pressure/vacuum monitoring, two-button control, press-and-hold confirmation, and abnormal-state lockout are not redundant; together, they provide defense in depth against different failure paths.

The thresholds, synchronization windows, holding times, transfer ratios, and safety factors discussed here must be established through project-level risk assessment, sample testing, and acceptance records. Unvalidated data should not be presented as a universal conclusion in website materials.

Upgrading tooling control from simple action control to state-safety control helps reduce the risks of release while suspended, release before stable seating, release after pressure loss, and incorrect human operation, and provides an actionable framework for the engineering design, design review, and acceptance of custom material-handling tooling.

Published by: Jiangsu AUREK Intelligent Technology Co., Ltd. · Engineering Research Center. This corporate engineering research material is intended to explain methods and support engineering communication; it does not replace project-specific safety assessment, test validation, or certification requirements.

Jiangsu AUREK Intelligent Technology Co., Ltd. · Engineering Research Center
Website Resource Center Release · V1.1 · 2026-06