

Risk-Based Engineering Change Control for Medical Device Manufacturing: A Framework and Representative Quantitative Case Study

Tushar S. Bendigeri, M.S.

Independent Quality Engineering Researcher, Connecticut, USA

Abstract - Engineering changes are necessary to improve product safety, manufacturability, traceability, and regulatory compliance, but they can also create new product and process risks. This research presents a risk-based engineering change control framework for medical device manufacturing. The framework converts an engineering change from an administrative transaction into a traceable risk-management argument that links the change rationale, hazard analysis, Design Failure Mode and Effects Analysis (DFMEA), Process Failure Mode and Effects Analysis (PFMEA), supplier assessment, validation evidence, release criteria, and post-implementation monitoring. A design-science approach was used to develop five decision gates and an evidence-intensity logic. A representative case study was then used to demonstrate the method for conversion of manual component verification to barcode and machine-vision verification. The quantitative examples use synthetic, illustrative data only; they do not describe an actual device, manufacturer, supplier, complaint population, or validation result. Representative analyses include Pareto prioritization, p-chart process behavior, process capability comparison, an ANOVA challenge-test example, exploratory regression, Monte Carlo scenario modeling, bow-tie analysis, and a residual-risk heat map. The case illustrates how a structured evidence chain can support prevention-focused controls, proportionate validation, and timely post-release review. The framework is intended to assist design quality engineers and cross-functional teams in documenting why a change is expected to reduce manufacturing escape opportunities without introducing unacceptable residual risk.

Keywords: engineering change control; medical devices; ISO 14971; DFMEA; PFMEA; risk management; validation; manufacturing escape

1. INTRODUCTION

Engineering changes are routine throughout the medical device lifecycle. Typical triggers include recurring nonconformances, complaint signals, supplier transfers, equipment replacement, capacity expansion, material changes, traceability improvements, and regulatory updates. A change that appears technically simple can nevertheless alter how a product is assembled, inspected, labeled, or released. Consequently, a completed change order and an attached test report are not sufficient by themselves to establish that the changed condition remains adequately controlled.

Medical device quality systems require risk-management thinking across product realization and production use. ISO 14971:2019 defines lifecycle risk-management principles for medical devices [1], while ISO 13485:2016 establishes quality-management-system requirements for regulatory purposes [2]. In the United States, the Quality Management System Regulation (QMSR) became effective on February 2, 2026 and incorporates ISO 13485:2016 by reference, subject to supplemental FDA requirements [3], [4]. These sources collectively favor a traceable relationship between change decisions, risk controls, objective evidence, and postmarket learning.

The recurring practical issue is weak integration across systems that are frequently maintained separately: risk-management files, DFMEA, PFMEA, control plans, validation protocols, supplier controls, complaint handling, and corrective action. This study presents a framework intended to make the linkage explicit. The framework does not replace a manufacturer's approved procedures or regulatory strategy. Instead, it offers a reusable structure for identifying change-related uncertainty, selecting risk controls, defining evidence, and monitoring implementation effectiveness.

2. RELATED LITERATURE AND REGULATORY CONTEXT

Risk management in medical devices is an iterative process in which production and post-production information can affect the risk evaluation and the effectiveness of risk controls [1], [5]. FMEA is commonly used to identify potential failure modes and to plan prevention and detection controls; IEC 60812:2018 and the AIAG & VDA handbook provide recognized guidance for FMEA practice [6], [7]. These methods are complementary to, rather than substitutes for, an ISO 14971 risk-management process.

Engineering change control is strengthened when FMEA outputs are connected to objective verification, measurable release criteria, and post-implementation monitoring. Statistical quality-control techniques such as Pareto analysis, control charts, capability analysis, regression, and designed comparisons can help distinguish signal from noise when their assumptions and data definitions are understood [8], [9]. Risk visualization techniques, including bow-tie and fault-tree logic, can clarify preventive versus mitigative barriers and identify common-cause dependencies [10].

Table I. Key sources and their practical contribution to the proposed framework.

Source / method	Practical contribution
ISO 14971:2019 [1]	Lifecycle risk-management principles, residual-risk evaluation, and production/post-production feedback.
ISO 13485:2016 and QMSR [2]-[4]	Quality-system basis for controlled changes, documented evidence, and medical-device manufacturing controls.
FMEA guidance [6], [7]	Structured identification of failure modes, causes, current controls, and action priorities.
SPC and capability methods [8], [9]	Objective evaluation of process behavior and variation after implementation.
ISO 31010 and human-factors guidance [10]-[12]	Selection of risk-analysis methods and consideration of human-dependent controls.

3. RESEARCH OBJECTIVE, QUESTIONS, AND CONTRIBUTION

The objective of this methodology paper is to propose and demonstrate a risk-based engineering change control framework that integrates design, process, supplier, validation, and post-release evidence. The research is guided by the following questions:

- RQ1: What decision structure can make change-related risk, controls, evidence, and residual-risk follow-up traceable across functions?
- RQ2: How can a representative quantitative case study demonstrate the relationship between prevention-focused controls and manufacturing-escape opportunity?
- RQ3: Which visual and statistical tools best support cross-functional review without replacing product-specific risk evaluation?

The contribution is a five-gate, evidence-chain model that can be scaled according to change impact. The model adds an explicit link from the change driver to hazard and FMEA analysis, control selection, verification/validation, release criteria, and post-implementation monitoring. The study is a design-science and representative-case methodology paper, not a clinical study or an empirical report of a specific manufacturer.

4. METHODOLOGY

4.1 Framework development

The framework was developed by integrating the lifecycle risk-management orientation of ISO 14971, FMEA concepts, validation planning, control hierarchy, and statistical monitoring. It uses five decision gates: define the change; assess change-related risk; select controls; verify and validate controls; and confirm effectiveness after release. Each gate produces an evidence output required for progression to the next gate.

Closed-Loop Risk-Based Engineering Change System



Risk information is continuously translated into controls, verification, and post-implementation learning.

Figure 1. Closed-loop quality model linking manufacturing and postmarket signals to risk assessment, verification, controlled release, and ongoing evidence. Source: Author-developed framework.

Five-Gate Risk-Based Engineering Change Workflow

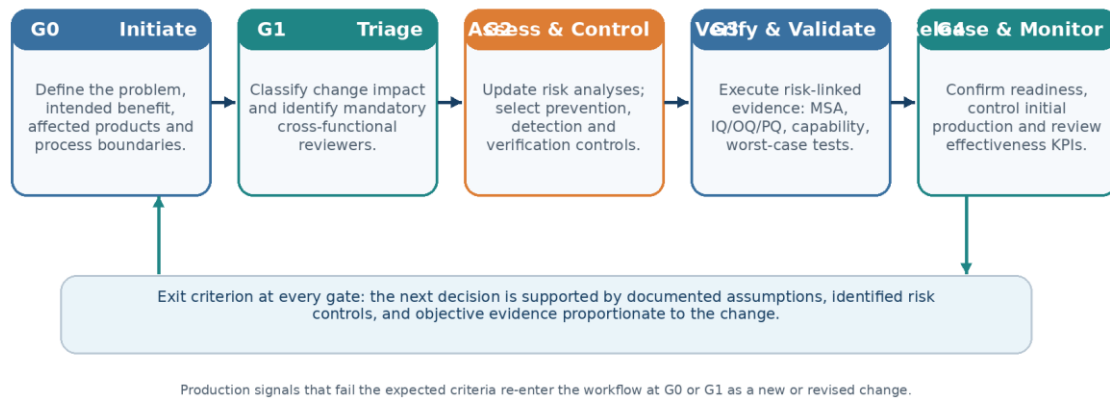


Figure 2. Five decision gates for risk-based engineering change control. Source: Author-developed framework.

4.2 Evidence intensity and traceability

Evidence intensity should be proportionate to the possible impact of the change. A narrow document correction may need a focused assessment. A change affecting product configuration, critical-to-quality characteristics, labeling, software, sterilization, acceptance equipment, supplier controls, or human-dependent setup requires stronger cross-functional review and more explicit objective evidence. Urgency is not evidence of acceptable risk; when uncertainty remains, the change package should document interim controls or obtain additional evidence before release.

Table II. Illustrative five-gate framework and minimum evidence outputs.

Gate	Decision question	Minimum evidence output
G1 - Define	What changes, why, and within what product/process boundary?	Problem statement, scope, affected items, assumptions, and intended benefit.
G2 - Assess	What new or changed failure modes and hazards may result?	Impact assessment; risk-file, DFMEA, PFMEA, and supplier-review inputs.
G3 - Control	Which prevention and detection controls are proportionate?	Control architecture, control-plan updates, work-instruction and training impacts.
G4 - Verify	What evidence shows the controls work under relevant conditions?	Protocol, MSA where applicable, IQ/OQ/PQ or equivalent, challenge tests, acceptance criteria.
G5 - Confirm	What production evidence will confirm effectiveness and residual-risk acceptability?	Release plan, KPI dashboard, owner, cadence, thresholds, and escalation path.

Risk Traceability: From Change Driver to Objective Evidence

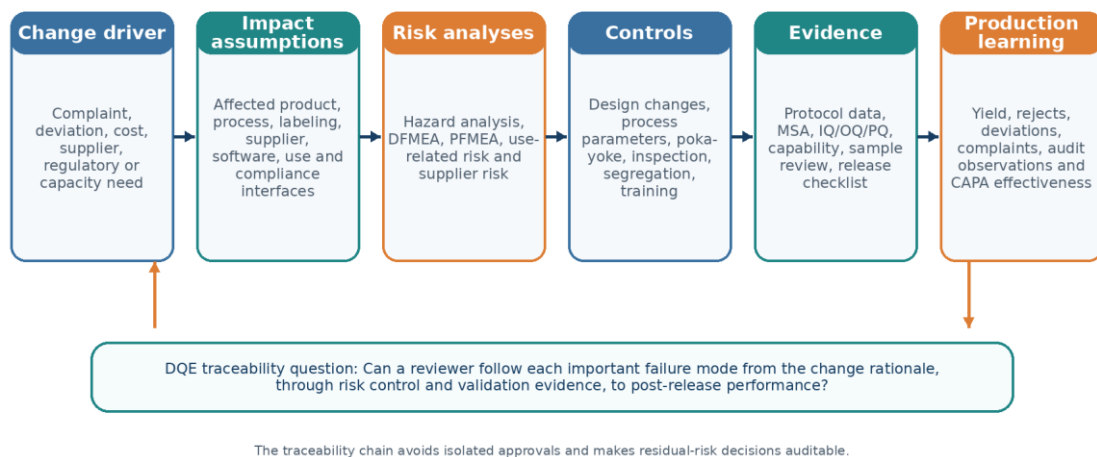


Figure 3. Traceability map from the initiating signal through risk analysis, control selection, validation evidence, and post-release review. Source: Author-developed framework.

Risk-Control Hierarchy for Change-Related Failure Modes

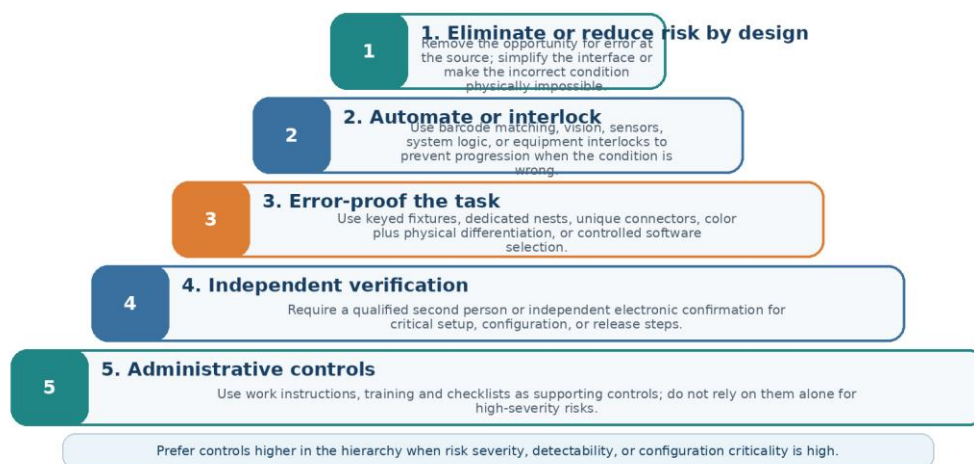


Figure 4. Risk-control hierarchy emphasizing prevention and error-proofing before reliance on memory or training. Source: Author-developed framework.

4.3 Representative case study and illustrative dataset

The representative case examines a critical manufacturing setup in which visually similar components are selected and verified manually. The process is assumed to have experienced configuration-related deviations attributable to wrong component selection, incomplete changeover, and identification mismatch. The proposed engineering change adds barcode-based identity verification, a machine-vision confirmation step, independent setup verification, and a defined safe response when identity information is unreadable or inconsistent.

All data used in this paper are synthetic and illustrative. The data were created to show how the framework can be evaluated; they must not be interpreted as actual product, process, supplier, complaint, validation, or field-performance data. The comparison uses a 12-period baseline and a 12-period post-implementation phase with constant denominator assumptions for demonstration only.

Table III. Representative case-study design and analysis plan.

Element	Representative specification
Change driver	Recurring configuration-related deviations during a critical setup/changeover operation.

Element	Representative specification
Baseline control	Single-operator visual verification and procedural confirmation.
Proposed control package	Barcode identity check, vision confirmation/interlock, independent verification, updated PFMEA/control plan, targeted challenge testing.
Primary response metric	Configuration deviations per completed setup.
Balancing measures	False rejects, cycle time, system downtime, and operator usability observations.
Quantitative tools	Pareto analysis, p-chart, Cp/Cpk, ANOVA, regression, and Monte Carlo scenario model.

5. RESULTS OF THE REPRESENTATIVE QUANTITATIVE EVALUATION

5.1 Baseline prioritization and post-implementation process behavior

The illustrative Pareto analysis identifies wrong component or kit selection, incomplete changeover, and barcode/label mismatch as the most frequent configuration-related deviation categories. This prioritization supports upstream prevention and early detection rather than adding only final inspection. The p-chart illustrates a sustained lower configuration-deviation proportion after the intervention. Interpretation must confirm that the data collection method and denominator definitions did not change across the periods.

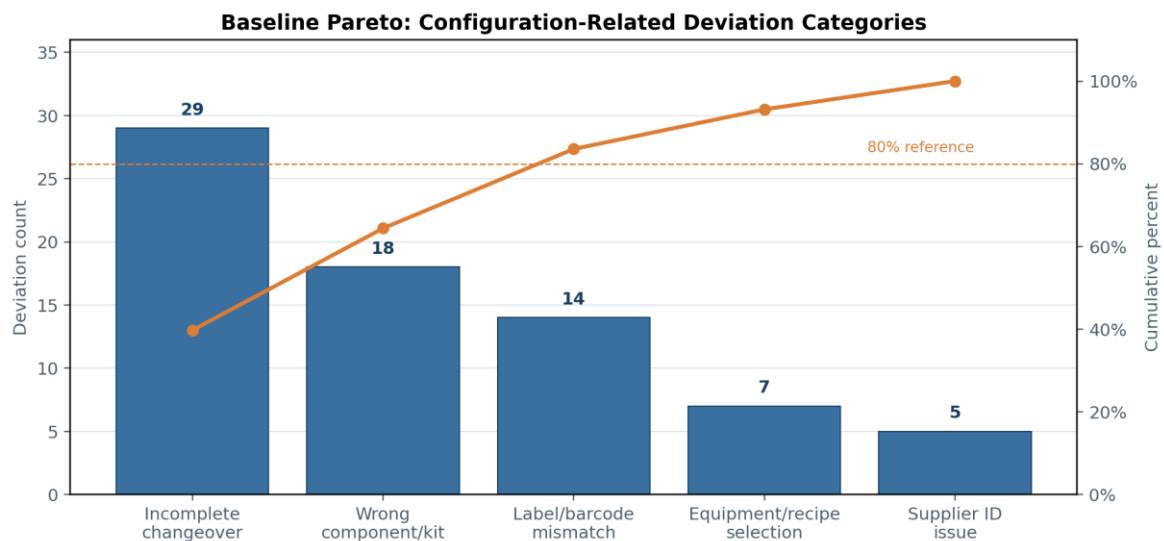


Figure 5. Illustrative Pareto analysis used to prioritize configuration-related deviation categories. Synthetic data; source: author-developed.

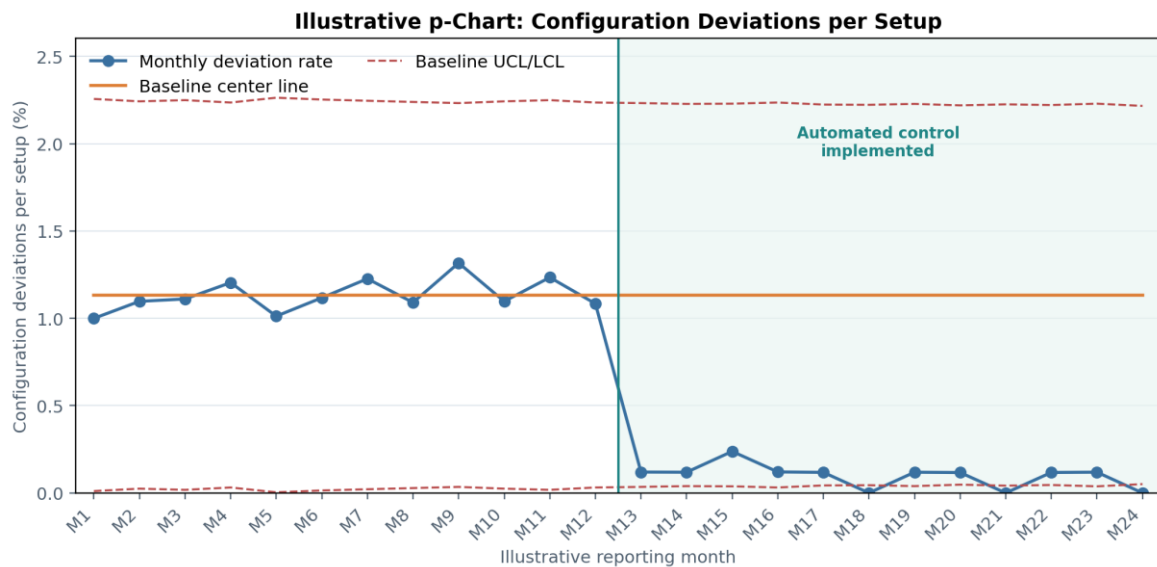


Figure 6. Illustrative p-chart comparing baseline and post-implementation configuration-deviation proportions. Synthetic data; source: author-developed.

5.2 Capability and challenge-test findings

For the illustrative critical setup position, the target is 10.00 mm with specification limits of 9.50 mm and 10.50 mm. The representative baseline condition has mean 10.02 mm, standard deviation 0.17 mm, $C_p = 0.98$, and $C_{pk} = 0.94$. The post-implementation condition has mean 9.98 mm, standard deviation 0.10 mm, $C_p = 1.61$, and $C_{pk} = 1.56$. Capability is interpreted only after confirming that the measurement system is fit for purpose and that the specification limits are scientifically justified.

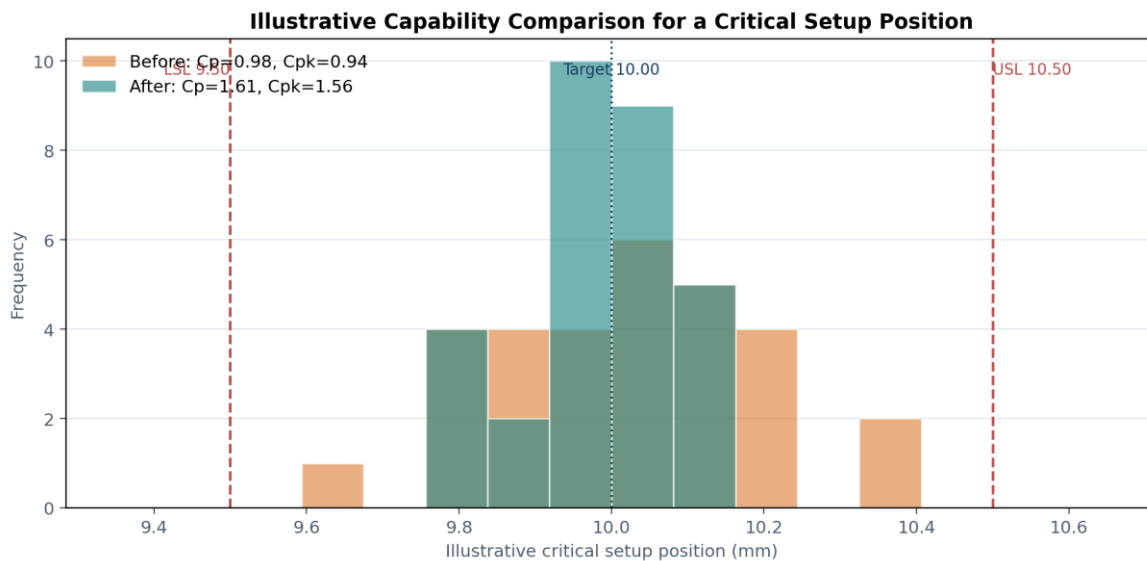


Figure 7. Illustrative capability comparison for a critical setup position before and after control standardization. Synthetic data; source: author-developed.

The representative challenge test compared detection latency for manual visual verification, barcode verification, and barcode plus vision interlock. The illustrative one-way ANOVA result was $F = 288.5$ with $p < 0.001$. This result indicates a difference among mean detection latencies within the synthetic dataset. It does not establish universal superiority of a technology; implementation still requires equipment-specific reliability, challenge testing, maintenance controls, and human-factors review.

Table IV. Illustrative quantitative findings used to demonstrate the evaluation approach.

Measure	Baseline / comparator	Representative post-change result	Interpretive caution
Configuration deviations	18 events per 12,000 setups	5 events per 12,000 setups	Synthetic counts; confirm denominators and data definition in actual use.
Critical setup capability	$C_p = 0.98$; $C_{pk} = 0.94$	$C_p = 1.61$; $C_{pk} = 1.56$	Use only with a fit-for-purpose measurement system and justified specifications.
Challenge-test ANOVA	Manual, barcode, barcode + interlock	$F = 288.5$; $p < 0.001$	Shows difference in synthetic means; requires practical significance review.
Exploratory regression	Manual selection burden	Slope = 0.61/1,000; $R^2 = 0.99$	Screening association only; not causal proof.
Scenario simulation	Selection error 1.2%; detection 70%	Selection error 0.4%; detection 98%	Inputs need evidence, sensitivity testing, and product-specific review.

5.3 Exploratory regression and scenario modeling

The illustrative regression associates each additional manual selection point with 0.61 additional deviations per 1,000 setups ($R^2 = 0.99$, $p = 0.0000$). The relationship should be used only as a screening signal because product complexity, staffing, training, material presentation, and setup frequency may confound the association. In the representative Monte Carlo scenario model, a manual process uses a 1.2% selection-error probability and 70% detection effectiveness, whereas the proposed control package uses 0.4% selection-error probability and 98% detection effectiveness. The estimated escape probability is 0.0036 for the manual scenario and 0.00008 for the controlled scenario. These values are assumptions, not a quantified risk estimate for any real device.

6. Risk Visualization and Control Logic

Statistical outputs do not show how barriers act or where controls can fail together. Risk visualization helps reviewers distinguish prevention from mitigation and probe dependencies among controls. These visualizations are supporting communication tools; they do not replace the approved risk-management file, FMEA, validation plan, or change-control procedure.

Illustrative Bow-Tie Analysis: Critical Configuration Verification

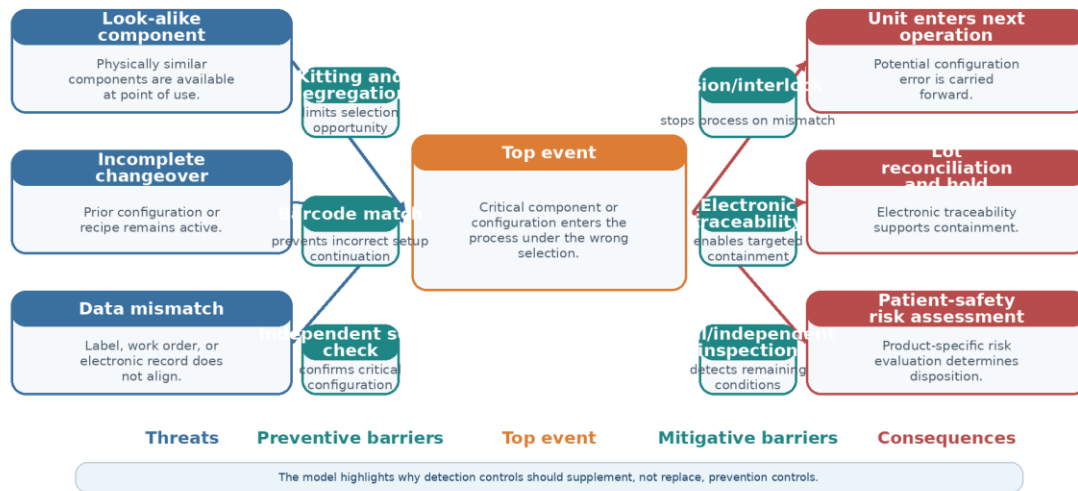


Figure 8. Illustrative bow-tie analysis for a configuration-control failure mode. The model differentiates preventive barriers from mitigative barriers. Source: author-developed.

Illustrative Risk Heat Map: Configuration-Control Improvement

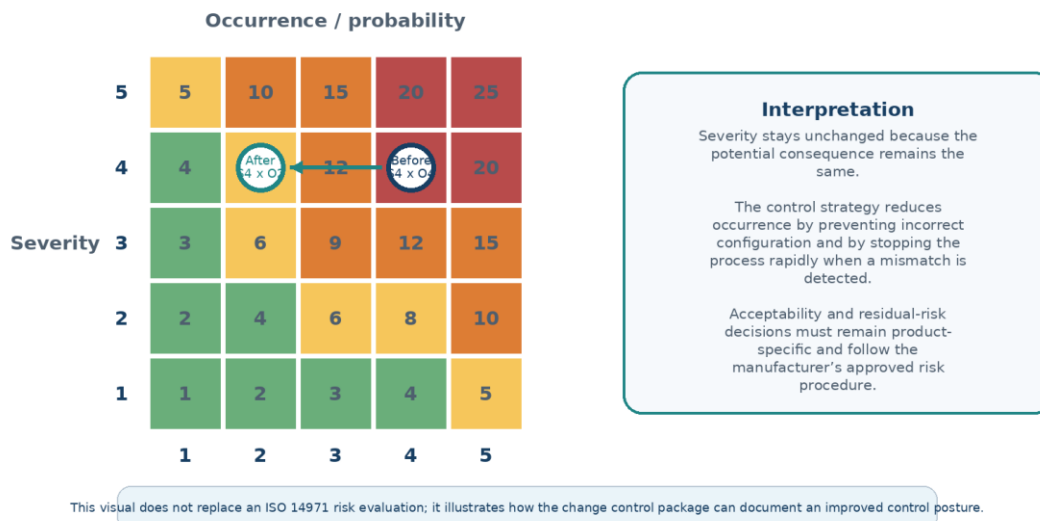


Figure 9. Illustrative residual-risk heat map. Severity remains constant while occurrence and detectability are improved through prevention and detection controls. Source: author-developed.

The bow-tie logic emphasizes that downstream inspection is not equivalent to prevention. Upstream component differentiation, barcode identity matching, physical error-proofing, and appropriate interlocks reduce the likelihood that the wrong condition is created or allowed to continue. The residual-risk heat map emphasizes a second point: a change can reduce occurrence and improve detectability without changing severity. Residual-risk acceptability still requires the manufacturer's approved criteria and, where applicable, benefit-risk review.

7. IMPLEMENTATION AND POST-RELEASE GOVERNANCE

Implementation should be controlled through a documented release plan. The plan should define the accountable owner, review cadence, data source, alert thresholds, response actions, and balancing measures. This prevents a common failure mode in change

control: declaring the change complete after the protocol is approved without reviewing whether the process remains effective during actual production.

Table V. Suggested post-implementation monitoring plan for a high-impact change.

Metric family	Example measure	Review cadence	Example response
Primary effectiveness	Configuration deviations per setup	Daily during launch; then weekly/monthly	Open escalation if defined threshold or trend is exceeded.
Control performance	Barcode/vision read rate; interlock challenge result	Per lot or defined frequency	Investigate degradation; assess maintenance and verification status.
Balancing measures	False rejects, cycle time, downtime, operator usability	Weekly during launch	Review trade-offs; revise control or work design as necessary.
Quality-system feedback	NCR, CAPA, complaint, audit findings	Monthly or management-review cadence	Re-enter risk review; assess whether change assumptions remain valid.

Post-Implementation Monitoring and Escalation Loop

Illustrative governance structure - alert thresholds and cadence must be defined in the organization's approved procedures.

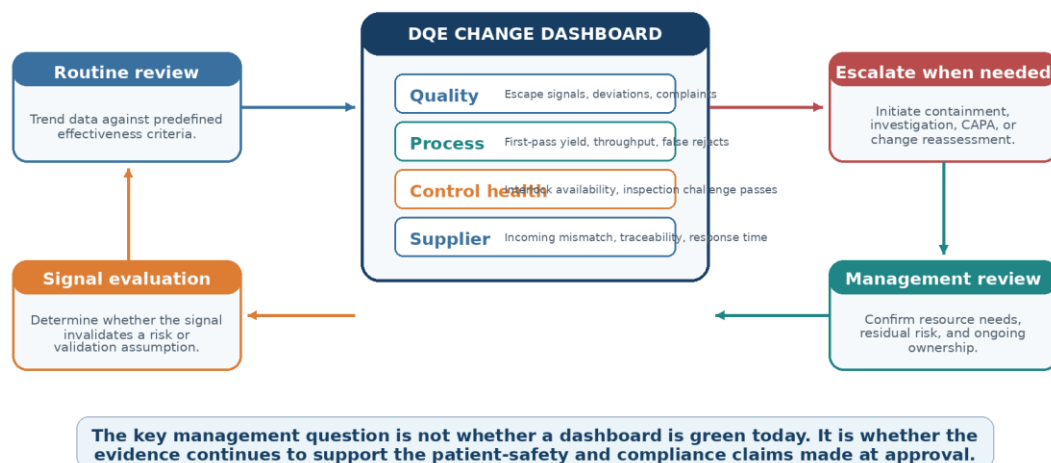


Figure 10. Illustrative post-implementation monitoring and escalation loop. A dashboard is effective only when metric ownership, cadence, and action thresholds are defined. Source: author-developed.

8. DISCUSSION

The primary value of the proposed framework is not a specific numerical reduction. It is the traceability of the engineering-change decision. The change rationale identifies the failure condition; hazard analysis and FMEA identify the risk mechanisms; control selection emphasizes prevention and independent barriers; validation challenges the control assumptions; and the release plan defines the evidence that will confirm performance in routine use.

The framework also supports disciplined use of analytics. Pareto analysis focuses attention on the categories that drive most deviations. Control charts help identify process shifts after implementation. Capability indices quantify the relationship between variation and specifications. ANOVA and regression can support investigation but must be interpreted with process knowledge. Monte Carlo models can make assumptions visible and support sensitivity analysis, but they do not replace an ISO 14971 risk evaluation or product-specific engineering judgment.

For high-severity or weakly detectable failure modes, prevention, physical constraints, automation, and independent verification should be considered before reliance on training or memory. However, automation introduces its own failure modes: false rejects, unreadable labels, system downtime, data integrity, maintenance lapses, and operator workarounds. Therefore, a risk-based change package must evaluate both the failure it intends to reduce and the new failure modes it introduces.

9. LIMITATIONS

- The paper is a methodology and representative-case study; it does not report empirical results from a real product, facility, supplier, or complaint system.
- All numerical results, charts, simulations, and statistical outputs are synthetic and illustrative. They should be replaced with authorized data and a transparent analysis plan before making product-performance claims.
- The framework does not replace manufacturer procedures, regulatory consultation, product-specific risk management, validation requirements, or benefit-risk analysis.
- The model is intended for medical-device manufacturing changes but requires adaptation to product category, automation maturity, supplier model, regulatory jurisdiction, and quality-system architecture.

10. CONCLUSION

Risk-based engineering change control is most effective when treated as an evidence chain rather than a document-routing activity. The proposed five-gate framework integrates change definition, risk assessment, control selection, validation, controlled release, and post-implementation monitoring. The representative case shows how a manual component-verification risk can be assessed through FMEA, control hierarchy, challenge testing, statistical monitoring, and risk visualization without relying solely on final inspection or training.

The framework is scalable and practical. Its essential question is simple: what evidence supports the conclusion that the change achieves its intended benefit without introducing unacceptable residual risk? When the answer is traceable from the initiating signal to production evidence, engineering change control becomes a more reliable mechanism for protecting quality, compliance, and patient safety.

Acknowledgment.

The author acknowledges the quality-engineering community and publicly available standards and guidance that informed this generalized methodology. No employer, supplier, product, site, customer, or patient data were used in this manuscript.

Declarations.

Table VI. Publication integrity and transparency declarations.

Item	Statement
Funding	No external funding was received for this methodology paper.
Conflict of interest	The author works in medical device quality engineering. The manuscript presents a generalized framework and does not disclose proprietary employer information.
Data availability	All quantitative data are synthetic, illustrative examples generated for the manuscript. No underlying clinical, manufacturing, supplier, complaint, or patient dataset is associated with this work.
Ethics approval	Not applicable. No human participants, patient information, clinical data, or animal data were used.
Author contribution	The author developed the framework, prepared the representative case study, performed the illustrative analyses, and drafted the manuscript.
Submission note	Replace the corresponding-author email, verify current target-journal instructions, complete employer publication review if applicable, and obtain approval before external submission.

REFERENCES.

- [1] International Organization for Standardization, ISO 14971:2019, Medical devices - Application of risk management to medical devices. Geneva, Switzerland: ISO, 2019.
- [2] International Organization for Standardization, ISO 13485:2016, Medical devices - Quality management systems - Requirements for regulatory purposes. Geneva, Switzerland: ISO, 2016.
- [3] U.S. Food and Drug Administration, "Quality Management System Regulation (QMSR)," FDA, updated Feb. 2, 2026. [Online]. Available: <https://www.fda.gov/medical-devices/postmarket-requirements-devices/quality-management-system-regulation-qmsr>
- [4] U.S. Food and Drug Administration, "Quality and Compliance (Medical Devices)," FDA, Jan. 30, 2026. [Online]. Available: <https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/quality-and-compliance-medical-devices>
- [5] International Organization for Standardization, ISO/TR 24971:2020, Medical devices - Guidance on the application of ISO 14971. Geneva, Switzerland: ISO, 2020.
- [6] International Electrotechnical Commission, IEC 60812:2018, Failure modes and effects analysis (FMEA and FMECA). Geneva, Switzerland: IEC, 2018.
- [7] Automotive Industry Action Group and Verband der Automobilindustrie, AIAG & VDA FMEA Handbook, 1st ed. Southfield, MI, USA: AIAG, 2019.
- [8] D. C. Montgomery, Introduction to Statistical Quality Control, 8th ed. Hoboken, NJ, USA: Wiley, 2020.
- [9] D. J. Wheeler, Understanding Statistical Process Control, 3rd ed. Knoxville, TN, USA: SPC Press, 2000.

- [10] International Organization for Standardization, ISO 31010:2019, Risk management - Risk assessment techniques. Geneva, Switzerland: ISO, 2019.
- [11] International Electrotechnical Commission, IEC 62366-1:2015, Medical devices - Part 1: Application of usability engineering to medical devices. Geneva, Switzerland: IEC, 2015.
- [12] U.S. Food and Drug Administration, Applying Human Factors and Usability Engineering to Medical Devices: Guidance for Industry and Food and Drug Administration Staff. Silver Spring, MD, USA: FDA, 2016.
- [13] International Council for Harmonisation, ICH Q9(R1): Quality Risk Management. Geneva, Switzerland: ICH, 2023.
- [14] J. M. Juran and A. B. Godfrey, Juran's Quality Handbook, 7th ed. New York, NY, USA: McGraw-Hill, 2017.

Appendix A. Reusable Risk-to-Evidence Traceability Template

Table VII. Template for evidence linkage within a risk-based engineering change package.

Change assumption / failure mode	Risk mechanism	Control(s)	Evidence / acceptance criterion	Post-release measure
Incorrect component selected during setup	Configuration mismatch may continue into manufacturing	Barcode match; vision interlock; physical differentiation	Challenge test detects mismatch and reaches defined safe state	Mismatch attempts; read rate; configuration deviations
Prior setup retained after changeover	Wrong program/tooling/component remains active	Electronic reset; independent setup confirmation; checklist	OQ test of reset logic and simulated changeover	Setup deviations; audit observations; repeat deviations
Vision unreadable or false reject	Control does not identify condition or disrupts flow	Defined safe response; maintenance; re-verification procedure	Readability challenge; false-reject threshold; recovery test	Read failures; downtime; false rejects; maintenance trend