ENGINEERING FIELD GUIDE

Developing and Manufacturing Medical Devices

A practical guide for electronics engineers

From architecture and risk control to production release, process control and post-market support

General cross-market guidance | Edition 1.0 | August 2026

How to use this guide

This guide explains how electronics engineering fits into the regulated medical-device lifecycle. It is intended for engineers designing printed circuit boards, power systems, sensors, analogue and digital circuitry, embedded platforms, wireless interfaces, test equipment and production electronics. It applies to both in-house design and outsourced development or manufacture.

CORE MESSAGE A technically sound circuit is not yet a compliant medical-device design. The design must also be derived from controlled requirements, address risk, be independently verified, be reproducible in manufacture, remain traceable through change, and generate objective evidence.

Scope and important limitations

- The manufacturer must determine the intended use, target markets, regulatory classification, applicable legislation, conformity-assessment route and standards for the specific device.
- IEC 60601 is not the universal electrical safety standard for every medical device. Medical electrical equipment commonly uses the IEC 60601 family; laboratory and IVD equipment may instead use the IEC 61010 family; other device types may require different product standards.
- Standards editions, amendments, national deviations and recognised or harmonised status change. Confirm the controlled standards list for the project before designing or testing.
- This guide supports engineering practice but does not replace the organisation's quality management system, regulatory strategy, risk management file, approved plans or the text of applicable legislation and standards.

Contents

1. What changes when electronics becomes part of a medical device

Medical-device electronics are developed within a quality system and a product safety case. Engineering decisions must be explainable months or years later to reviewers who were not present when the decision was made. Those reviewers may include systems and risk engineers, test laboratories, notified bodies, regulators, auditors, manufacturing partners, complaint investigators and future maintainers.

The four simultaneous engineering objectives

Objective	What it means for the electronics engineer
Functional performance	The circuit performs its specified functions over stated operating, storage, transport and lifetime conditions.
Safety and risk control	Hardware contributes to preventing or detecting hazardous situations and does not introduce unacceptable electrical, thermal, mechanical, EMC, radiation, battery, data or use-related risks.
Reproducible manufacture	Approved suppliers, processes, tolerances, test methods, programming, calibration and acceptance criteria consistently produce conforming units.
Objective evidence	Requirements, analyses, reviews, test records, deviations and changes are documented, approved, traceable and retrievable.

Design assurance is not extra paperwork

The documentation should be the durable record of engineering work that was necessary anyway: what the device must do, what could go wrong, why the architecture is suitable, how tolerances and faults were considered, what was tested, what failed, what changed and why the released design is acceptable. Weak documentation usually signals that important engineering decisions cannot be independently reconstructed.

USEFUL TEST If a competent engineer outside the project cannot reproduce the reasoning from the controlled records, the design evidence is probably incomplete.

2. Lifecycle overview and engineering evidence

Medical-device development is iterative, but it is controlled iteration. Each phase should consume approved inputs, produce defined outputs and close its reviews before the product advances. Risk management, usability, cybersecurity, supplier management and configuration control run across the entire lifecycle.

Lifecycle stage	Electronics focus	Typical evidence
Concept and feasibility	Technology options, feasibility risks, preliminary power/size/cost estimates, proof-of-concept circuits.	Feasibility reports, trade studies, early hazards, prototype records, assumptions.
Planning and design inputs	Applicable standards, interfaces, electrical and environmental requirements, safety-related constraints.	Development plan, standards list, hardware requirements, interface specifications, risk plan.
Architecture and detailed design	Partitioning, protection concepts, schematics, PCB, component derating, diagnostics and manufacturability.	Architecture, design descriptions, calculations, analyses, schematics, layout, BOM, reviews.
Verification and validation	Prove outputs meet inputs; support system validation in representative use.	Protocols, objective results, anomaly records, traceability, compliance reports.
Design transfer	Convert the design into controlled production specifications and test processes.	Manufacturing package, test specifications, fixtures, process validations, transfer review.
Production and release	Maintain process capability, traceability, calibration, programming and acceptance.	Device history/build records, inspection/test data, nonconformities, release records.
Post-market and change	Investigate field issues, control redesigns, manage components and security-relevant hardware.	Complaint investigations, CAPA inputs, change assessments, re-verification, trend reports.

The evidence chain

1. **Need and intended use.** Explain the clinical or operational purpose, users, use environment and patient population.
2. **System and risk-derived requirements.** Translate needs, standards and risk controls into measurable engineering inputs.
3. **Design outputs.** Define the circuit, PCB, components, programmable-device configuration, interfaces and production instructions.
4. **Verification.** Demonstrate that each applicable input and risk control is implemented correctly.
5. **Validation and clinical/performance evidence.** Demonstrate that the finished device supports intended use under representative conditions.
6. **Production evidence.** Show that each released unit or batch was built and accepted using controlled processes.
7. **Post-market evidence.** Feed complaints, service, trends, supplier changes and new knowledge back into risk and design control.

3. Intended use, regulatory strategy and standards planning

Electronics design should not begin from an assumed list of familiar standards. It begins from the intended purpose and the regulatory strategy. The same processor, power supply or radio may require different controls depending on whether it forms part of a home-use infusion system, an IVD analyser, a wearable monitor or a hospital accessory.

Questions to settle early

- **Device identity.** What is the device, accessory, subsystem or platform, and what medical purpose does it support?
- **Users and patients.** Professional or lay users? Which patient populations and foreseeable limitations?
- **Environment.** Hospital, laboratory, ambulance, home, outdoors, transport, sterile field or uncontrolled consumer environment?
- **Patient connection.** Is there an applied part, conductive connection, fluid path, sensor contact or energy delivered to the patient?
- **Power and communications.** Mains, internal battery, charging, USB, Ethernet, wireless, cloud or third-party accessories?

- **Essential performance.** Which performance loss or degradation could create an unacceptable risk?
- **Markets.** Which jurisdictions, device classification rules and market-specific requirements apply?
- **Product family.** What variants, options and accessories must be included in the compliance strategy?

Selecting the electrical safety framework

Typical product context	Likely starting point	Engineering implication
Medical electrical equipment or system interacting with a patient for a medical purpose	IEC 60601-1 plus applicable collateral and particular standards	Basic safety, essential performance, means of protection, leakage currents, EMC and risk-management integration.
Laboratory, measurement, control or IVD analyser equipment	IEC 61010-1 plus applicable particular standards, such as those for IVD equipment	Protection against electrical, mechanical, thermal, chemical and other hazards in laboratory use.
Standalone accessory or non-ME component	Product-specific assessment; possibly another IEC/UL/ISO standard	Do not claim IEC 60601 applicability automatically; assess how the accessory affects the finished system.
External power supply, battery pack, radio module or IT equipment used within the device	Component approvals can support but rarely replace finished-device evaluation	Verify conditions of acceptability, ratings, isolation, interfaces and use within the final device.

PLANNING RULE Create and approve an applicable standards and regulatory requirements list early. Record the selected edition, amendments, national or regional adoption, rationale for applicability, and the evidence planned for compliance.

4. Requirements, architecture and traceability

Good hardware requirements are testable

A requirement should state an observable outcome, its conditions and its acceptance limit. Avoid requirements that merely restate a design solution unless the solution itself is mandated by architecture, risk control or an external constraint.

Weak statement	Improved requirement
Use a low-noise amplifier.	Across the specified sensor source impedance and 0.5-40 Hz band, input-referred noise shall not exceed the defined limit when measured using the approved test configuration.
The battery must last a long time.	The device shall complete at least the specified number of use cycles after the stated storage period and under the defined worst-case temperature, radio and load profile.
Protect against overvoltage.	A single specified input overvoltage shall not result in an unacceptable hazardous situation; recovery behaviour and any protective shutdown shall meet the defined acceptance criteria.
The PCB shall pass EMC.	The finished device shall maintain the defined basic safety and essential performance during and after the specified immunity tests and remain within the stated emissions limits.

Sources of electronics requirements

- System and subsystem requirements, including primary functions and essential performance.
- Risk controls from hazard analysis, FMEA, fault-tree analysis, cybersecurity threat modelling and usability engineering.
- Interfaces with sensors, actuators, power sources, software, mechanics, disposables, accessories and external systems.
- Applicable standards and regulations, including electrical safety, EMC, radio, environmental and substance restrictions.
- Manufacturing, service, calibration, testability, traceability and diagnostic needs.
- Reliability, lifetime, storage, transport, cleaning, disinfection, sterilisation and environmental constraints.

Architecture must make safety visible

The hardware architecture should identify energy and signal paths, isolation boundaries, protective components, patient or operator connections, safety-related sensors and actuators, diagnostic coverage, power states, communication boundaries and dependencies on software. It should also show which elements implement risk controls and how independence is achieved where required.

INTERFACE DISCIPLINE Every electrical interface needs agreed ownership, signal definition, voltage/current limits, timing, fault behaviour, connector/pin assignment, grounding/shielding concept and verification responsibility.

Traceability expectations

Bidirectional traceability should connect requirements to design outputs, risk controls, verification evidence and unresolved anomalies. Traceability is not a late spreadsheet exercise; it is a design completeness check. An orphan requirement indicates missing implementation or test evidence. An unexplained circuit function indicates an undocumented requirement, unnecessary complexity or both.

5. Risk management for electronics

ISO 14971-style risk management is performed at device level. Hardware FMEA is useful but is not the whole risk analysis. Start with hazards and sequences of events leading to hazardous situations and harms; then use detailed analyses to understand failure mechanisms and confirm controls.

Common electronics-related hazard contributors

Area	Examples to consider
Electrical energy	Shock, leakage current, dielectric breakdown, unexpected current path, incorrect polarity, connector mis-mating.
Thermal and fire	Hot surfaces, battery heating, component overstress, ignition, blocked ventilation, single-fault dissipation.
Functional failure	Missed detection, false result, unintended actuation, loss of therapy, timing error, sensor drift, latent fault.
EMC and RF	Disturbance-induced reset or corruption, degraded measurement, excessive emissions, coexistence and radio blocking.

Area	Examples to consider
Power integrity	Brownout, sequencing error, corrupted non-volatile memory, unsafe restart, charger fault, depleted battery.
Data and security	Unauthorised debug access, insecure key storage, malicious firmware, tampered calibration or identity data.
Manufacturing variation	Wrong part, counterfeit component, solder defect, contamination, incorrect programming, fixture escape.
Ageing and environment	Electrolytic or battery ageing, corrosion, moisture, ESD damage, connector wear, component drift.

Risk control hierarchy

1. **Inherently safe design.** Remove or reduce the source of risk through architecture, energy limitation, isolation, component rating, physical separation or elimination of the hazardous condition.
2. **Protective measures.** Add detection, shutdown, redundancy, guards, fuses, current limiting, alarms or monitoring where risk cannot be sufficiently reduced by design alone.
3. **Information for safety.** Use labelling, instructions, service information or training only for residual risks that cannot practicably be controlled by design or protection.

Single faults and fault combinations

Analyse open circuit, short circuit, stuck-at, drift, intermittent connection, component substitution, supply reversal, wrong assembly, loss of clock, memory corruption and common-cause conditions. Do not assume a component is infallible without a justified exclusion. A protection circuit controlled by the same failing element it is intended to supervise may not provide meaningful independence.

Risk-control verification

- Verify that the control is present in the design output.
- Verify its effectiveness under specified normal and fault conditions.
- Check that the control does not introduce new hazards or unacceptable risks.
- Confirm production controls will reliably realise the safety feature.
- Maintain traceability from risk-control measure to requirement, implementation and objective test evidence.

6. Detailed electronic design considerations

6.1 Power architecture, batteries and charging

- Define all operating states, peak and average loads, startup/inrush, brownout behaviour, shutdown order and recovery from interrupted power.
- Perform worst-case power, thermal and energy-budget analyses using tolerance, temperature, ageing, firmware duty cycle and radio behaviour.
- Specify protection against overcurrent, overvoltage, undervoltage, reverse polarity, overtemperature, short circuit and inappropriate chargers.
- For batteries, address cell qualification, pack protection, state estimation, ageing, swelling, shipping, replacement, deep discharge, charging temperature and storage.
- Consider whether energy remains available long enough to enter a safe state, preserve records or communicate an alarm.

6.2 Isolation, spacing and protective earth

- Identify working voltages, transients, pollution degree, material group, altitude and insulation type before allocating creepage and clearance.
- Define means of operator and patient protection where applicable, including isolation components and their conditions of acceptability.
- Control PCB slots, coatings, barriers, transformer construction, optocouplers, connectors, fasteners and conductive contamination that affect spacing.
- Treat protective earth paths as engineered safety functions: conductor sizing, attachment, corrosion, mechanical security and production test must be controlled.

6.3 Analogue and sensor interfaces

- Budget accuracy from sensor through analogue front end, ADC, reference, calibration and algorithm; include tolerance, noise, drift, temperature and ageing.
- Define saturation, overload recovery, disconnected sensor, shorted input, common-mode range and out-of-range detection.
- Prevent diagnostic stimulation, leakage or test currents from affecting the patient, sample or measurement.
- Design calibration so coefficients, units, version, integrity and traceability are protected throughout production and service.

6.4 Digital, clocks, memory and programmable devices

- Specify reset sources, watchdog behaviour, boot state, safe GPIO defaults, clock-failure response and deterministic power-up/down states.

- Protect critical configuration and calibration data with range checking, integrity checks, versioning and controlled write mechanisms.
- Define the hardware/firmware boundary for safety-related monitoring and ensure each side has testable responsibilities.
- Control FPGA, CPLD and programmable logic source, synthesis settings, tool versions, bitstreams, programming verification and device security settings.

6.5 EMC, signal integrity and radio

- Create an EMC control plan early: enclosure, grounding, return paths, filtering, cable shielding, connector entry, ESD paths and PCB stack-up must work as a system.
- Define essential performance and observable pass/fail criteria before compliance testing. “No damage” is usually insufficient.
- Test risky circuits and cable configurations during development, including maximum cable lengths, accessories, charging and communication modes.
- For wireless functions, consider regulatory radio approval, coexistence, antenna detuning, body loading, enclosure variation, security and loss-of-link behaviour.

6.6 Component selection and derating

- Use approved manufacturers and orderable part numbers, not only generic values.
- Define voltage, current, power, temperature and environmental derating appropriate to reliability and risk.
- Review lifecycle status, change-notification terms, authenticity controls, moisture sensitivity, storage, reflow limits and alternative sources.
- For safety-critical parts, record the function, critical characteristics, approval data, tolerances and incoming or supplier controls.
- Evaluate component qualification evidence critically; automotive or industrial qualification can support reliability but does not prove medical-device suitability by itself.

6.7 Design for manufacture, assembly and test

- Design footprints, pad geometry, fiducials, panelisation, test access and programming connections with the manufacturing partner.
- Avoid hidden or ambiguous assembly orientation; make polarity and variant identification inspectable.
- Provide electrical test access for rails, communications, critical sensors and safety features without creating an uncontrolled service or security interface.

- Define cleanliness, conformal coating, staking, encapsulation, adhesives and underfill only with compatible, validated processes and inspection criteria.
- Plan serialisation and traceability for PCB, PCBA, firmware, calibration data, test results and final device assembly.

6.8 Hardware cybersecurity

- Disable or control debug and programming interfaces in released product.
- Protect device identity, cryptographic keys and secure-boot roots of trust from unauthorised readout or replacement.
- Support authenticated update and rollback control where updateable firmware is used.
- Define tamper response, service access, manufacturing provisioning and recovery processes.
- Treat component and production-programming supply chains as part of the threat model.

7. Design outputs and configuration control

Design outputs are the controlled specifications from which the device can be manufactured, inspected, programmed, calibrated, tested, serviced and maintained. They must be sufficiently complete for a competent person or supplier to reproduce the intended design without relying on undocumented project knowledge.

Minimum controlled electronics package

Output group	Typical controlled content
Architecture and descriptions	Block diagrams, power tree, safety concept, grounding/isolation, interfaces, modes, diagnostics and rationale.
Circuit design	Schematics, calculations, simulations, tolerance analyses, derating, component stress and fault analyses.
PCB definition	Layout database, fabrication drawings, stack-up, materials, impedance, panelisation, drill and manufacturing notes.
Assembly definition	Approved BOM/AVL, assembly drawings, special processes, workmanship and inspection requirements.
Programmable content	Firmware/FPGA identifiers, bootloader, configuration bits, keys/certificates, programming files and checksums.

Output group	Typical controlled content
Test and calibration	Test specifications, limits, equipment, fixture definition, software version, calibration method and data format.
Manufacturing and service	Handling, ESD, cleaning, coating, storage, repair restrictions, service tests and traceability requirements.

Configuration baseline

The verification and release baseline should uniquely identify every item needed to interpret the test result: hardware revision, BOM revision, PCB fabrication revision, assembly variant, firmware and programmable-logic version, configuration/calibration dataset, test method, fixture and test-software version. Photographs alone are not a configuration record.

GOLDEN RULE Never write “tested on the latest prototype.” Identify the exact, reproducible configuration.

8. Prototypes, reviews and design maturity

Prototype stages have different purposes

Stage	Primary purpose	Control expectation
Proof of concept	Resolve technical feasibility and major unknowns.	May use informal parts and methods, but assumptions, build state and results must be recorded; do not treat as verification evidence.
Engineering prototype	Exercise architecture, interfaces, tolerance and pre-compliance behaviour.	Controlled enough to reproduce; deviations from intended design are documented.
Design-verification unit	Generate formal evidence against approved design inputs.	Built to a released or frozen baseline using representative materials and processes; all deviations assessed.
Production-equivalent unit	Support validation, process qualification and transfer.	Representative of production tooling, suppliers, firmware, programming, calibration and inspection.

Design reviews

Reviews should occur at planned maturity points and include people with appropriate independence. A useful electronics review checks requirements coverage, safety architecture, unresolved risks, analyses, schematics, layout, BOM, DFM/DFT, verification readiness, manufacturing readiness and open anomalies. Record attendees, reviewed baselines, findings, actions, decisions and approval.

Example review gates

- **Architecture review.** Is the concept capable of meeting essential performance, safety, interfaces, power, EMC, cybersecurity and production needs?
- **Schematic review.** Are calculations, ratings, protections, component selections and fault responses complete?
- **PCB review.** Do layout, stack-up, return paths, isolation, thermal paths, test access and assembly rules realise the design intent?
- **Verification readiness review.** Are inputs approved, methods valid, samples representative, traceability complete and anomalies controlled?
- **Transfer review.** Can production build, program, calibrate, inspect, test, trace and release the device consistently?

9. Verification, validation and compliance testing

Verification versus validation

Activity	Question answered	Electronics examples
Design verification	Did the design outputs meet the design inputs?	Rail accuracy, battery endurance, sensor noise, isolation, EMC immunity, fault response, PCB inspection.
Design validation	Does the finished device meet user needs and intended use?	Representative use with production-equivalent hardware, environment, accessories, users and workflows.
Process validation	Can a process whose result cannot be fully verified later consistently produce the required result?	Coating, bonding, soldering or calibration processes where complete output verification is impractical or destructive.

A defensible verification protocol

- Approved requirement and risk-control references.
- Purpose, scope, responsibilities and configuration under test.
- Sample-size rationale and treatment of variants or worst cases.
- Equipment, calibration status, fixtures, software and environmental conditions.
- Detailed method with objective acceptance criteria defined before execution.
- Raw-data capture, calculations, uncertainty where relevant, deviations and anomaly handling.
- Clear pass/fail conclusion and review/approval.

Worst-case and margin thinking

Test the combinations most likely to challenge the requirement, not only nominal units at room temperature. Consider component tolerance, supply limits, battery age, temperature, humidity, altitude, cable length, radio state, accessory load, patient or sample impedance, manufacturing variation and software timing. Use analysis to identify worst cases and testing to confirm the analysis.

Pre-compliance before formal testing

Formal laboratory testing is expensive and scheduled late. Reduce risk through staged pre-compliance work: bench fault injection, leakage and dielectric checks, ESD probing, conducted and radiated emissions scans, immunity spot tests, thermal mapping, antenna measurements and worst-case power operation. Record results and design decisions even when the work is exploratory.

Handling failures

A failed test is not erased by a successful retest. Open an anomaly or nonconformity, investigate the cause, assess impact on risk and previous evidence, control any change, update the baseline and define the required regression. The final report should preserve the history and explain why the released configuration is acceptable.

10. Suppliers, components and obsolescence

The legal manufacturer retains responsibility for the finished device even when electronics are designed, fabricated, assembled or tested by suppliers. Supplier capability and controls must match the significance of the supplied product or service.

Supplier controls for electronics

- Define technical, quality, traceability, change-notification, record-retention and right-of-access requirements in purchasing information and quality agreements.
- Qualify PCB fabricators, EMS providers, test houses, calibration providers and safety-critical component suppliers using risk-based criteria.
- Confirm process capability for fine-pitch, BGA/LGA, selective solder, cleaning, coating, press-fit, wire processing and other relevant technologies.
- Require approval before changes to source, site, material, process, equipment, tooling, programming or test method that could affect the device.
- Monitor quality, delivery, escapes, yield, corrective actions and change notifications.

Component lifecycle and change notifications

Maintain lifecycle status and alternates for constrained or critical components. Product-change notifications and end-of-life notices require documented impact assessment, including function, risk, compliance, EMC, layout, firmware, cybersecurity, production test and existing verification. “Form-fit-function equivalent” is a supplier claim to evaluate, not an automatic approval.

Counterfeit and broker purchases

Unapproved-market sourcing increases the risk of counterfeit, reclaimed, improperly stored or untraceable parts. If exceptional sourcing is unavoidable, apply documented approval, authentication, inspection and testing proportionate to component criticality. Do not silently introduce broker parts into medical-device production.

11. Design transfer and manufacturing readiness

Design transfer converts an approved design into a stable production system. It is complete only when manufacturing can consistently build and release the correct product, and when engineering can explain the relationship between production specifications and the verified design baseline.

Transfer readiness checklist

- Released drawings, BOM/AVL, Gerbers or ODB++ data, stack-up, assembly information and variant controls.
- Approved firmware, FPGA and configuration images with secure distribution, checksums and version controls.
- Qualified suppliers and approved purchasing specifications.

- Manufacturing flow, work instructions, ESD controls, equipment and trained personnel.
- Validated special processes and qualified fixtures/test software where applicable.
- Incoming, in-process and final inspection/test plans with justified limits and sampling.
- Calibration method, standards, data integrity, traceability and acceptance criteria.
- Serialisation, lot traceability, device history/build record and nonconformity workflow.
- Pilot-build results, yield review, open issues and formally approved transfer decision.

Pilot builds

Use pilot builds to test the complete production system, not merely to obtain units. Record material lots, operators, equipment, process settings, programming, calibration, inspection results, yield, defects, rework and deviations. Investigate systemic issues before routine manufacture.

TRANSFER QUESTION Could a new approved manufacturing partner build and test the device correctly from the controlled package without relying on undocumented help from the development team?

12. Controlled manufacture of electronics

Incoming controls

- Verify identity, revision, quantity, damage, storage condition and certificates as appropriate.
- Apply risk-based inspection or supplier evidence for bare PCBs, critical components, custom magnetics, batteries, cables and safety parts.
- Control moisture-sensitive devices, shelf life, bake history, electrostatic discharge and suspect material.
- Maintain traceability to supplier lots where needed for investigation or containment.

Assembly process controls

- Control solder paste, stencil, placement program, reflow profile, selective/wave parameters, hand soldering and inspection criteria.

- Define workmanship standard and class contractually; do not assume an IPC class automatically establishes medical-device acceptance.
- Control cleaning, ionic contamination, conformal coating, masking, curing, staking, bonding and encapsulation.
- Use trained and qualified operators where workmanship or special process competence is important.
- Control repair and rework instructions, permitted cycles, inspection and traceability.

Programming and provisioning

- Release programming files and configuration data through the same change system as other design outputs.
- Verify programmed content using identifiers, checksums, read-back or cryptographic verification as appropriate.
- Protect keys, certificates, serial numbers and production credentials; separate duties and retain secure audit records.
- Prevent cross-programming of variants through fixture, barcode and software interlocks.

Production test strategy

Test layer	Purpose	Typical examples
Inspection	Detect visual and assembly defects.	AOI, X-ray, polarity, coating coverage, connector and label inspection.
In-circuit or boundary test	Detect component, connection and assembly faults.	Opens/shorts, value checks, programming, rail checks.
Functional PCBA test	Confirm board-level function and calibrate where appropriate.	Sensor simulation, communications, loads, safety monitoring, current consumption.
Final device test	Confirm integrated product and configuration before release.	Self-test, essential functions, calibration confirmation, alarms, interfaces and identity.
Safety test	Confirm unit-level safety characteristics where required.	Protective-earth continuity, dielectric strength or leakage-current tests according to the approved strategy.

Test limits and measurement systems

Production limits should be derived from design requirements and process capability, with allowance for measurement uncertainty and guard-banding where justified. Validate or qualify test methods, fixtures and software proportionate to risk. Control fixture version, maintenance, calibration, golden units, access rights and backups. Monitor false failures and false passes, not only throughput.

Traceability and release

The production record should identify what was built, from which controlled configuration and relevant material lots, using which processes and equipment, by whom, and with what results. Release must occur only after all required records are complete and accepted by authorised personnel.

13. Nonconformity, rework and production feedback

Contain first, then investigate

1. **Identify and contain.** Segregate affected material and determine the potentially affected population.
2. **Document the condition.** Record requirement, configuration, quantity, evidence and discovery point.
3. **Evaluate disposition.** Rework, repair, use-as-is, return or scrap only under authorised procedures and risk-based review.
4. **Verify the disposition.** Re-inspect or retest and retain objective evidence.
5. **Investigate trends.** Escalate recurring, systemic or safety-relevant issues into supplier corrective action or CAPA as appropriate.

Rework is a controlled process

Define allowable methods, tools, materials, temperature exposure, operator qualification, cleaning, inspection and limits on repeated rework. Assess whether rework could affect reliability, coating, pad integrity, calibration, safety spacing or evidence generated before rework. Uncontrolled “touch-up” destroys traceability and can create latent field failures.

Yield is engineering information

Track first-pass yield, failure modes, component lots, process stations and retest outcomes. A high final-pass yield can conceal excessive rework or weak test limits. Feed

manufacturing data into design risk management, supplier controls, tolerance analysis and future revisions.

14. Change control, maintenance and post-market support

Every change needs an impact assessment

Impact area	Questions
Requirements and intended use	Does the change alter function, performance, users, environment, indications, variants or accessories?
Risk	Does it affect existing hazards, risk controls, fault behaviour, cybersecurity or create new hazardous situations?
Compliance	Does it affect the standards strategy, certification, regulatory submission, radio approval or supplier conditions of acceptability?
Verification/ validation	Which analyses and tests remain valid? What regression or new evidence is required?
Manufacturing	Do BOM, drawings, programs, fixtures, processes, training, inspection, stock or rework instructions change?
Fielded product	Is retrofit, service action, customer communication, vigilance reporting or recall assessment required?

Post-market electronics responsibilities

- Support complaint and service investigations using controlled schematics, logs, test methods and failure-analysis techniques.
- Preserve returned units, configuration and chain of custody when evidence may be important.
- Trend resets, battery failures, sensor drift, charging issues, EMC susceptibility, connector damage and intermittent faults.
- Review new component safety information, supplier notices, vulnerabilities and obsolescence.
- Update the risk management file and determine whether corrective or preventive action is required.

No fault found is not a root cause

Intermittent electronics faults may disappear when a device is opened, powered differently or removed from its use environment. Investigations should consider configuration, logs, environmental exposure, accessories, charger, wireless conditions, contamination, connector wear and production history. Define what evidence would be needed to close the investigation responsibly.

15. Common failure patterns and practical checklists

Common project failure patterns

Failure pattern	Why it causes trouble	Better practice
Design starts before inputs stabilise	Architecture choices become hidden requirements and late risk controls force redesign.	Use controlled assumptions, mature inputs by gate and review architecture against risk early.
Compliance testing is treated as verification planning	The lab arrives too late to define essential performance, worst cases or measurable criteria.	Build a requirements-based verification strategy and use compliance tests as one evidence source.
Prototype evidence is reused without configuration control	The tested unit cannot be shown to represent the released device.	Define evidence purpose and record exact baseline, deviations and representativeness.
BOM substitutions are considered purchasing decisions	Electrical, EMC, safety, reliability or firmware behaviour changes without assessment.	Apply engineering change control and verification proportional to impact.
Production test is added after layout	Critical nodes are inaccessible and fixtures become fragile or intrusive.	Design for test during architecture and PCB layout.
FMEA scores replace device risk management	Hazardous situations, harms, risk-control hierarchy and benefit-risk reasoning are missed.	Link detailed failure analyses into the device-level risk process.

Failure pattern	Why it causes trouble	Better practice
Passing units are repeatedly retested	False passes and unstable processes are hidden.	Control retest rules, retain all results and investigate recurring failures.

Electronics engineer's phase checklist

At this point	Confirm before proceeding
Before architecture	Intended use, users, environments, essential performance, interfaces, markets, standards plan and preliminary hazards are understood.
Before schematic release	Requirements allocated; protection concept, calculations, fault responses, ratings, diagnostics and critical components reviewed.
Before PCB release	Stack-up, EMC, isolation, thermal, test access, DFM/DFT, variants, drawings and manufacturing notes reviewed.
Before formal verification	Inputs approved; units representative; baseline frozen; methods, samples, worst cases, equipment and acceptance criteria approved.
Before transfer	All outputs released; suppliers/processes/test systems ready; pilot evidence acceptable; open issues formally controlled.
Before change approval	Requirement, risk, compliance, evidence, manufacturing, stock and field impact assessed.

ENGINEER'S STOP SIGNAL Pause and escalate when a requested shortcut would make the tested configuration uncertain, bypass a risk control, use an unapproved component or process, obscure a failure, or release product without required objective evidence.

Appendix A. Electronics deliverables by lifecycle phase

Phase	Core electronics deliverables
Planning	Electronics development activities and responsibilities; standards inputs; supplier strategy; verification approach; configuration and tool strategy.
Inputs	Hardware requirements; interfaces; environmental, lifetime, EMC, safety, power, cybersecurity, calibration and manufacturing requirements.
Architecture	Block diagrams; safety/protection concept; power tree; partitioning; grounding/isolation; diagnostics; component technology selections; trade studies.
Detailed design	Schematics; PCB data; BOM/AVL; calculations; simulations; tolerance, derating, thermal, reliability and fault analyses; review records.
Verification	Plan, protocols, fixtures, test software, sample rationale, raw data, reports, traceability, anomalies and compliance evidence.
Transfer	Released manufacturing package; work/test/calibration instructions; process qualifications; supplier approvals; pilot build and transfer review.
Production	Build/device history records; inspection and test results; calibration; nonconformities; rework; release and yield records.
Post-market/ change	Investigation support, trend analysis, component notifications, change assessment, regression evidence and risk-file updates.

Appendix B. Commonly relevant standards and frameworks

This list is a starting point, not an applicability determination. Use the project's controlled standards process to select editions, amendments, regional adoptions and particular standards.

Topic	Common reference	Why electronics engineers care
Quality system	ISO 13485:2016; US FDA 21 CFR Part 820 QMSR	Design and development, supplier controls, production, records, nonconformity, CAPA and change control.
Risk management	ISO 14971:2019 and ISO/TR 24971	Hazards, risk estimation/evaluation, risk controls, residual risk and production/post-production feedback.

Topic	Common reference	Why electronics engineers care
Medical electrical equipment	IEC 60601-1 family and applicable particular standards	Basic safety, essential performance, electrical/thermal/mechanical protection and collateral requirements.
Laboratory/IVD equipment	IEC 61010-1 family and applicable particular standards	Safety of measurement, control and laboratory equipment, including relevant IVD analysers.
EMC	IEC 60601-1-2 or product-specific EMC standards	Emissions, immunity, essential performance and test configuration.
Home or emergency environments	IEC 60601-1-11 or IEC 60601-1-12 when applicable	Environmental, supply, mechanical and usability conditions beyond controlled facilities.
Usability	IEC 62366-1; IEC 60601-1-6 where applicable	Use-related risk, controls, user interfaces, connectors, alarms and physical interaction.
Software and cybersecurity	IEC 62304; IEC 81001-5-1; applicable regulatory cybersecurity guidance	Hardware/software interfaces, programmable content, secure boot, debug access, provisioning and update support.
PCB and assembly workmanship	IPC-2221/2222, IPC-A-600, IPC-A-610, J-STD-001 and related documents as contractually selected	PCB design/fabrication, soldering process requirements and acceptance criteria.
Batteries and transport	IEC 62133-2, UN Manual of Tests and Criteria 38.3 and product/market rules as applicable	Cell/pack safety, charging, qualification, transport and supplier evidence.
Environmental substances and waste	RoHS, REACH, WEEE and market-specific environmental law	Material declarations, restricted substances, labelling, recycling and supplier data.
Radio	Applicable regional radio and spectrum rules; coexistence guidance	Module integration, antennas, emissions, receiver performance, coexistence and approvals.

Appendix C. Glossary

Term	Meaning in this guide
AVL	Approved Vendor List: approved manufacturer/source combinations for specified components.
Basic safety	Freedom from unacceptable risk directly caused by physical hazards when equipment is used under normal and single-fault conditions, as defined in the applicable safety framework.
BOM	Bill of Materials: the controlled list of components and materials needed to build a defined configuration.
CAPA	Corrective and Preventive Action: structured investigation and action for actual or potential systemic quality problems.
Design input	Approved physical and performance requirements forming the basis for design.
Design output	Results of design work that define the device and support production, inspection, installation, servicing and acceptance.
Design transfer	Controlled conversion of design outputs into production specifications and a capable manufacturing process.
Essential performance	Performance necessary to achieve freedom from unacceptable risk, as determined for the device and applicable standard.
EMS	Electronics Manufacturing Services provider.
GSPR	General Safety and Performance Requirements in Annex I of the EU MDR or IVDR.
Objective evidence	Verifiable records, facts or data demonstrating that a requirement or process has been fulfilled.
PCBA	Printed Circuit Board Assembly.
QMS	Quality Management System.
Validation	Confirmation that requirements for a specific intended use or application have been fulfilled.
Verification	Confirmation that specified requirements have been fulfilled.

Appendix D. Authoritative starting sources

- ISO 13485:2016 — Medical devices — Quality management systems
- ISO 14971:2019 — Application of risk management to medical devices
- IEC 60601-1 — General requirements for basic safety and essential performance
- IEC 61010-1 — Safety requirements for measurement, control and laboratory equipment
- Regulation (EU) 2017/745 on medical devices
- Regulation (EU) 2017/746 on in vitro diagnostic medical devices
- FDA Quality Management System Regulation (QMSR)
- IPC J-STD-001 and IPC-A-610 revision information

CONTROLLED USE Purchase or access the authorised standards and regulatory texts needed for the project. Summaries and component certificates are supporting information, not substitutes for the applicable requirements.

Closing perspective

The electronics engineer's contribution extends far beyond schematics and PCB layout. It includes turning system and risk needs into measurable hardware requirements; designing for faults, variation, use and manufacture; generating credible verification evidence; transferring a reproducible product; and supporting that product throughout its commercial life. When these activities are integrated from the start, regulatory evidence becomes the natural output of good engineering rather than a retrospective reconstruction.