NoioMed

Technique	*Origin / Standard*	*Primary Purpose*	*ISO 14971 Phase(s)*	*Typical Outputs / Artifacts*	*Strengths*	*Limitations*	*Best-Fit Use Cases*	*Audit / Regulatory Value*
Item / System Definition	ISO 26262	Define scope, boundaries, modes	Intended use, hazard ID	System boundaries, interfaces, modes	Prevents missed hazards	Requires early rigor	Complex E/E/EP & software devices	Demonstrates completeness
Preliminary Hazard Analysis (PHA)	System Safety	Early hazard identification	Hazard ID	Initial hazard list	Fast, proactive	High-level only	Concept phase	Shows early safety thinking
HAZID	System Safety	Structured hazard brainstorming	Hazard ID	Hazard register	Simple, inclusive	Team dependent	Early reviews	Common & accepted
Scenario-Based Hazard Analysis (HARA-style)	ISO 26262	Hazard + malfunction + scenario	Hazard ID, risk analysis	Hazardous situations, sequences	Excellent context modeling	Requires discipline	Multi-use or workflow-heavy devices	Strong ISO 14971 alignment
DFMEA	AIAG / ISO	Bottom-up design failures	Risk analysis	Failure modes, effects, controls	Structured, traceable	Misses systemic hazards	Components, subsystems	Expected but insufficient alone
PFMEA	AIAG / ISO	Manufacturing/process risk	Risk analysis	Process failure risks	Strong production focus	Not design-centric	Assembly & manufacturing	Strong production evidence

UFMEA / Use-Related Risk Analysis	IEC 62366-1	Use error identification	Hazard ID, risk analysis	Use error scenarios	Mandatory for usability	User-focused only	User-facing devices	High regulatory scrutiny
Software Hazard Analysis / SFMEA	IEC 62304	Software-related hazards	Risk analysis	Software hazard list	Software focus	Needs top-down complement	Embedded & SaMD	Expected for SW devices
Fault Tree Analysis (FTA)	System Safety / ISO 26262	Top-down causal analysis	Risk analysis	Fault trees, cut sets	Identifies root causes	Needs defined top event	High-severity hazards	Very persuasive
Quantitative FTA	ISO 26262	Probability modeling	Risk analysis, residual risk	Event probabilities	Strong evidence	Data intensive	Safety-critical hazards	Exceptional credibility
Event Tree Analysis (ETA)	System Safety	Consequence modeling	Risk evaluation	Event sequences	Captures escalation	Not root-cause focused	Protective response analysis	Strong sequence clarity
Cause-Consequence Analysis (CCA)	System Safety	Combine FTA + ETA	Risk analysis	Integrated causal maps	Holistic view	Modeling effort	Complex systems	Advanced rigor
Common Cause / Dependent Failure	ISO 26262	Identify shared failures	Risk analysis	Dependency lists	Exposes hidden risks	Often overlooked	Redundant systems	Addresses auditor red flags

Analysis (CCFA / DFA)								
FMEDA	ISO 26262	Diagnostic effectiveness	Risk analysis, verification	Diagnostic coverage, failure rates	Quantifies detection	Data heavy	Sensors, actuators, alarms	Strong risk control evidence
Reliability Block Diagrams (RBD)	Functional Safety	Architecture reliability	Risk evaluation	Reliability estimates	Visual architecture logic	Simplifying assumptions	Redundancy decisions	Good design justification
Markov / State-Based Analysis	Functional Safety	Time-dependent risk	Risk analysis	State transition models	Handles repair/degraded states	Specialized skill	Maintenance-dependent devices	Advanced but credible
HAZOP	Process Safety	Deviation-based analysis	Risk analysis	Deviations, causes, effects	Very systematic	Time-intensive	Complex processes	Strong rigor signal
Sneak Circuit Analysis	System Safety	Unintended behaviors	Risk analysis	Sneak paths	Finds hidden logic	Niche	Safety-critical electronics	Niche but powerful
Functional Safety Concept (FSC)	ISO 26262	Define safety goals	Risk control option analysis	Safety goals, FS requirements	Clear intent	Formal	High-severity hazards	Excellent traceability
Technical Safety Concept (TSC)	ISO 26262	Allocate safety controls	Risk control implementation	Allocated requirements	Strong design linkage	Overhead	Complex architectures	Audit-proof design linkage

Safety Mechanism Pattern Analysis	ISO 26262	Apply proven patterns	Risk control implementation	Watchdogs, checks	Reusable knowledge	Must justify fit	Embedded systems	Strong engineering practice
Independence / Decomposition Analysis	ISO 26262	Split risk across controls	Risk control option analysis	Independence rationale	Prevents single-point failure	Independence must be proven	Dual-channel systems	Highly respected
Freedom from Interference Analysis	ISO 26262	Prevent SW cross-impact	Risk control implementation	Partitioning evidence	Essential for mixed-criticality	Architectural effort	AI / multifunction devices	Increasingly expected
Risk Graphs / Risk Matrices	ISO 14971	Risk acceptability	Risk evaluation	Risk classification	Transparent decisions	Subjective	All devices	Accepted if justified
Benefit-Risk Analysis	ISO 14971	Residual risk justification	Residual risk evaluation	Benefit-risk rationale	Enables high-risk devices	Needs strong evidence	Life-saving devices	Mandatory for high risk
Confirmation Measures (Independent Review)	ISO 26262	Verify controls	RM review, verification	Review & test records	Strong governance	Org maturity needed	Novel / high-risk tech	Excellent audit defense
Safety Case / Structured Argumentation	Functional Safety	Coherent safety argument	RM report	Claim-argument-evidence	Executive & regulatory clarity	Not mandated	Class III / novel tech	Gold-standard communication

Complaint Trending & PMS Signal Detection	ISO 14971	Detect emerging risks	Post-market	Signals, CAPAs	Lifecycle continuity	Reactive	All marketed devices	Critical compliance element