



AF 9100:2026

Aerospace Quality Management System

TECHNICAL PROFILE BOOK

Systems Engineering and Mission Assurance — Technical Application Book

AF-TP-9100-001

FIRST EDITION

30 September 2026 | English master text

Publication identity and application

Control	Publication value
Title	Systems Engineering and Mission Assurance — Technical Application Book
Document code	AF-TP-9100-001
Edition / language	FIRST EDITION / English master text
Companion edition identity	30 September 2026
Controlling source	AF 9100:2026 — FIRST EDITION — 29 September 2026
Responsible owner function	Systems engineering authority
Primary source anchors	11, C, E, F, Z
Delivery status	Prepared implementation companion. Actual approval, adoption, effectivity and operational decisions are recorded separately.

Use and document-control boundary

This companion implements the supplied AF 9100 requirement basis without changing the original standard. Its process allocation, examples, checklists and record design are authored implementation material. Actual mission or product limits, specialist procedures, permissions and genuine observations must be completed before consequential use. Applicable source minima and independent decision conditions cannot be reduced by this companion.

The printed edition date identifies the companion series; it is not evidence that later preparation, review or operational decisions occurred on that date. New support codes in this set are proposed allocations for controlled registration. Established AF-IG-9100-001, AF-FAQ-9100-001 and AF-TR-9100-001 identities are retained; earlier files, the corporate master list and ASTRA codes are not overwritten.

Equivalent combined or digital records are permitted when all required fields, relationships, authority and history remain intact. A completed PDF field or typed name is not evidence of an authenticated approval. Blank records in this delivery contain no invented applicant, signature, event or result.

Contents and reading route

Publication identity and application	2
Contents and reading route	3
1 Scope, responsibility and source priority	4
2 Technical profile and prospective parameter completion	4
3 Subject-by-subject implementation	4
4 Representative evaluation and adverse evidence	6
5 Interface records, decisions and continuing use	6
Appendix A — Controlling source and evidence	7
Source tables — complete field and decision payloads	14
Appendix B — Local implementation and release	18

Select actual scope → complete application criteria → use the applicable procedure and technical book → capture authentic evidence → evaluate every applicable condition → obtain the required independent decision. Document availability does not establish implementation or conformity.

1 Scope, responsibility and source priority

Mission concepts, requirement allocation, interfaces, lifecycle gates, hazards, reliability, models, resources and integrated handover.

Boundary	Required implementation decision
Object and route	Identify ORG, PRD, SVC, PRC, PER, SUB or CAB separately. Combined records do not merge outcomes.
Activity	Apply source technical modules by performed or retained responsibility, including relevant outsourced work.
Authority	Technical release, employer task permission, independent attestation and statutory authorization remain distinct.
Source priority	AF 9100:2026 and all compatible binding obligations control. This companion does not import ASTRA programme rules or external normative schemes.

2 Technical profile and prospective parameter completion

Mission duration; phase and mode; verification method; interface limits; mass/power/thermal/data allocations; margin convention; residual-risk authority

Parameter record	Content required before evaluating results
Identity and trigger	Stable criterion ID, source anchor, owner, actual object, phase, mode and reason it applies.
Limit or attribute	Value/range with compatible units and boundary convention, or an observable state with every essential step.
Technical basis	Actual environment, duty, consequence, derivation, qualified evidence and relevant approval.
Method and representation	Inspection, analysis, demonstration or test; method version, article/population, configuration and validity limits.
Uncertainty and decision	Corrections, model, covariance, coverage, pre-agreed rule, sample/scoring logic and hold conditions.
Authority and change	Technical and independent approvals, actual effectivity, preserved earlier basis and reopening triggers.

The fields above are completed for the actual application. A blank limit, undefined domain or unvalidated method prevents the dependent claim; the book deliberately does not invent one severity, tolerance or task threshold for unrelated applications.

3 Subject-by-subject implementation

11.1 — Mission and concept definition

Source p. 28; complete conditions reproduced in Appendix A.

Implementation record: Mission concept; scenario catalogue; boundary assumptions; success and safe-state criteria.

Application check: Map local gates to the decision content of G0-G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

11.2 — Requirements decomposition and interface control

Source p. 28; complete conditions reproduced in Appendix A.

Implementation record: Requirement allocation; interface-control documents; integration assumptions; cross-interface verification.

Application check: Map local gates to the decision content of G0-G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

11.3 — Assurance planning and lifecycle gates

Source p. 28; complete conditions reproduced in Appendix A.

Implementation record: Gate plan; review packages; decision records; conditions and verified closure.

Application check: Map local gates to the decision content of G0-G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

11.4 — Reliability, availability and maintainability

Source p. 28; complete conditions reproduced in Appendix A.

Implementation record: RAM plan; models and assumptions; test plan; field exposure; repair-time and downtime definitions.

Application check: Map local gates to the decision content of G0-G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

11.5 — Hazard analysis and assurance case

Source p. 28; complete conditions reproduced in Appendix A.

Implementation record: Assurance case; hazard log; analysis rationale; evidence index; limitations and independent challenge.

Application check: Choose methods that reveal initiating events, local and system effects, common causes, detection and failed interfaces. State probabilities only with compatible populations, exposure and supported models.

Review boundary: Unsupported critical consequence, unverified protection or unacceptable residual risk prevents dependent progression. Record each source condition separately in the linked checklist and preserve approved exclusions.

11.6 — Verification strategy and model credibility

Source p. 28; complete conditions reproduced in Appendix A.

Implementation record: Verification matrix; method-selection rationale; model-credibility dossier; approved extrapolations.

Application check: Map local gates to the decision content of G0-G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

11.7 — Technical budgets and margin management

Source p. 29; complete conditions reproduced in Appendix A.

Implementation record: Budget register; margin definitions; allocation history; uncertainty and change assessments.

Application check: Map local gates to the decision content of G0-G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

11.8 — Integrated readiness and handover

Source p. 29; complete conditions reproduced in Appendix A.

Implementation record: Integrated readiness review; handover dossier; receiving acknowledgement; long-life support arrangements.

Application check: Map local gates to the decision content of G0-G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

4 Representative evaluation and adverse evidence

Design, Systems Engineering and Lifecycle Gates

Witness or trace: Review hazards, common causes, resource budgets and assumptions. Validate models for their exact decision domain; identify where simulation cannot observe or bound an essential physical property.

Synthetic challenge: A component qualifies on the bench but the installation changes cooling and power supply. Retain only relevant unchanged evidence. Add installation-specific verification and update hazards and support instructions before an integrated-system conclusion.

Risk, Criticality, Hazards and Residual Acceptance

Witness or trace: Convert each relied-upon mitigation into a controlled requirement with an owner, acceptance condition and verification. Examine whether a human action has enough time and information to work.

Synthetic challenge: An expensive support cart is classified C0 because it is not flight hardware. Reassess actual human exposure and credible unintended movement. Use consequence rather than equipment label; require the corresponding technical review and protective evidence.

Performance, Reliability and Customer Evidence

Witness or trace: Retain formulas, units, inputs, uncertainty and known-answer checks. Apply the Technical Reports methods only within their stated assumptions; undefined denominators remain undefined.

Synthetic challenge: A service has 96% availability while some available periods produce incorrect data. Report availability and output correctness separately and investigate affected outputs. The availability measure does not prove technical validity.

5 Interface records, decisions and continuing use

Record	Required implementation purpose
AF-FR-9100-016	Design, Interfaces, Gates and Engineering Budgets
AF-FR-9100-014	Risk, Hazard, Criticality and Residual Decision
AF-FR-9100-023	Sample, Verification Campaign and Technical Report

Qualification, instance acceptance, current operating capability and independent attestation retain separate evidence and decisions. A new site, material, supplier, digital load, use environment or duty requires a relevant difference and requalification review. No previous result transfers automatically because the name is unchanged.

Appendix A — Controlling source and evidence

Source: AF 9100:2026, Aerospace Quality Management System, FIRST EDITION, 29 September 2026; supplied 131-page PDF. Source page references below locate the original publication. These excerpts are read with the complete applicable standard; local implementation sequences do not replace it.

11.1 Mission and concept definition

SOURCE p. 28 | Normative when applicable

11.1(a) The organization shall establish a mission or service concept identifying users, objectives, success criteria, operational scenarios, environments, external interfaces and constraints. Normal, degraded, emergency, maintenance and retirement states shall be considered. Assumptions about external services or operator behavior shall be explicit.

11.1(b) The concept shall define the boundary between mission success and safe behavior when mission success is no longer achievable. A system shall not be permitted to continue an unsafe action merely to preserve a mission objective. Changes to the concept shall trigger reassessment of derived requirements and evidence.

Required evidence: Mission concept; scenario catalogue; boundary assumptions; success and safe-state criteria.

11.2 Requirements decomposition and interface control

SOURCE p. 28 | Normative when applicable

11.2(a) System requirements shall be allocated to subsystems, functions, operators and external services with traceable rationale. Interfaces shall specify physical, electrical, data, timing, environmental, human and procedural characteristics as applicable.

11.2(b) The organization shall assess emergent behavior and incompatible assumptions between separately acceptable subsystems. Interface changes shall be jointly reviewed by the affected authorities. Verification of each component independently shall not be assumed to verify the integrated system.

Required evidence: Requirement allocation; interface-control documents; integration assumptions; cross-interface verification.

11.3 Assurance planning and lifecycle gates

SOURCE p. 28 | Normative when applicable

11.3(a) Programs shall define lifecycle gates with entry criteria, required evidence, accountable decision makers, independent review, open-issue rules and exit criteria. Annex C provides minimum decision content. Gate names may be adapted to the organization, but the required decisions shall remain identifiable.

11.3(b) Gate decisions shall distinguish unconditional progression, bounded conditional progression and hold. Conditions shall have owners, deadlines and limits on work permitted before closure. A schedule milestone shall not be recorded as a passed technical gate when required evidence is missing.

Required evidence: Gate plan; review packages; decision records; conditions and verified closure.

11.4 Reliability, availability and maintainability

SOURCE p. 28 | Normative when applicable

11.4(a) RAM requirements shall be derived from operational needs, exposure, consequence, support concept and applicable obligations. The organization shall state the population, mission duration, failure definition, repair boundary, confidence and statistical assumptions associated with every numerical claim.

11.4(b) Analysis shall address failure mechanisms, dependencies, common causes, wear-out, maintenance-induced failure, dormant failures and environmental stress as relevant. Predicted reliability shall be distinguished from demonstrated performance. Qualification tests shall not be interpreted as proving rare-event safety rates without a defensible statistical and engineering basis.

11.4(c) Maintainability shall consider access, diagnosis, repair errors, tools, spares, human factors and verification after intervention. Availability claims shall identify whether logistics and administrative downtime are included. Annex F provides worked methods and limits.

Required evidence: RAM plan; models and assumptions; test plan; field exposure; repair-time and downtime definitions.

11.5 Hazard analysis and assurance case

SOURCE p. 28 | Normative when applicable

11.5(a) The organization shall maintain a structured safety and mission-assurance argument proportionate to criticality. Claims shall be bounded by configuration and operational domain and supported by traceable evidence. The argument shall expose uncertainty, counter-evidence and unresolved limitations.

11.5(b) Hazard analysis shall be maintained as the design and operating context evolve. Failure-mode analysis, fault trees, scenario analysis and other methods shall be selected for the problem rather than used as paperwork substitutes. Shared resources, common software, environmental exposure and organizational dependencies shall be assessed.

Required evidence: Assurance case; hazard log; analysis rationale; evidence index; limitations and independent challenge.

11.6 Verification strategy and model credibility

SOURCE p. 28 | Normative when applicable

11.6(a) The organization shall select inspection, analysis, demonstration and testing methods capable of establishing each requirement. The selected method shall address representativeness, observability, uncertainty, test-article differences and required confidence.

11.6(b) For models and simulations, credibility shall be established for the stated decision use. Verification of implementation, validation against relevant observations, input quality, sensitivity and uncertainty shall be addressed. Extrapolation beyond the demonstrated domain shall be identified and approved with compensating evidence.

Required evidence: Verification matrix; method-selection rationale; model-credibility dossier; approved extrapolations.

11.7 Technical budgets and margin management

SOURCE p. 29 | Normative when applicable

11.7(a) The organization shall manage relevant budgets such as mass, power, thermal capacity, memory, latency, structural loads and resource consumption. Each budget shall have a baseline, allocation, margin definition, uncertainty treatment, owner and review trigger.

11.7(b) Margins shall be defined consistently so that reserve is not counted twice across subsystem and system levels. Changes that consume allocated margin shall be evaluated for cumulative effects and compatibility with qualification evidence. A positive arithmetic margin shall not substitute for a valid physical model.

Required evidence: Budget register; margin definitions; allocation history; uncertainty and change assessments.

11.8 Integrated readiness and handover

SOURCE p. 29 | Normative when applicable

11.8(a) Before operational handover, the organization shall reconcile the released configuration, validated operational procedures, support capability, training, maintenance data, open issues and contingency arrangements. The receiving organization shall acknowledge responsibilities and limitations.

11.8(b) The handover shall include information required for continued assurance and not merely delivery acceptance. Long-duration missions shall plan how evidence, expertise, spares and secure updates remain available after original project personnel or suppliers are no longer present.

Required evidence: Integrated readiness review; handover dossier; receiving acknowledgement; long-life support arrangements.

C.1 Gate governance and evidence package

SOURCE p. 54 | Normative when applicable

C.1(a) For each gate, the program shall identify the decision authority, required specialists, independence, entry criteria, evidence package and permissible outcomes. Evidence shall correspond to the reviewed configuration. A gate package shall include open issues, dissent, assumptions and the limitations of analysis or testing.

C.1(b) The decision record shall state pass, conditional progression or hold, with permitted downstream activity and conditions. Conditional progression shall not permit an irreversible action that depends on missing critical evidence. Closure shall be verified before the dependent activity occurs.

C.2 Iterative and emergency development

SOURCE p. 54 | Normative when applicable

C.2(a) Incremental delivery shall define the assurance boundary of each increment and its compatibility with existing configurations. An increment shall not rely on a future increment to make current operation safe unless operation is explicitly restricted until that future control is verified.

C.2(b) Emergency development shall preserve necessary technical authority and evidence. Compressed scheduling may change sequencing, but it shall not reclassify unknown performance as verified. Temporary deployment shall have limitations, monitoring, expiry and recovery arrangements.

E.1 Choosing an analysis method

SOURCE p. 57 | Definition, explanation or informative example; no new universal limit

E.1(a) A useful assessment begins with the decision and the system boundary. Process FMEA is appropriate for examining operation-level failure and escape mechanisms; design FMEA helps examine component or function failures; fault trees examine combinations contributing to an event; scenario analysis addresses interactions and unusual operating states. None is automatically sufficient for every system.

E.1(b) The analysis should record credible failure modes, initiating conditions, local and system effects, exposed populations, detection, mitigation, evidence and ownership. The analyst should actively seek shared dependencies and conditions that can defeat multiple safeguards. Negative evidence, uncertainty and model limitations should remain visible.

E.2 Severity-first FMEA interpretation

SOURCE p. 57 | Definition, explanation or informative example; no new universal limit

E.2(a) A priority index may help organize work, but multiplying ordinal severity, occurrence and detection scores does not create a physical risk quantity. Two rows with the same product can represent very different consequences. A serious hazard with uncertain occurrence should remain visible even when its numerical ranking is lower than a frequent cosmetic defect.

E.2(b) For example, an illustrative severity score of 10 with occurrence 1 and detection 2 produces 20, while a cosmetic issue with scores 2, 8 and 8 produces 128. The larger product does not make the cosmetic issue more safety-critical. A sensible response uses severity gates, evidence quality and explicit critical-control decisions in addition to prioritization.

E.3 Probability calculations and dependence

SOURCE p. 58 | Definition, explanation or informative example; no new universal limit

E.3(a) Consider two synthetic failure events with probabilities $P(A)=0.002$ and $P(B)=0.003$ over the same defined exposure. Under independence, the probability of either event is $1-(1-0.002)(1-0.003)=0.004994$. The probability of both is $0.002 \times 0.003 = 0.000006$. These calculations are conditional on the stated model, not measured performance.

E.3(b) Without independence, $P(A \text{ and } B)$ cannot be obtained by multiplication. The general union relation is $P(A \text{ or } B) = P(A) + P(B) - P(A \text{ and } B)$. From the given marginals alone, the intersection lies between 0 and 0.002; the union lies between 0.003 and 0.005. Shared power, common software or environmental exposure can invalidate the independent model.

Source calculation note: $(E-1) P(A \cup B) = P(A) + P(B) - P(A \cap B)$ All probabilities must refer to the same population and exposure. The equation is an identity; the independent-product approximation is an additional assumption, not part of the identity.

E.4 Common-cause sensitivity example

SOURCE p. 58 | Definition, explanation or informative example; no new universal limit

E.4(a) Assume, purely for illustration, a common-cause event has probability $q=0.001$ and causes both channels to fail. Conditional on no common cause, the channel failure probabilities are 0.002 and 0.003 and are independent. The combined loss probability is $q + (1-q) \times 0.002 \times 0.003 = 0.001005994$, much larger than 0.000006.

E.4(b) This is a sensitivity demonstration, not a validated common-cause model. It shows why a redundancy claim needs evidence about independence, common environments, implementation diversity and shared resources. A reviewer should challenge an analysis whose impressive result comes mainly from assuming every dependency

away.

E.5 Risk acceptance record and review

SOURCE p. 58 | Definition, explanation or informative example; no new universal limit

E.5(a) A defensible record states the scenario, configuration, applicable obligations, controls, evidence, uncertainty, residual risk, decision authority, operating restrictions and review trigger. Acceptance should be withdrawn or reconsidered when an assumption is violated or material counter-evidence appears.

E.5(b) The record should distinguish a technical decision from an administrative acknowledgement. “Customer informed” is not the same as “customer authorized the specific departure”, and neither can waive an applicable authority requirement. Acceptance should not be retroactively inferred from use of the product.

F.1 Exponential mission-reliability example

SOURCE p. 59 | Definition, explanation or informative example; no new universal limit

F.1(a) Assume a non-repairable item has a constant failure rate $\lambda=2 \times 10^{-5}$ per operating hour over the demonstrated domain. For mission duration t , $R(t)=\exp(-\lambda t)$. At 1,000 hours, $R=\exp(-0.02)=0.9801987$; at 5,000 hours, $R=\exp(-0.10)=0.9048374$.

F.1(b) The model requires a credible constant-rate region and a consistent failure definition. It does not describe wear-out, early failures, changing stress, systematic software defects or maintenance effects unless those phenomena are separately represented. A numerical prediction is not a confidence bound or proof of mission safety.

Source calculation note: (F-1) $R(t) = \exp(-\lambda t)$; $\lambda = 1 / \theta$ λ is the constant failure rate in h^{-1} ; t is operating time in h ; θ is the corresponding mean life or mean inter-failure interval under the applicable exponential/HPP model. λt is dimensionless.

F.2 Series and parallel systems

SOURCE p. 59 | Definition, explanation or informative example; no new universal limit

F.2(a) Three independent series elements with mission reliabilities 0.990, 0.995 and 0.998 produce system reliability $0.990 \times 0.995 \times 0.998 = 0.9830799$. Every series element is required for the modeled success event.

F.2(b) Two independent active parallel elements, each with mission reliability 0.98, give $1 - (1 - 0.98)^2 = 0.9996$ if either element alone provides the required function. This assumes perfect switching or load-sharing behavior where relevant, no common-cause failure and no harmful interaction. Annex E demonstrates how a shared failure can dominate the result.

Source calculation note: Figure F-1 — Synthetic exponential reliability curves. The three constant rates are illustrative model assumptions, not measured aircraft, vehicle or spacecraft failure rates. (F-2) $R_{\text{series}} = \prod R_i$; $R_{\text{parallel}} = 1 - \prod (1 - R_i)$ The product formulas require appropriate independence. The parallel formula also requires that any one surviving element is sufficient for the modeled mission function.

F.3 Zero-failure binomial demonstration

SOURCE p. 59 | Definition, explanation or informative example; no new universal limit

F.3(a) For n independent, identically distributed trials with all n successes, a one-sided exact lower confidence bound on the success probability is $R_L = \alpha^{1/n}$. To demonstrate R_L at least R_0 with confidence $1 - \alpha$, choose n at least $\ln(\alpha) / \ln(R_0)$ and round upward.

F.3(b) At 95% confidence and target $R_0=0.99$, $n = \text{ceil}[\ln(0.05) / \ln(0.99)] = 299$ successful trials with no failures. With 300 successes, the bound is 0.9900639. This is not a claim that the next trial is guaranteed to succeed. The confidence statement describes the coverage of the procedure under its model.

Source calculation note: (F-3) $n = \text{ceil}[\ln(\alpha) / \ln(R_0)]$; $R_L = \alpha^{1/n}$ $0 < \alpha < 1$ and $0 < R_0 < 1$. Trials must have the declared mission conditions and failure criteria. Repeated dependent trials on the same article may not provide n independent observations. Figure F-2 — Required all-success trials versus target reliability at 90% and 95% confidence. Logarithmic vertical scale; independent Bernoulli trials assumed.

F.4 Time-on-test with no failures

SOURCE p. 60 | Definition, explanation or informative example; no new universal limit

F.4(a) For a constant-rate model with total valid exposure T and zero failures, the one-sided upper rate bound is $\lambda_U = -\ln(\alpha) / T$. With $T=60,000$ item-hours and 95% confidence, $\lambda_U = 4.992887 \times 10^{-5} h^{-1}$. The corresponding lower mean-life bound is 20,028.492 hours.

F.4(b) Pooling exposure across units requires the same relevant failure mechanism and rate model. Parallel testing reduces calendar time, not the required total exposure. A 60,000-hour exposure does not mean that one article has demonstrated a 60,000-hour wear-out life.

Source calculation note: (F-4) $\lambda_U = -\ln(\alpha)/T$; $\theta_L = T/[-\ln(\alpha)]$ T is valid accumulated item-hours under a constant-rate model. Censoring and test interruptions must be recorded; excluded exposure requires a justified rule established before analysis.

F.5 Time-on-test with observed failures

SOURCE p. 60 | Definition, explanation or informative example; no new universal limit

F.5(a) For a fixed-time Poisson/HPP assessment with r observed failures and exposure T , a one-sided upper rate bound is $\chi^2(1-\alpha; 2r+2)/(2T)$. With $r=3$, $T=100,000$ hours and 95% confidence, the upper bound is $7.753657 \times 10^{-5} \text{ h}^{-1}$. The corresponding lower mean interval is approximately 12,897 hours.

F.5(b) The test plan and failure classification should be fixed before observing outcomes. Deleting early failures or treating repaired versions as unchanged units can invalidate the claim. If the rate changes over time, a reliability-growth or other suitable model is needed instead of mechanically applying this expression.

Source calculation note: (F-5) $\lambda_U = \chi^2(1-\alpha; 2r+2) / (2T)$ $\chi^2(p; v)$ denotes the lower-tail p quantile of a chi-square distribution with v degrees of freedom. This notation avoids the ambiguity between upper-tail and lower-tail tables.

F.6 Weibull life and B10 example

SOURCE p. 60 | Definition, explanation or informative example; no new universal limit

F.6(a) For an illustrative two-parameter Weibull model with shape $\beta=1.5$ and scale $\eta=10,000$ hours, $R(t)=\exp[-(t/\eta)^\beta]$. At 5,000 hours, reliability is 0.7021885. The B10 life, where 10% of the modeled population has failed, is $\eta[-\ln(0.9)]^{1/\beta}=2,230.755$ hours.

F.6(b) The example parameters are assumed, not fitted. In an actual program, estimation should address censoring, sample representativeness, uncertainty and mechanism validity. A B10 point estimate without a confidence bound may be insufficient for a life-limit decision. Extrapolating accelerated tests requires a validated acceleration relationship.

Source calculation note: (F-6) $R(t) = \exp[-(t/\eta)^\beta]$; $B_p = \eta[-\ln(1-p)]^{1/\beta}$ η has units of time; β is dimensionless; p is the cumulative failed fraction. The two-parameter model assumes zero location parameter.

F.7 Availability and repair boundaries

SOURCE p. 61 | Definition, explanation or informative example; no new universal limit

F.7(a) For an ideal alternating failure/repair model, intrinsic availability is $A_i = \text{MTBF}/(\text{MTBF} + \text{MTTR})$. With $\text{MTBF}=1,200$ hours and mean active repair time 6 hours, $A_i=0.9950249$, or 99.50249%. This excludes logistics and administrative delay.

F.7(b) For observed operational availability, a synthetic record of 960 available hours and 40 unavailable hours gives $A_o = 960/(960+40)=0.96$, or 96%. The two values are not contradictory: their downtime boundaries differ. Reports should state whether scheduled maintenance, spares waiting, software recovery and external-service outages are included.

Source calculation note: (F-7) $A_i = \text{MTBF}/(\text{MTBF} + \text{MTTR})$; $A_o = \text{uptime}/(\text{uptime} + \text{downtime})$ Use consistent time units and an explicitly defined observation window. Availability does not imply that all operations performed while available are safe or successful.

F.8 Evidence checklist for reliability claims

SOURCE p. 61 | Definition, explanation or informative example; no new universal limit

F.8(a) A reliability report should state the failure definition, mission profile, population, configuration, exposure, censoring, independence assumptions, model choice, parameter estimation, confidence level and sensitivity. It should distinguish analysis, demonstration, qualification and field observation.

F.8(b) Before accepting a claim, the reviewer should ask whether common causes, software/systematic failures, environmental changes, repair effects and selection bias are represented. Confidence arithmetic cannot rescue an invalid physical or sampling model.

Z.1 Metric definitions and numerical examples

SOURCE p. 101 | Definition, explanation or informative example; no new universal limit

Z.1(a) Each measure should have an owner, purpose, denominator, data source, reporting window, inclusion/exclusion rule and action threshold. Targets should be set before reporting. A favorable operational metric does not compensate for a mandatory conformity failure.

Z.1(b) The following examples are independent unless a shared dataset is explicitly stated. They should not be combined into a single invented organization's performance score.

Z.2 Margin definitions and reserve double counting

SOURCE p. 101 | Definition, explanation or informative example; no new universal limit

Z.2(a) Assume an available power capacity of 5.0 kW and a predicted demand of 4.0 kW for a stated condition. Margin relative to demand is $(5.0 - 4.0) / 4.0 = 25\%$. Unused fraction of available capacity is $(5.0 - 4.0) / 5.0 = 20\%$. Both calculations are correct but use different denominators.

Z.2(b) The budget should define which convention is used and whether uncertainty, degradation, contingency and reserve have already been included. Allocating the same reserve independently to multiple subsystems can overstate system margin. Simultaneous peak and transient conditions may require a separate assessment.

Source calculation note: (Z-1) $\text{Margin_relative_to_demand} = (\text{capacity} - \text{demand}) / \text{demand}$ Use the same physical quantity and compatible units. A nominal positive margin is not sufficient when the prediction uncertainty or unmodeled transients can consume it.

Z.3 Mission-support energy example

SOURCE p. 101 | Definition, explanation or informative example; no new universal limit

Z.3(a) Assume a non-flight mobile support unit has nominal stored energy 6.0 kWh. A predefined usable fraction of 0.80 already includes the chosen state-of-charge reserve; a condition factor of 0.85 and conversion efficiency of 0.90 are also assumed. Usable delivered energy is $6.0 \times 0.80 \times 0.85 \times 0.90 = 3.672$ kWh.

Z.3(b) If average loads are 0.72 kW propulsion, 0.18 kW computing and 0.10 kW auxiliaries, total average demand is 1.00 kW and the simplified endurance estimate is 3.672 hours. This does not demonstrate peak-power capability, thermal safety, terrain performance or battery life. The reserve shall not be deducted a second time without explaining the changed convention.

Source calculation note: (Z-2) $t_{\text{est}} = E_{\text{nominal}} \times f_{\text{usable}} \times f_{\text{condition}} \times \eta / P_{\text{average}}$ Energy in kWh divided by power in kW gives hours. The factors are assumptions for a simplified budget and require validation for a real mission.

Z.4 Generic structural-margin arithmetic

SOURCE p. 102 | Definition, explanation or informative example; no new universal limit

Z.4(a) For a purely illustrative uniaxial calculation, assume a nominal stress demand of 80 MPa, a separately justified load factor of 1.5 and an applicable allowable of 150 MPa. Factored demand is 120 MPa and the arithmetic margin is $150 / 120 - 1 = 0.25$.

Z.4(b) These assumed numbers are not material properties or approved factors. The example does not address multiaxial stress, fatigue, buckling, joints, defects, temperature, scatter or load-path validity. A real structural decision requires the applicable design basis and competent analysis; this calculation only demonstrates an explicit margin convention.

Source calculation note: (Z-3) $MS = \text{allowable} / \text{factored_demand} - 1$ Allowable and demand must refer to the same failure mode, units and condition. Avoid applying the same safety factor twice or omitting it through inconsistent definitions.

Z.5 Integrated ground-support case and release decision

SOURCE p. 102 | Definition, explanation or informative example; no new universal limit

Z.5(a) The synthetic ground-support cart used in Annexes B, D and W illustrates an end-to-end evidence chain. The organization defines the handling task and exposure, classifies the motion-control function, allocates requirements, approves suppliers, qualifies the process and verifies the actual hardware/software configuration.

Z.5(b) Before release, it checks dimensional acceptance using a pre-agreed decision rule, verifies the stop and control functions against the program-specific safety basis, assesses energy assumptions, closes the fixture-offset corrective action and validates operator handover. An AI inspection aid is restricted when its separate challenge-set performance is inadequate.

Z.5(c) The final release decision is requirement-based. Good OEE, a positive energy budget or a high aggregate inspection accuracy cannot compensate for missing safety verification, an unresolved configuration mismatch or

an unapproved critical characteristic. The released dossier states the exact operating boundary and remaining support obligations.

Z.6 Calculation reproducibility and verification limits

SOURCE p. 102 | Definition, explanation or informative example; no new universal limit

Z.6(a) The accompanying calculation package contains deterministic synthetic data, formula implementations, computed results and figure-generation code. Arithmetic assertions check selected identities, confidence/sample-size behavior and consistency of results. This is computational verification, not independent engineering validation.

Z.6(b) Before using a method operationally, the organization should verify the implementation, software environment, input provenance, units, numerical precision and applicability assumptions. Successful arithmetic checks do not replace competent review of applicability, assumptions and operational use.

Source tables — complete field and decision payloads

Table C-1 — Lifecycle transition requirements

Source p. 54 | Required structure when applicable

Gate	Required evidence before decision	Exit condition
G0 — Concept and feasibility	User need; intended domain; candidate architecture; initial hazards; applicable obligations; technology gaps; support concept.	The mission is defined, feasibility gaps are owned and unacceptable concepts are eliminated or bounded.
G1 — Requirements baseline	Traceable requirements; acceptance methods; interfaces; special requirements; constraints; initial assurance allocation.	Requirements are coherent and verifiable; open assumptions cannot invalidate the next work stage.
G2 — Architecture and preliminary design	Allocated functions; hazard controls; budgets; supplier strategy; model assumptions; planned V&V; independence.	Architecture plausibly satisfies requirements and critical assumptions have a verification path.
G3 — Detailed design release	Controlled design outputs; analyses; software architecture; process and material suitability; updated hazards; interface agreement.	Design data are sufficient for controlled realization; required reviews and approvals are complete.
G4 — Manufacturing or service readiness	Qualified processes; competent personnel; equipment; work instructions; inspection methods; source approvals; traceability.	The actual route can produce or perform the defined output with valid acceptance evidence.
G5 — Test and integration readiness	Test configuration; procedures; instrumentation; uncertainty; safety arrangements; acceptance criteria; anomaly rules.	The test or integration can proceed safely and produce interpretable evidence for the intended claims.
G6 — Qualification and operational readiness	Verification results; validation; configuration reconciliation; resolved anomalies; training; support; contingency capability.	Required performance and controls are demonstrated for the approved domain; limitations are accepted by authorized parties.
G7 — Delivery or deployment	Acceptance dossier; authorized deviations; life status; software manifest; required documentation; release checklist.	All release-blocking obligations are closed and the receiving party has the necessary information.
G8 — Change or life extension	Current condition; field evidence; changed requirements; remaining life; impact analysis; requalification and support.	Continued or modified use is justified for a bounded configuration and period; unsupported assumptions are not carried forward.
G9 — Retirement and disposal	Isolation plan; hazardous inventory; reuse restrictions; disposal route; sensitive data; records and remaining-user support.	Disposition is verified and remaining obligations have an owner and accessible evidence.

Table C-2 — Minimum gate-decision record

Source p. 54 | Required structure when applicable

Field	Required content
Identity	Program, gate, date, reviewed configuration, evidence-package version.
Participants	Decision authority, technical reviewers, independent reviewer and conflicts of interest.
Criteria	Entry and exit criteria, status against each criterion and evidence references.
Open matters	Issues, assumptions, risk decisions, dissent and required external approvals.
Decision	Pass, conditional progression or hold; exact activities permitted or prohibited.
Conditions	Owner, due date, verification method, dependent activity and escalation trigger.
Closure	Evidence of completion, independent verification where required, and authority to release the dependency.

Table E-1 — Minimum useful hazard-log content

Source p. 57 | Illustrative or explanatory source table

Record element	Purpose and example
Identity and configuration	H-GSC-02; ground-support cart GSC-004; configuration baseline CB-03.
Scenario and phase	Unintended movement during payload handling while personnel are in the access zone.
Initiating conditions	Incorrect command, stale state information, control failure or maintenance misconfiguration.
Consequences and exposure	Potential personnel injury and payload damage; exposure depends on task and exclusion-zone effectiveness.
Existing controls	Physical access control, motion authorization, stop function, operator procedure; each linked to a requirement.
Likelihood basis	Relevant field data or analysis with conditions and uncertainty; “unlikely” without evidence is not a quantitative estimate.
Verification and evidence	Test case, representative load, software version, independent review and anomaly disposition.
Residual decision	Named authority; accepted operating boundary; unresolved limitations; monitoring and review date.
Change triggers	Software, payload, speed, terrain, access zone, operator procedure or failure evidence changes.

Table E-2 — Filled illustrative FMEA extract

Source p. 57 | Illustrative or explanatory source table

Failure / effect	Occurrence control	Escape control and evidence	Decision
Incorrect controller version / motion behavior differs from validated baseline.	Signed release manifest and controlled installation; prevent unauthorized update.	Read-back version/hash and functional verification at deployment.	Hold release until identity is reconciled; review actual installed population.
Measurement bias / nonconforming dimension accepted.	Calibration, temperature control and validated method.	Uncertainty-aware decision rule; independent check of affected interval.	Assess prior accepted output; recalibration alone does not close the event.

Failure / effect	Occurrence control	Escape control and evidence	Decision
Supplier material substitution / hidden strength or environmental mismatch.	Approved source and change notification; controlled specification.	Identity and certificate validation plus risk-based confirmatory testing.	Obtain design-authority disposition; no automatic equivalence.
Scratched non-functional label / reduced readability.	Handling improvements and suitable label material.	Visual criterion and readability check.	Correct according to actual function; escalate if identification or warnings are impaired.

Table F-1 — Calculated zero-failure sample sizes at 95% confidence

Source p. 60 | Illustrative or explanatory source table

Target success probability R_0	Required all-success trials	Interpretation
0.9000	29	A modest target still requires independent representative trials.
0.9500	59	Zero observed failures is not the same as zero true failure probability.
0.9900	299	Useful illustrative demonstration level; not an AF safety target.
0.9990	2,995	Sample burden grows rapidly as the target approaches one.
0.9999	29,956	Rare-event assurance normally requires broader engineering evidence, not a small test campaign.

Table Z-1 — Calculated quality and delivery metrics

Source p. 101 | Illustrative or explanatory source table

Metric	Definition and synthetic inputs	Calculated result / limit
First-pass yield	940 units accepted without rework out of 1,000 entering the defined process.	$940/1,000 = 94.0000\%$.
Rolled throughput yield	Three sequential stage yields 0.98, 0.97 and 0.99, using compatible conditional stage definitions.	$0.98 \times 0.97 \times 0.99 = 94.1094\%$; not the arithmetic average.
On-time delivery	92 of 100 orders due in the period delivered in full by the agreed date; cancellation/partial rules fixed.	92.0000%; denominator is due orders, not only shipped orders.
Defective units per million	7 nonconforming units out of 20,000 inspected units; each unit counted once.	350 ppm; do not confuse units with number of individual defects.
Cost of poor quality	Scrap 18,000 + rework 12,000 + returns 9,000 + failure investigation 6,000 monetary units.	45,000; 3.0000% of an illustrative 1,500,000 revenue base.
Overall equipment effectiveness	Availability 0.90 × performance 0.95 × quality 0.98 under defined time and ideal-rate boundaries.	83.7900%; does not establish safe or conforming operation.

Metric	Definition and synthetic inputs	Calculated result / limit
Earned-value cost index	Earned value 180,000 / actual cost 200,000.	CPI = 0.9000; financial progress is not technical readiness.
Earned-value schedule index	Earned value 180,000 / planned value 225,000.	SPI = 0.8000; does not measure calendar delay directly.
Evidence completion	Verified applicable requirement records / all applicable requirement records.	Report critical missing records separately; no aggregate conformity pass.
Corrective-action effectiveness	Actions meeting their pre-defined effectiveness test / actions evaluated.	State evaluation exposure; "closed on time" is a different measure.

Table Z-2 — Integrated case decision chain

Source p. 102 | Illustrative or explanatory source table

Decision	Evidence used	What is not inferred
Define scope and category	Annex A activity matrix; Annex B hazard-based category.	No automatic equivalence to an external safety-integrity level.
Control design and configuration	Requirements and interface records; Annex D trace chain.	No assumption that a model matches the physical item without reconciliation.
Establish production capability	Annexes J-L supplier, first article and special- process evidence.	One conforming first article does not guarantee every later unit.
Evaluate numerical evidence	Annexes F-I calculations and valid actual program tests.	Synthetic examples are not test results for the cart.
Control digital functions	Annexes N-O release cards, model limits and security/update evidence.	High accuracy or a secure update alone does not prove system safety.
Resolve a detected defect	Annex W occurrence/escape causes and effectiveness evidence.	Recalibration alone does not resolve earlier product impact.
Authorize release	Clause 8.6 and Annex V requirement-based evidence review.	No score-based compensation and no invented statutory approval.

Appendix B — Local implementation and release

Readiness condition	Evidence before consequential use
Authority and responsibility	Actual legal operator, owner, competent technical authority, independent reviewer and permitted result class are recorded.
Scope and criteria	Object, configuration, site, period, trigger, every technical value or observable attribute, units and prospective approval are complete.
Evidence and methods	Original accessible evidence, representative observations, valid methods, uncertainty, adverse cases and limitations support the intended conclusion.
People and independence	Competence is current for each task; genuine conflicts, relevant prior work and needed separation have been checked.
Records and tools	Field meanings, unique IDs, original history, access, retention, recovery and actual deployed workflows have passed local validation.
Decision and public use	All relevant blockers are resolved; required independent decision and written permissions precede the exact public claim.
Continuity and handover	Receiving custody, unresolved duties, corrections and historical decisions survive transfer, retirement or provider closure.

Record the completed local readiness and actual authorization in AF-FR-9100-032 or an equivalent controlled record. Preserve the unchanged source standard and each earlier decision basis. A blocked activity may continue only within a genuinely permitted development boundary, not as a provisional conformity certificate.