Chapter Outline

Fault Hazards and Safety Assessment

Chapter 7 Health Management and Safety Assessment

7.1 Health Management Fundamentals

7.2 Unified Fault Modeling

7.3 Safety Reinforcement and Fault Data

7.4 Fault Hazards and Safety Assessment

7.5 Diagnosis and Prognostics

7.6 Safety Decisions and Improvement

7.7 Fault Injection Interfaces

7.8 Experiments and Validation

7.9 Exercises and Classroom Discussion

4 Units in This Section

7.4.1 Scenarios and Hazards

Textbook: Sec. 7.1.2.2, 7.1.2.4

7.4.2 Safety Analysis Methods

Textbook: Sec. 7.1.2.2, 7.1.2.4

7.4.3 Reliability and Mission Metrics

Textbook: Sec. 7.1.2.4

7.4.4 Risk Ranking and Design Improvement

Textbook: Sec. 7.1.5.3, 7.1.2.5

7.4.1 Scenarios and Hazards: Health and Safety

Stable Flight, Mission Capability, and Acceptable Risk

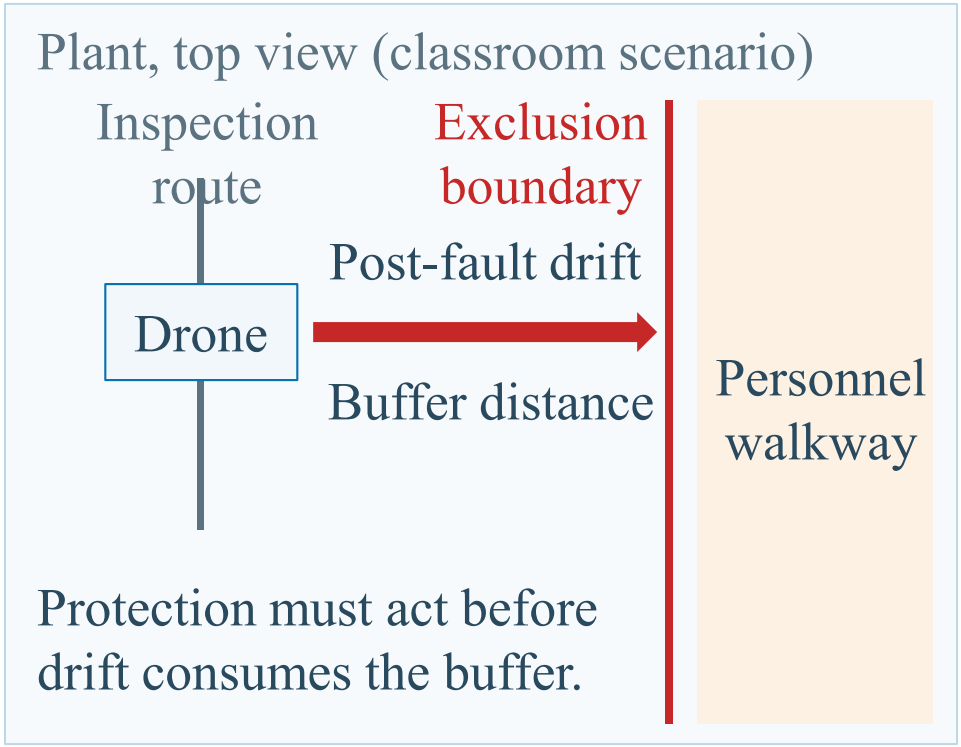
Running case: one motor falls to 70% effectiveness; other conditions stay fixed. See Section 7.1 for health versus safety.

Judgment	What to examine	Inspection example
Health	Departure from normal component state or performance	Motor effectiveness falls; compensation may mask abnormal motion
Mission capability	Can acceptable inspection results be obtained within constraints?	Hold the path, image the target clearly, and return
Safety	Is risk to people, equipment, and environment acceptable?	Could deviation or landing injure people or damage facilities?

Fault severity describes a component; hazard severity also depends on mission and environment.

7.4.1 Scenarios and Hazards: Operating Scenarios

The Same Thrust Loss Has Different Consequences



Open test field

Effect: path error/abort; controlled landing possible.

Needs: exclusion zone, level landing site, remaining thrust.

Personnel walkway at a plant

Effects: occupied-area entry; collision risk.

Needs: people's positions, buffer, warning/response delay.

Near power-transmission facilities

Effects: collision damage, secondary impacts.

Needs: facility clearance, wind, positioning/avoidance capability.

Compare fault, scenario, flight phase, and protection conditions before/after improvement.

7.4.1 Scenarios and Hazards: Environmental Exposure

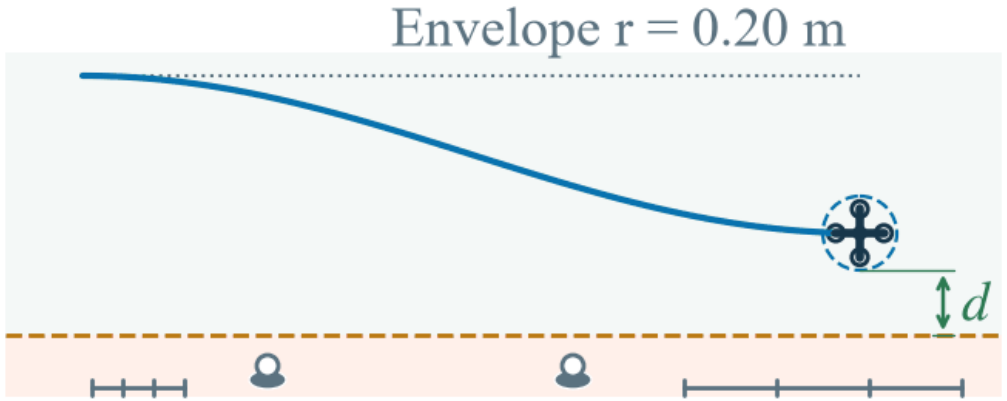
The Same Drift Trajectory Enters Different Exposure Zones

Same fault/drift; only exposure boundaries change. Values: body-envelope clearance.

Same deviation path, different exposure

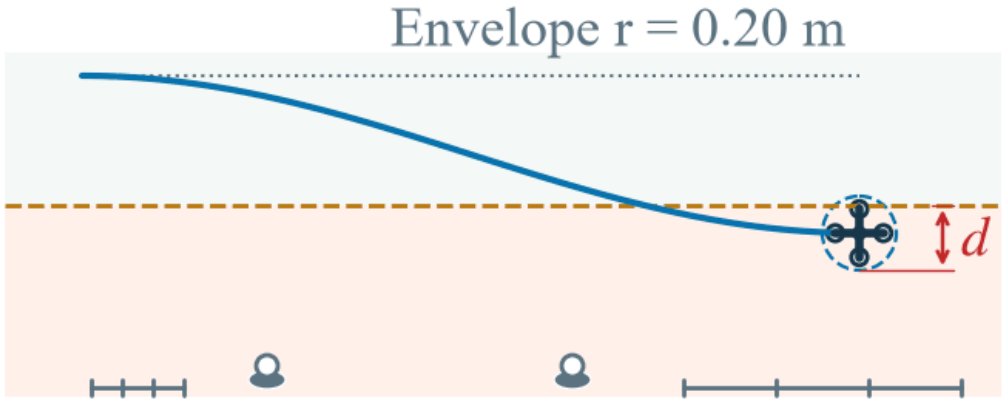
$t = 6.0$ s

Open, isolated area



Outside exposure zone +0.35 m

Passage beside obstacles



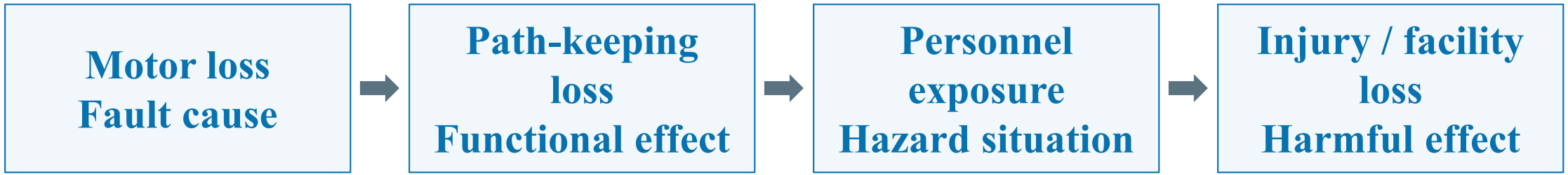
Exposure-zone entry -0.35 m

d is envelope clearance; negative values indicate exposure-zone entry

Negative clearance means entry into the exposure zone, not an observed collision.

7.4.1 Scenarios and Hazards: Expressing Risk

Faults Lead to Hazards Through Functional Failure and Exposure



$$\text{Risk} = \text{Probability} \times \text{Severity}$$

Textbook Eq. (7.1)

- **Quantified consequence:** probability is dimensionless. With severity in monetary loss, the product is expected loss for the event.
- **Empirical categories:** when severity is ordinal, the product supports ranking only.

- **Specify event, period, and units:** e.g., boundary crossing per mission or component failure per hour.

7.4.1 Scenarios and Hazards: Scope of Aviation Classifications

Development Assurance Levels Specify Process Rigor

Development Assurance Level (DAL): development and verification rigor assigned according to failure consequences.

Consequence	Probability / flight h	DAL	Consequence
Catastrophic	$<10^{-9}$	DAL A	May cause an accident or major casualties
Hazardous	$<10^{-7}$	DAL B	Severely reduced safety margins; occupant injury
Major	$<10^{-5}$	DAL C	May interrupt the mission or cause ground damage
Minor / no safety effect	$<10^{-3}$ or qualitative (D)	DAL D / E	Minor effects; no probability limit for E

Transport-airplane context: AC 25.1309-1B. UAV objectives depend on the operation.

7.4.1 Scenarios and Hazards: Adaptation to Unmanned Systems

Risk Objectives Depend on the Specific Operation

Set the scenario, event, and applicable basis. Specific Operations Risk Assessment (SORA) uses the operating concept to assess ground/air risk and set protection/evidence needs.

Application examples	Example max. rate / flight h	Operating context
Photography / leisure	$10^{-3}\ \mathrm{h}^{-1}$	Low-risk scenarios
Industrial inspection	$10^{-4}\ \mathrm{h}^{-1}$	Payload / duration demands
Urban logistics	$10^{-5}\ \mathrm{h}^{-1}$	Low altitude over populated areas
Large / military	$10^{-7}\ \mathrm{h}^{-1}$	High safety requirements

As low as reasonably practicable (ALARP): keep reducing risk where reasonably practicable, balancing reduction against time, cost, and difficulty.

Chapter Outline

Fault Hazards and Safety Assessment

Chapter 7 Health Management and Safety Assessment

7.1 Health Management Fundamentals

7.2 Unified Fault Modeling

7.3 Safety Reinforcement and Fault Data

7.4 Fault Hazards and Safety Assessment

7.5 Diagnosis and Prognostics

7.6 Safety Decisions and Improvement

7.7 Fault Injection Interfaces

7.8 Experiments and Validation

7.9 Exercises and Classroom Discussion

4 Units in This Section

7.4.1 Scenarios and Hazards

Textbook: Sec. 7.1.2.2, 7.1.2.4

7.4.2 Safety Analysis Methods

Textbook: Sec. 7.1.2.2, 7.1.2.4

7.4.3 Reliability and Mission Metrics

Textbook: Sec. 7.1.2.4

7.4.4 Risk Ranking and Design Improvement

Textbook: Sec. 7.1.5.3, 7.1.2.5

7.4 Fault Hazards and Safety Assessment

7.4.2 Safety Analysis Methods: Safety Design Process

Safety Requirements Are Checked Through Decomposition and Integration

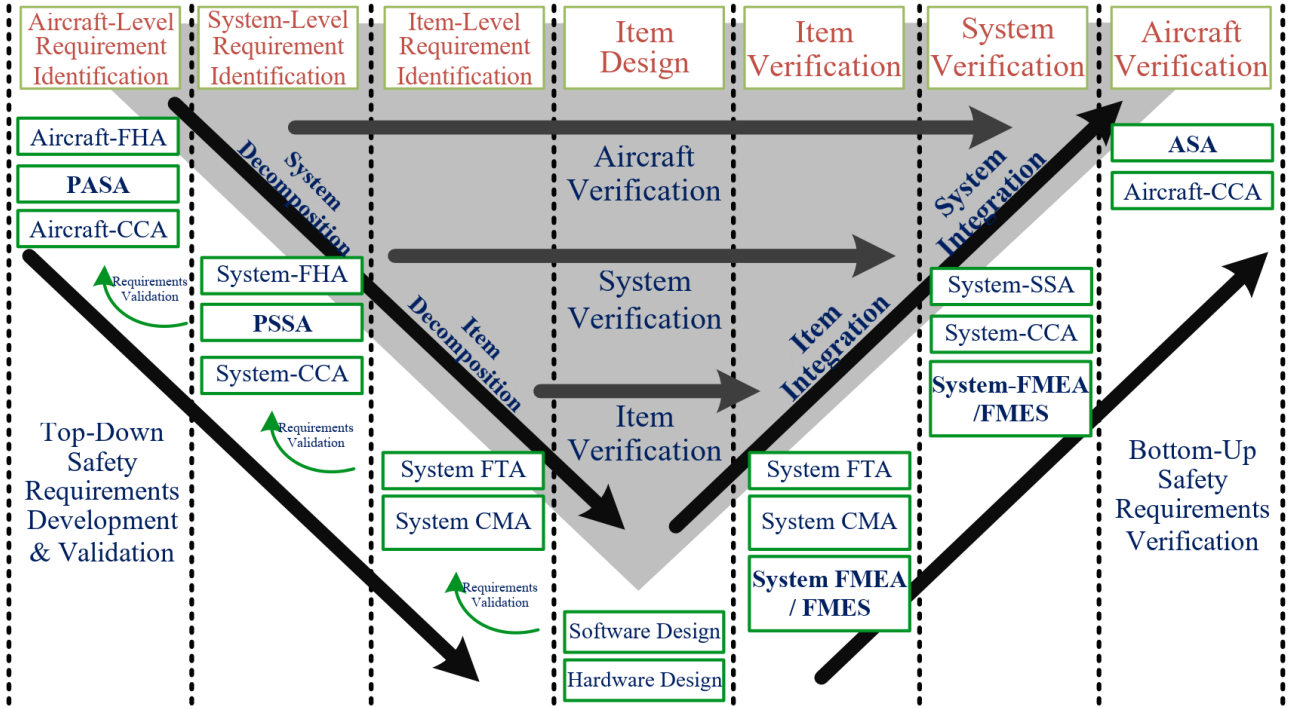
FHA: functional hazard assessment

PASA: preliminary aircraft safety assessment

CCA: common cause analysis

FTA: fault tree analysis

CMA: common mode analysis



FMEA: failure mode and effects analysis

FMES: failure modes and effects summary

SSA: system safety assessment

ASA: aircraft safety assessment

PSSA: preliminary system safety assessment

Fig. 7.2 Safety design process for manned aircraft

Green boxes: safety analyses. Left: requirements down; right: integration/verification up.

7.4.2 Safety Analysis Methods: Identifying and Validating Requirements

Functional Consequences Drive Safety Requirements

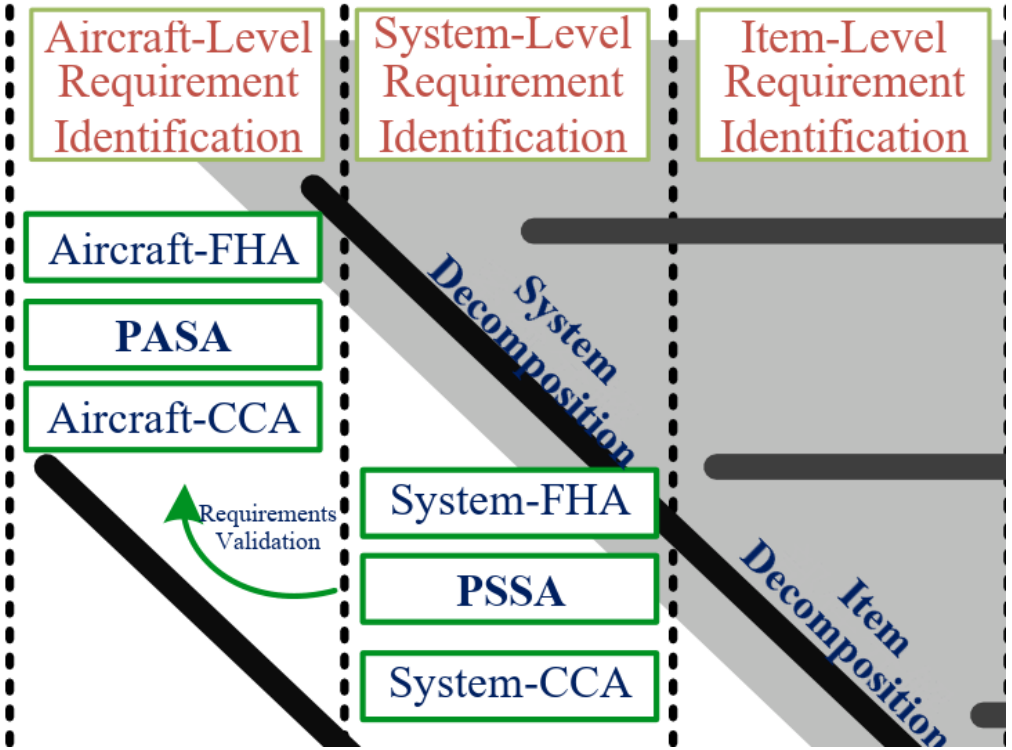


Fig. 7.2, requirements side

Functional hazard assessment (FHA): derive safety objectives from functional consequences.

Preliminary aircraft safety assessment (PASA): check early risk allocation.

System level: preliminary system safety assessment (PSSA).

Common cause analysis (CCA): trace sources that can defeat several channels at once.

7.4.2 Safety Analysis Methods: Component Design and Analysis

Implementation Requires Propagation and Independence Checks

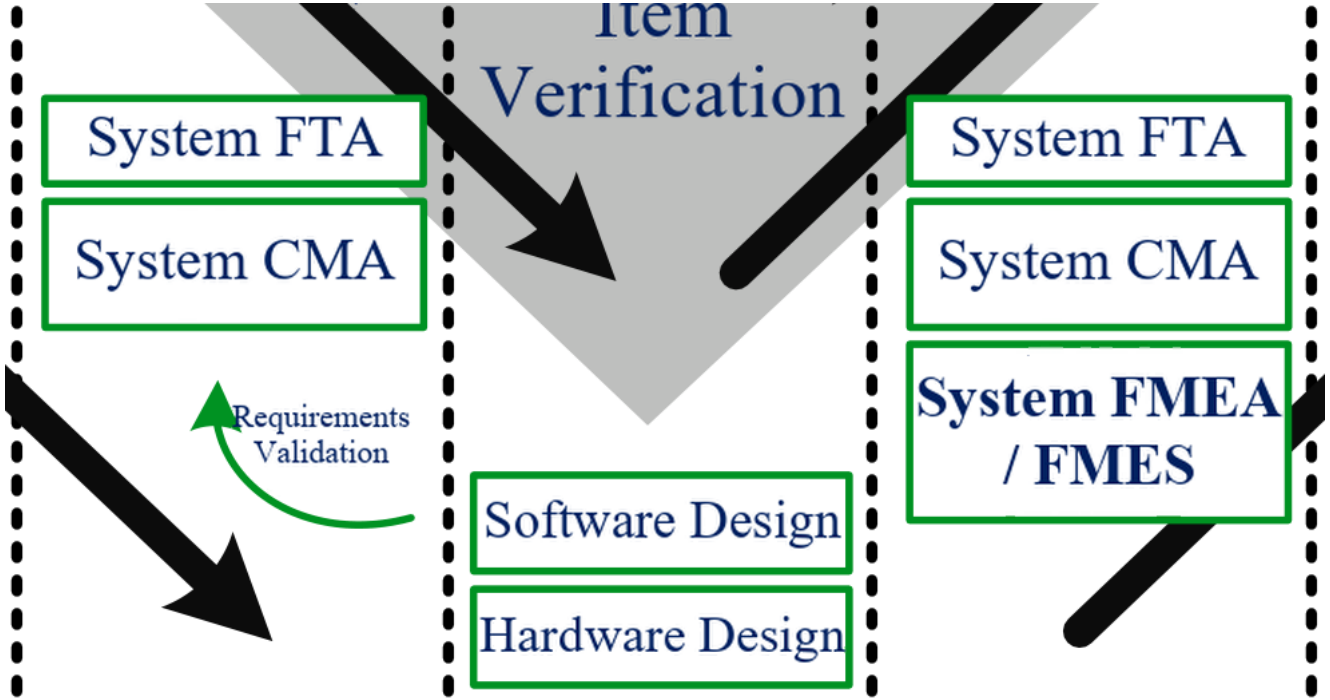


Fig. 7.2, implementation side

Fault tree analysis (FTA): expand a top-level hazard into event combinations.

Common mode analysis (CMA): check independence of redundant channels.

Failure mode and effects analysis (FMEA): trace component failures to system effects.

Failure modes and effects summary (FMES): provide summarized results to higher levels.

7.4.2 Safety Analysis Methods: Integration and Verification

Verification Returns to System and Aircraft Safety Objectives

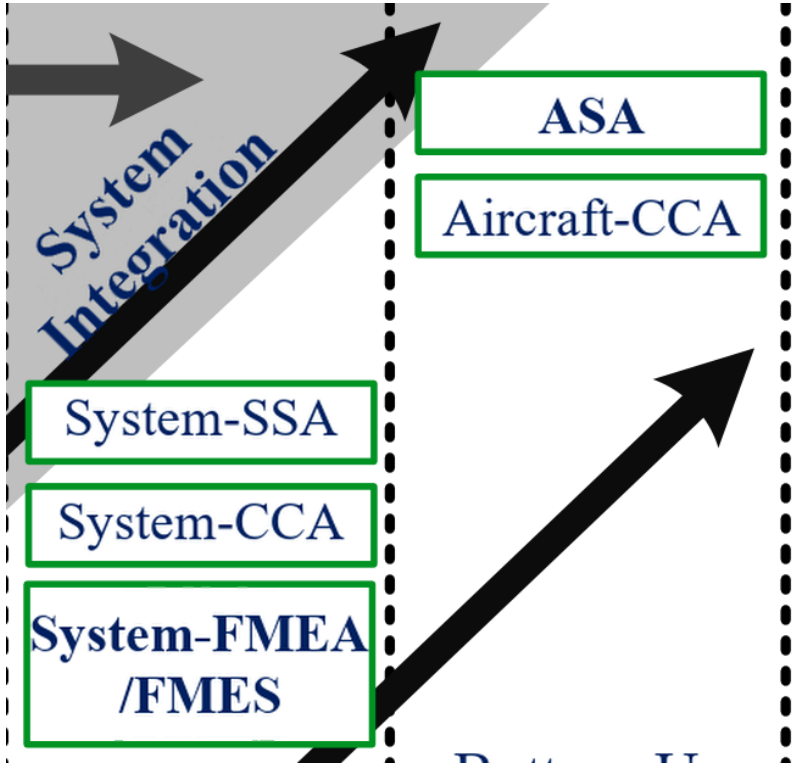


Fig. 7.2, verification side

System safety assessment (SSA): check system objectives using architecture, probability, and test evidence.

Aircraft safety assessment (ASA): review interactions in the integrated aircraft.

Inspection application: check protection actions, separation distance, and remaining whole-vehicle capability.

7.4.2 Safety Analysis Methods: Connecting the Methods

Three Analyses Answer Three Specific Questions

Method / flow	Inspection input	Reviewable result
FHA **Function → effect**	Loss of path keeping; personnel exposure at a plant	Boundary-crossing hazard, separation and response requirements
FMEA **Component → system**	Single-motor effectiveness loss; monitoring and control capability	Local/mission effects, measures, responsible owner
FTA **Top event → combinations**	Top event: crossing the personnel exclusion boundary	Separate paths, event combinations, common causes, weak barriers

Analysis turns hazards into testable design requirements.

7.4.2 Safety Analysis Methods: Functional Hazard Assessment

Look for Loss, Error, and Unintended Activation

Fixed scenario: inspection along a plant edge beside a personnel walkway. Function: keep the flight path inside the exclusion boundary.

Failure mode	Credible consequence	Safety requirement
Loss of path keeping	Lateral drift may enter the personnel walkway	Preserve separation; protect before boundary crossing.
Wrong path target	Wrong destination reduces facility clearance	Check target and boundary; reject infeasible commands
Unintended motion activation	Injury to nearby workers during preparation	Arming conditions and personnel-exclusion interlocks

Functional records define what to prevent; component analysis identifies what can cause it.

7.4.2 Safety Analysis Methods: Failure Mode and Effects Analysis

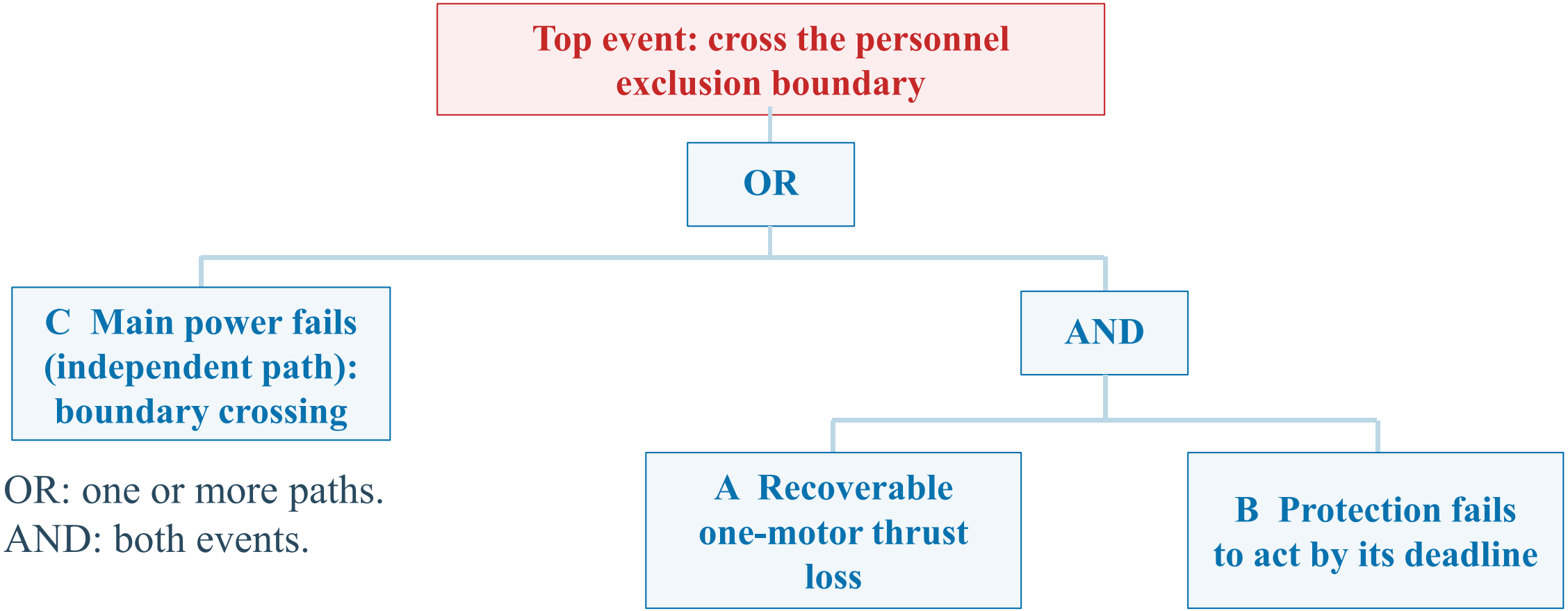
One FMEA Record Connects Cause, Effect, and Protection

Record field	Plant-inspection example
Object / mode / cause	One motor; effectiveness falls to 70%; winding damage is a hypothesized cause
Local / system effects	Insufficient thrust → other motors compensate → less control margin
Phase / scenario hazard	Path drift in turns or gusts may enter an occupied area
Monitoring / improvements	Propulsion residual, output saturation, path error; warn and head to a safe landing area
Verification / responsibility	Record warning delay, minimum separation, action effect, version, and owner

Causes and protection evidence first; then severity, occurrence, detection ratings (7.4.4).

7.4.2 Safety Analysis Methods: A Simple Fault Tree

Boundary Crossing Has Separate and Combined Paths



OR: one or more paths.
AND: both events.

7.4.2 Safety Analysis Methods: Fault-Tree Calculation

Check Independence Before Combining Probabilities

Theoretical example, per 30 min mission: $P(A) = 0.002,\ P(B) = 0.1,\ P(C) = 0.0001.$

Assumptions: mutual independence; dimensionless probabilities; only the two shown paths.

$$P(A \cap B) = P(A)P(B) = 0.002 \times 0.1 = 0.0002$$

$$P(T) = P(C) + P(A)P(B) - P(C)P(A)P(B) = 0.00029998$$

T: personnel-boundary crossing, about 0.0300% per mission; crossing is not injury.

$$P(A \cap B) = P(A)P(B \mid A)$$

Dependence requires conditional probability. Redundant hardware may share common causes.

Chapter Outline

Fault Hazards and Safety Assessment

Chapter 7 Health Management and Safety Assessment

7.1 Health Management Fundamentals

7.2 Unified Fault Modeling

7.3 Safety Reinforcement and Fault Data

7.4 Fault Hazards and Safety Assessment

7.5 Diagnosis and Prognostics

7.6 Safety Decisions and Improvement

7.7 Fault Injection Interfaces

7.8 Experiments and Validation

7.9 Exercises and Classroom Discussion

4 Units in This Section

7.4.1 Scenarios and Hazards

Textbook: Sec. 7.1.2.2, 7.1.2.4

7.4.2 Safety Analysis Methods

Textbook: Sec. 7.1.2.2, 7.1.2.4

7.4.3 Reliability and Mission Metrics

Textbook: Sec. 7.1.2.4

7.4.4 Risk Ranking and Design Improvement

Textbook: Sec. 7.1.5.3, 7.1.2.5

7.4.3 Reliability and Mission Metrics: Mean Time Between Failures

Estimating Mean Time Between Failures (MTBF)

Mean time between failures (MTBF): mean operating time from a repairable system's return to service until its next failure.

$$\widehat{\mathrm{MTBF}} = \frac{T_{\mathrm{op}}}{N_{\mathrm{f}}} = \frac{2000\,\mathrm{h}}{4} = 500\,\mathrm{h}$$

Textbook Eq. (7.2)

- Exposure: T_{op} is cumulative effective operating time (h); N_{f} counts failures under the same definition.
- For comparison, match vehicle type, payload, environment, maintenance rules, and observation scope.
- The 500 h estimate is a sample mean, not a guaranteed lifetime or a guarantee of fault-free missions.

7.4.3 Reliability and Mission Metrics: Rate versus Probability

Failure Rate Has Time Units; Mission Probability Does Not

Constant-rate example: inter-failure times are independent, identically distributed, and exponential. No repair is counted during a mission.

$$\lambda = \frac{1}{\mathrm{MTBF}}$$

λ: constant failure rate, in h^{-1}; t: mission duration, in h.

$$R(t) = e^{-\lambda t}$$

$R(t)$: probability of no failure during the mission, dimensionless.

$$F(t) = 1 - e^{-\lambda t}$$

$F(t)$: probability of at least one failure, dimensionless. $\lambda t \ll 1$ is required for $F(t) \approx \lambda t$.

Mission time affects failure probability; constant rates need matching operating conditions.

7.4.3 Reliability and Mission Metrics: Reliability Calculation

Mission Reliability for a 500 h MTBF

$$\hat{\lambda} = \frac{4}{2000\,\mathrm{h}} = 0.002\,\mathrm{h}^{-1}, \quad t = 0.5\,\mathrm{h}$$

$$F(0.5) = 1 - e^{-0.002\times0.5} = 0.0009995 \approx 0.09995\%$$

Mission duration	At least one failure	No-failure probability
15 min	0.04999%	99.95001%
30 min	0.09995%	99.90005%
60 min	0.19980%	99.80020%

If $\lambda t \ll 1$, doubling duration about doubles failure probability (same event and conditions).

7.4.3 Reliability and Mission Metrics: Mission Indicators

Completion, Capability Match, and Distance to Safety Limits

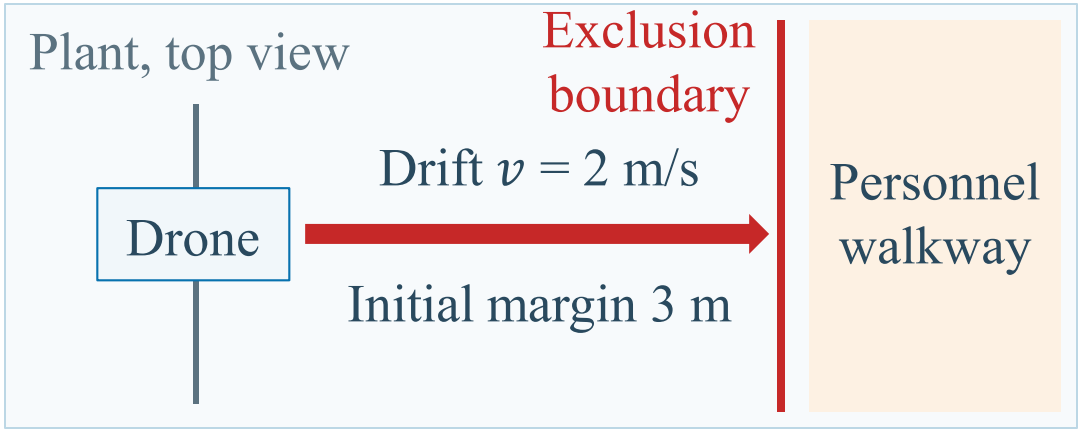
Mission completion probability	Mission health	Mission safety margin
Given goals, environment, resources. Factors: health, environmental uncertainty, fault risk, task complexity. **Inspection:** define success (clear images of all targets + return), then count successes in matched missions.	Current charge, temperature, and redundancy matched to mission payload needs. Often a normalized score for platform/task comparisons. **Inspection:** can energy + redundancy cover the remaining route + return? Otherwise adjust or abort.	Tolerance to fault propagation/path deviation while completing the mission. **Focus:** unsafe events affecting people/critical facilities. **Inspection:** minimum clearance to the personnel boundary (m) must exceed drift during the delay.

No universal formulas: state success criteria, mission period, and margin units.

7.4.3 Reliability and Mission Metrics: Safety-Margin Example

Delay Consumes Separation; Kinetic Energy Describes Impact

Delay distance at constant speed, neglecting braking and positioning error.



$$d = v\tau = 2 \times 1.5 = 3\,\text{m}$$

After τ = 1.5 s: drift 3 m; margin 0 m.

Kinetic energy at impact: mass 2 kg, speed 5 m/s.

$$E = \frac{1}{2}mv^2 = \frac{1}{2} \times 2 \times 5^2 = 25\,\text{J}$$

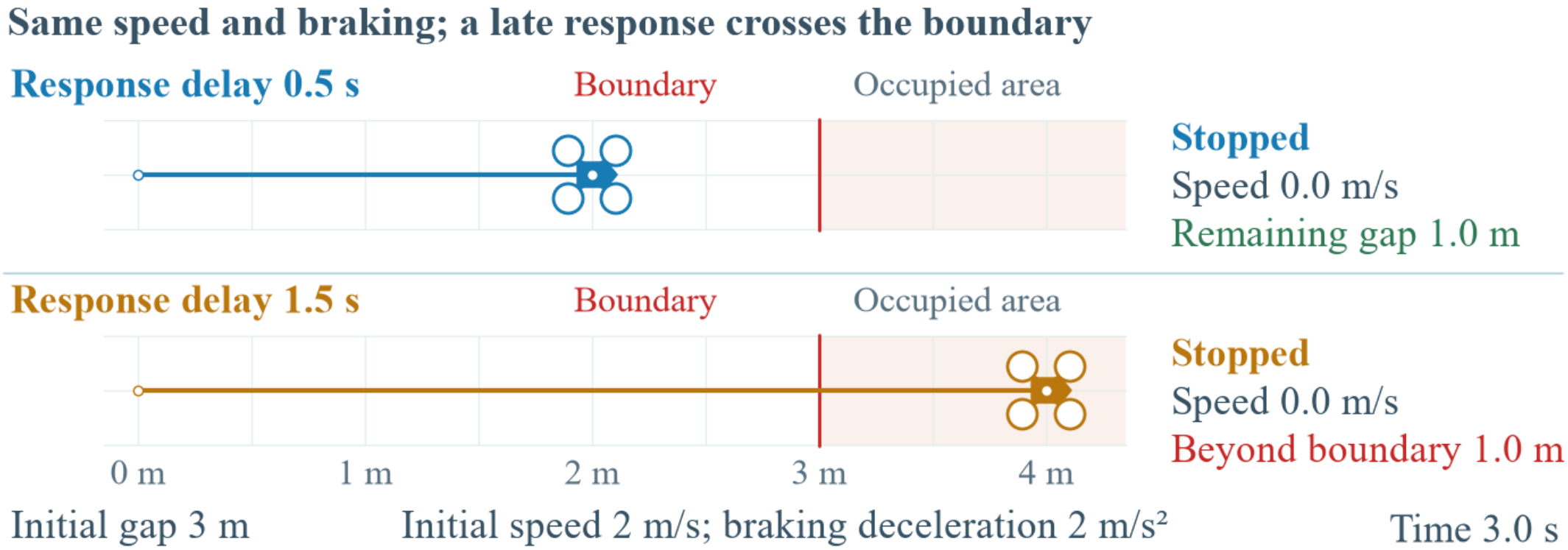
m: mass (kg); v: speed (m/s). At ground impact, this can be FallEnergy in e8_SafetyAssExp.

Kinetic energy describes impact conditions. Injury also depends on impact location, structure, and protection.

Separation must exceed $v\tau$, plus allowances for braking and positioning error.

7.4.3 Reliability and Mission Metrics: Safety-Margin Example

Later Protection Leaves Less Distance for Braking



Delay/braking consume margin (point mass); add vehicle-size and positioning-error allowances.

7.4.3 Reliability and Mission Metrics: Probability Evidence

Statistics, Monitoring, and Simulation Provide Different Evidence

Evidence source	Direct evidence	Interpretation conditions
Operating statistics	Cumulative operating time, failure count, mission conditions	Consistent failure definition; complete reporting; statistical uncertainty
Online monitoring / protection	Built-in test (BIT); fault detection, isolation, and recovery (FDIR): delay and effectiveness.	After detection, protection must act within scenario constraints
Random simulation	Monte Carlo: event frequencies from specified input distributions	Credible distributions/models; enough samples for rare events

Injection fraction supports coverage; real fault probabilities need independent evidence.

Chapter Outline

Fault Hazards and Safety Assessment

Chapter 7 Health Management and Safety Assessment

7.1 Health Management Fundamentals

7.2 Unified Fault Modeling

7.3 Safety Reinforcement and Fault Data

7.4 Fault Hazards and Safety Assessment

7.5 Diagnosis and Prognostics

7.6 Safety Decisions and Improvement

7.7 Fault Injection Interfaces

7.8 Experiments and Validation

7.9 Exercises and Classroom Discussion

4 Units in This Section

7.4.1 Scenarios and Hazards

Textbook: Sec. 7.1.2.2, 7.1.2.4

7.4.2 Safety Analysis Methods

Textbook: Sec. 7.1.2.2, 7.1.2.4

7.4.3 Reliability and Mission Metrics

Textbook: Sec. 7.1.2.4

7.4.4 Risk Ranking and Design Improvement

Textbook: Sec. 7.1.5.3, 7.1.2.5

7.4.4 Risk Ranking and Design Improvement: Mission-Based Classes

Mission Consequences Describe Remaining Capability

Textbook examples	Remaining capability	Inspection considerations
A Catastrophic	Loss of control; no safe forced landing	Uncontrolled path; exposure of people/facilities
B Hazardous	No return or degraded mission, but a controlled forced landing is possible	Forced-landing area and remaining control
C Serious	Mission fails; return or an alternative mission remains possible	Risk and quality requirements after abort
D Minor	Mission completed with acceptable reduced quality	Image quality, path, remaining margin
E No safety effect	Preset mission and quality are unaffected	Still assess risks to people, facilities, environment

Textbook A–E mission examples; no DAL mapping. Mission success still requires scenario safety.

7.4.4 Risk Ranking and Design Improvement: Risk Priority

Severe Consequences Retain Priority over an Empirical Product

Risk priority number (RPN) uses ordinal ratings: severity S, occurrence O, and detection difficulty D. A higher D means harder timely detection.

$$\mathrm{RPN} = S \times O \times D$$

Classroom consequence	S / O / D (ratings 1–5)	RPN / priority rule
Entry into personnel area	5 / 2 / 2	20; severe personnel hazards first
Reduced image quality	2 / 5 / 4	40; use the ranking to plan improvements

Class ratings: S=5, severe personnel hazard; O=2 low, O=5 high; D=2 easier, D=4 harder detection. Ratings and RPN have no probability units.

7.4.4 Risk Ranking and Design Improvement: Dynamic Ranking

Verified Improvements Change Paths and Residual-Risk Priorities

Theoretical design comparison: keep the 30 min mission and probabilities of A and C fixed. Assume effective protection reduces B's failure probability from 0.1 to 0.02.

Design state	Modeled crossing probability	Improvement record
Before improvement	$0.00029998 \approx 0.0300\%$	Combined A–B path contributes more risk
Assumed protection improvement	$0.000139996 \approx 0.0140\%$	Validate warning delay, action success, and minimum distance

Independent path C remains. Reduce this residual risk by improving power-supply reliability.

Rank → verify improvements → update risk database → rerank → test residual risk

7.4.4 Risk Ranking and Design Improvement: Assessment Challenges

Software and Scenario Changes Require Risk Reassessment

Software-defined functions

Risk: changed control logic alters remaining capability on the same hardware.
Action: fix state and input; test functional limits.

Triggered software defects

Risk: extreme inputs or specific states trigger an incorrect path.
Action: abnormal-input, combined-fault, boundary regression tests.

Learning models / interpretability

Risk: opaque models; wind, light, or objects beyond training affect decisions.
Action: cross-scenario tests; independent monitoring and executable fallback.

Versions / over-the-air (OTA) updates

Risk: a new version changes thresholds, actions, or interface constraints.
Action: record versions; retest protection delay and risk records.

Intelligent assessment adds behavior, robustness, and interpretability to hardware reliability.

7.4.4 Risk Ranking and Design Improvement: Safety Scoring

Software Development Kit (SDK) Scoring Rules

Window / channel Target value → **Two-point mean Squared error** → **Piecewise map Local score** → **Membership Aggregate score/class**

$$e_i = (\overline{v}_i - v_{\mathrm{cmd}})^2$$

$\overline{v}_i$: pair mean; v_{cmd}: same-channel target.

Code category	Velocity error²	Score
Normal (Nomal)	$0 \le e_i < 0.015$	0.999→0.9
Slight	$0.015 \le e_i < 0.04$	0.9→0.7
Serious	$0.04 \le e_i < 0.16$	0.7→0.4
Hazard	$0.16 \le e_i < 0.5$	0.4→0.1

Mapping / aggregation

Membership: if >0.9, use 1; else keep.
If falling, multiply by (1−drop).
Weighted mean: 1/3/6/9/12.
$e_i \ge 0.5$: ground impact; 0.1 here.

Velocity in m/s gives error in m²/s²; scores rank errors, not accident probabilities.

7.4.4 Risk Ranking and Design Improvement: Scoring Calculation

From One Error Value to a Score and Output Class

Step	Input	Calculation	Result
① **Assign range**	e=0.1	Serious: [0.04,0.16)	Local score 0.529
② **Membership**	0.529	Not above 0.9: retain	0.529
③ **Time update**	Previous value 0.8	$0.8\times(1-0.271)$	0.583

- ④ **Weighted mean:** Slight 0.8, Serious 0.583, weights 3 and 6 give ≈0.66.
- ⑤ **Class:** Serious has the largest weighted count (weight 6); output: Medium.
- Low-score categories carry more weight; a few large errors can sharply lower the score.

Learning Resources

Official Sources for Definitions, Methods, and Scope

MTBF and constant rates: National Institute of Standards and Technology (NIST) handbook

https://www.itl.nist.gov/div898/handbook/apr/section1/apr171.htm

FMEA scope and maintenance: International Electrotechnical Commission (IEC) 60812

https://webstore.iec.ch/en/publication/26359

Functional hazards and development assurance: Federal Aviation Administration (FAA) Advisory Circular (AC) 25.1309-1B

https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_25.1309-1B.pdf

Specific-operation risk and SORA: Joint Authorities for Rulemaking on Unmanned Systems (JARUS)

https://jarus-rpas.org/publications/

Exercises and Discussion

Adapt an Open-Field Record to a Personnel Walkway

Given: one motor falls to 70% effectiveness; the path is temporarily maintained. The open field has an exclusion zone; the plant borders a walkway.

FMEA field	Open-field example	Plant walkway: complete
Exposure / consequence	Inside exclusion zone: mission abort, equipment damage	Exposed people/objects: ____ Worst credible effect: ____
Monitoring / measures	Monitor control margin; exit mission, land under control	Monitored quantity: ____ Action / effective conditions: ____
Verification criteria	Land within the exclusion zone; controllable response	Response deadline: ____ Personnel separation: ____

Reference Answers

Add Personnel Exposure and a Protection Deadline

Field	Reference entry
Exposure / credible effect	Personnel walkway; drift across the boundary may strike people or equipment
Monitoring evidence	Path error, propulsion residual, output saturation; align with fault onset
Action / conditions	Stop inspection; head to an unoccupied landing area if remaining capability permits
Response criterion	Total detection/execution delay is below the time allowed by remaining separation
Evidence / update	Record minimum distance, delay, control margin, version; review residual risk

Reuse fault records, but rewrite scenario hazards and protection conditions for each mission.

Section Summary

Assessment Connects Faults to Scenarios and Improvements

- **Start with the scenario:** health describes state; capability describes function; safety assesses consequences for people, facilities, and environment.
- **Methods:** FHA sets consequences/requirements; FMEA traces component effects; FTA checks combinations and common causes.
- **Numbers need conditions:** mission time turns rate into mission probability; dependence determines the combination rule.
- **Improvements need evidence:** empirical scores and RPN support comparison; verify protection timing/effectiveness and update residual risk.
- **Common errors:** scores are not accident probabilities; MTBF is a sample mean, not lifetime. Alarms change detection D; severity falls only when consequences are limited.

After identifying risk, select protection actions that can execute and have been verified.