

GOVERNED TEMPLATE RENDERING REFERENCE: EDGE CASE ANALYSIS DEFAULT V2 (DRAFT)

definition 144e59e2...1d59

EDGE CASE ANALYSIS · PROJECT ARTIFACT

SPECIRA

Edge Case Analysis: Dispatch Modernization

Meridian Field Services: instructional example, not project evidence

DRAFT · WATERMARK POLICY: DRAFT_ONLY

template edge_case_analysis v2 · pack: specira_default_delivery

derive, never brainstorm: analysis specifies, tests execute by id

§1 Boundary Conditions

mandatory1 decision1 evidence rule

validators: every_edge_case_has_derivation_technique_cited · every_edge_case_has_disposition_with_owner · collection_surfaces_cover_zero_one_many · state_matrix_used_past_four_states_three_actions

Every case cites its technique; every row documents expected behavior, a specification, not a test step. The empty set breaks first.

Id	Technique	Case → expected behavior	Severity	Disposition
EC-01	zero/one/many	A ready job has ZERO eligible technicians → the panel states the empty result and its reason (no eligible match, not a failure), the full list opens, the job flags for exception review (US-3 ^[1])	high · possible	handle

Id		Technique	Case → expected behavior	Severity	Disposition
EC-02	BVA · 4 points		Position.assigned_at at the 300-s skew bound (299 / 300 / 301 / far-future) → 300 accepted, 301 dropped and counted (VR-02 ^[3])	moderate · possible	handle
					Sandova
EC-03	state corner · INVALID		A technician confirms an assignment already reassigned away → rejection with the stale_version contract and a board notice (error registry ^[4])	moderate · likely	handle
					Sandova
EC-04	CRUD × many		Deleting a job with active assignments → forbidden; archive is the only exit while assignments exist (lifecycle ^[5])	moderate · rare	handle
EC-06	equivalence partition		A job addressed outside any hub's service polygon → intake accepts and routes to manual review	low · rare	accept
					pilot (rare occurrence observed review & owner M revisit a

The assignment lifecycle earns the matrix (five states × four actions, twenty cells, three forbidden transitions explicit). The matrix surfaced EC-05 , shift ends mid-assignment, whose expected behavior was UNDEFINED at analysis. Promoted to an FR revision (the assignment persists and the confirmation window extends into the next shift; FR-016 revision^[2]): the analysis records the discovery, the FRD owns the behavior.

State ↓ · Action →	Assign	Confirm	Override	Complete
ready	→ assigned	forbidden	forbidden	forbidden

State ↓ · Action →	Assign	Confirm	Override	Complete
assigned	re-assign (reason)	→ confirmed	→ assigned'	<i>forbidden</i>
confirmed	EC-03 → stale_version	idempotent	→ assigned' (notice)	→ complete
on-hold	<i>forbidden (BR-04 clock paused)</i>	n/a	n/a	n/a
complete	<i>terminal: EC-05's shift-end row promoted to FR-016</i>			

§2 Failure Scenarios

mandatory

1 decision

1 evidence rule

validators: failure_rows_carry_four_parts · failure_rows_cite_designed_behavior · malicious_variants_cross_link_threat_model

Four parts, every row (what fails, how detected, what the user experiences, recovery), citing designed behavior, never inventing it. Malicious faces live in the threat model.

Id	What fails	Detected by	User experiences	Recovery	Malicious fa
F-01	Position feed stops	The gap indicator (INT-1 ^[6])	Stale-marked positions; manual assignment proceeds	The feed-loss drill (DV-5 ^[7])	TM-01 ^[8] (p
F-02	Suggestion path degrades	The 2-s boundary timer (FLW-01 ^[9])	Full list with a degradation notice (suggestions_unavailable ^[4])	Automatic on next request	n/a
F-03	Notification gateway fails	Delivery-failure counts	Technician silence: the 10-min confirmation timer catches it, re-notifies, then flags (exception_paths ^[9])	Manual call tree at 30 min	TM-06 ^[8] (f
F-04	Nightly file truncated: the ISS-2 case	Checksum	None (quarantined before load)	Quarantine-and-rerun (RSK-08 ^[10] , ISS-2 ^[11])	n/a

§3 Concurrency & Race Conditions

mandatory

1 decision

1 evidence rule

validators: concurrency_cases_include_race_window_and_countermeasure · residual_behavior_specified_per_race · production_discovered_races_carry_issue_links

Design-time discipline: these rows exist before the race ships. Every row names its window, cites its countermeasure, and specifies what the losing request experiences.

Id	Pattern	Race window	Countermeasure (cited)	Residual: the loser sees
R-01	double-submit	The assign click retried by the client while the first request is in flight, same job	The Idempotency-Key contract (POST /assignments ^[4])	The retry receives the first respo E. Sandoval
R-02	lost update	Two dispatchers edit the same job between read and save	Optimistic-lock version check (concurrency ^[5])	stale_version → re-read (er
R-03	check-then-act	Eligibility checked at suggest time; the technician's shift ends before assign	Eligibility re-checked server-side at assignment write; the suggest-time check is advisory (FR-002 ^[2] , BR-01 ^[3])	validation_failed, with the

No production-discovered races yet: stated, so the first one arrives into a table that already exists.

§4 AI Model Edge Cases

conditional · AI components exist, ENGAGED

1 decision

1 evidence rule

validators: ai_families_addressed_or_explicitly_na · ai_rows_cite_designed_degradation

The governing posture: degrade before erroring; every row cites its designed degradation.

Family	Disposition
Malformed output	eliminated structurally : constrained output, ranked ids from the eligible set only (ADR-5^[12] , SR-016^[13]); the residual is a schema-valid but empty ranking, which is EC-01's empty-set behavior; one case, one place
Latency spike	handle : the 2-s boundary timer degrades to the full list (FLW-01^[9]); slow-but-valid responses past the timer are discarded, never late-applied
Empty candidate set	handle : distinguished from EC-01; a model returning nothing for an eligible pool is a model FAULT and counts toward the suggestion-quality indicator (RSK-06^[10]); a genuinely empty pool is domain truth
Hallucination	not applicable · a claim : no free text reaches the board in the constrained design; the eliminating decision cited (ADR-5^[12])

§5 Open Questions

mandatory

1 decision

Question	Owner	Answer by	Blocks
Does EC-06's accept-gap survive hub-two volumes (the two-per-month observation is Toronto-only)?	M. Chen	At the hub-two go decision	The EC-06 disposition only

Refs References & Package Contents

In the Specira workspace

specira	[1] User stories: US-3 exception review app.specira.ai/projects/dispatch-modernization/artifacts/user-stories#us-3
specira	[2] FRD: FR-002, FR-016 revision (EC-05's promotion) app.specira.ai/projects/dispatch-modernization/artifacts/frd
specira	[3] Business rules: BR-01, VR-02 app.specira.ai/projects/dispatch-modernization/artifacts/business-rules
specira	[4] API contracts: error registry, idempotency, degradation contract app.specira.ai/projects/dispatch-modernization/artifacts/api-contracts

specira	[5] Data model: lifecycle, concurrency (optimistic locking)	app.specira.ai/projects/dispatch-modernization/artifacts/data-model
specira	[6] Integration inventory: INT-1 gap indicator	app.specira.ai/projects/dispatch-modernization/artifacts/integration-inventory#int-1
specira	[7] Deployment verification: DV-5	app.specira.ai/projects/dispatch-modernization/artifacts/deployment-verification#dv-5
specira	[8] Threat model: TM-01, TM-06 (the malicious faces)	app.specira.ai/projects/dispatch-modernization/artifacts/threat-model
specira	[9] Process flows: FLW-01 timers, exception paths	app.specira.ai/projects/dispatch-modernization/artifacts/process-flows
specira	[10] Risk register: RSK-06 indicator, RSK-08	app.specira.ai/projects/dispatch-modernization/artifacts/risk-register
specira	[11] Issues: ISS-2	app.specira.ai/projects/dispatch-modernization/issues/iss-2
specira	[12] Decision log: ADR-5 constrained output	app.specira.ai/projects/dispatch-modernization/artifacts/decision-log#adr-5
specira	[13] Security requirements: SR-016	app.specira.ai/projects/dispatch-modernization/artifacts/security-requirements#sr-016