

CPIT- 455

Haram Safe

|  |  |
| --- | --- |
| **Student Name** | **ID** |
| 1. Ammar Binyamin | 2236034 |
| **Section: IT1** | |

***Prof. Name:*** *Adeeb Noor*

Contents

Topic Page number

Concept .….………………………………………………………………….. 3

Context, Hazards, Targets …….….………………………………………….. 4

Architecture & Patterns…..……….………………………………………….. 5

Fault tree …....….….……….….….….….….….….….….….….….….….….. 5

Programming Guidelines for Reliability.…..………..….….….….….…..…… 6

Metrics & Prototype …..…….……….….….….…………………………….. 7

Humanization Checklist …..….…..………………………………………….. 7

Vision 2030, Roadmap, Ethics …...…….….….…………………………….. 8

**Concept**

Haram Safe is a reliability-driven crowd management system for Masjid al-Haram. It estimates live crowd density from diverse sensors, self-checks those estimates using two independent analytics channels, and—when a safety threshold is crossed—an independent protection service issues automatic actions (Close, Reroute, One-Way, signage/PA). Operators always retain manual override.

Reliability is tracked with Availability (AVAIL), POFOD (probability of failure on demand), ROCOF (false-alert rate), and p95 detection latency, with strict targets during peak periods.

Why does this matter now. Peak-hour density can rise faster than humans can perceive and coordinate. A few seconds of delay can turn heavy congestion into crush-risk. Haram Safe’s design makes fast, predictable responses possible even during partial outages.

Reliability goals :

* Availability (AVAIL): ≥99.99% during peak hours
* POFOD (safety actions): ≤1×10⁻⁵ per demand
* ROCOF (false-red): ≤1 per 12 hours
* p95 detection latency: ≤2 seconds

How we achieve them. We use diversity (two CV models + presence sensors), timeouts and bounded retries on critical calls, idempotent commands to prevent double-actions, and active-active monitoring stacks. Weekly drills and “chaos” tests (drop a camera, fail a link, crash a model) verify that the protection service still acts within the ≤90-second intervention budget.

**Context, Hazards, Targets**

**Context :**

* The Haram faces extreme, variable densities during Hajj, Ramadan, Friday prayers, and evening Umrah.
* Small response delays can escalate to dangerous densities in minutes.

**Primary Hazards :**

* Dangerous density / crush
* Heat stress surges
* Digital/sensor outages
* Alert fatigue (operator overload)
* Evacuation impediments
* Privacy risks

**Crowd Thresholds :**

* Green: ≤ ~4 people/m²
* Red: ≥ ~6 people/m² sustained (time-based)

**Reliability Targets :**

* Availability (AVAIL): ≥ 99.99% per peak hour
* POFOD (safety actions): ≤ 1×10⁻⁵ per demand
* ROCOF (false-red): ≤ 1 per 12 h
* p95 detection latency: ≤ 2 s

**Architecture & Patterns**

1. **Owl sensing:** CCTV CV, overhead thermal counters, BLE/Wi-Fi presence, manual clickers.
2. **Dual transport:** 5G + fiber, QoS, store-and-forward buffers.
3. **Self-monitoring analytics:**
   * Channel A (Model A, vendor)
   * Channel B (Model B, different vendor)
   * **Comparator**: if |A−B|/mean > ε for N frames ⇒ **safe-side fallback**.
4. **Independent Protection Service (tiny & simple):** watches only density/derivative/heat and issues **Close/Reroute/One-Way/PA** directly to controllers.
5. **Operator UI:** bilingual console + playbooks; manual override.
6. **Actuators:** dynamic signage, gates/barriers, misting, water dispatch, PA.

**Fault-Tolerance Patterns (from Reliability Engineering)**

* **Protection system:** independent, simple, last line; very low POFOD.
* **Self-monitoring:** two heterogeneous channels + comparator; conservative fallback on mismatch.
* **High availability:** active-active stacks; time-bounded calls; bounded retries; **idempotent** actuation commands; health heartbeats.

**Fault tree**

**Top event:** Critical crowd crush in zone **Z**.

**AND:** (**Density ≥ 6 people/m²** for **≥ 30 s**) **AND** (**Intervention delay > 90 s**).

**Density drivers (OR):** inflow spike; bottleneck formation; bidirectional conflict; obstacle; micro-stoppages (heat/medical).

**Intervention delays (OR):** sensor miss; analytics outage; mismatch not detected; alert not acted; command path failure; physical jam.

**Mitigations:** one-way routing & obstacle control; dual-channel analytics + comparator; heartbeats/SLA monitors; **independent protection service** with **timeouts + retries**; predefined detours; weekly drills and chaos tests.

**Programming Guidelines for Reliability**

* **Information hiding / encapsulation** (private config/state; minimal APIs)
* **Validate all inputs** (range/format checks)
* **Handle every exception** (no silent failures; friendly operator messages)
* **Avoid error-prone constructs** (no FP equality; no hidden globals)
* **Restart/resume safely** (remember last safe state/action; idempotency)
* **Bounds checks** (fixed windows/ring buffers; guard indexes)
* **Timeouts** (treat slow actuation as failure; retry within limits)
* **Named constants** (all thresholds/time budgets centralized)

**Metrics & Prototype**

We track Availability, POFOD, ROCOF, p95 detection latency.  
A simple discrete-time prototype (arrivals → density → thresholds) showed baseline AVAIL ~96.9% and POFOD ~4.0% before redundancy/repair improvements. To reach targets: raise MTBF, cut MTTR with auto-failover, run two independent stacks in parallel, and keep the protection service tiny and formally reviewed.

**Humanization Checklist**

* **Clear communication:** Bilingual (Arabic/English) UI & PA; green/amber/red with icons.
* **Accessibility:** Wheelchair/elderly lanes; gentle slopes; rest/shade; large fonts & high contrast.
* **Heat & hydration:** Heat-index monitoring; automatic misting; water dispatch triggers.
* **Wayfinding & flow:** One-way guidance at peaks; remove obstacles; avoid counter-flows; detour suggestions.
* **Respect & privacy:** Edge blurring; store counts/heatmaps (no faces at rest); short retention; PDPL notices.
* **Human override:** Operator can approve/override any automatic action; regular drills; visible manual controls.
* **Inclusivity:** Consistent iconography; audio prompts; color-blind-safe palettes.

**Vision 2030, Roadmap, Ethics**

**Vision 2030 (Pilgrim Experience)**

* Safer, smoother journeys; clearer multilingual guidance.
* Integrates with national digital services (permits, transport, emergency).
* KPIs: incident-free peak hours, time in hot zones, operator confirmation rate, satisfaction.

**12–24-month Roadmap**

* **0–6 months :** one precinct; A/B CV + comparator; minimal protection rules; bilingual console.
* **6–12 months :** expand zones; active-active analytics; misting & water triggers; metro/bus feed alerts.
* **12–24 months :** digital twin; 5G slicing + fiber ring; city-scale one-way routing & emergency playbooks.

**Ethics & PDPL**

* Data minimization: counts/heatmaps; no faces at rest; short retention.
* Edge blurring; encrypted links; strict role-based access & audit logs.
* Transparent signage; inclusive design (Arabic/English, color-blind-safe, wheelchair routes).
* Human override always; monthly drills.