SCS - Hazard Analysis

Muhammad Muzamil

July 4th, 2025

1 FMEA - Failure Mode and Effect Analysis

Table 1: FMEA Table for TCAS II Components

Component	**Function**	**Failure Mode**	**Sev.**	**Cause**	**Occ.**	**Prob.**	**RPN**	**Action**	**R**
Identify/Track	Velocity/Position Input	Out of bound values	8	Unvalidated input	4	2	64	Define min/max bounds	Mu
Identify/Track	Input Data	Missing values	9	Not initialized	5	3	135	Validate inputs	Mu
Identify/Track	Range Calculation	Range = 0	8	Same position	3	2	112	Add range==0 check	Mu
Identify/Track	Closing Velocity	Velocity = 0	8	Equal velocity	3	2	96	Check velocity==0	Mu
Identify/Track	TAU Calculation	TAU = NaN/Inf	8	Range/velocity=0	4	2	96	Handle special cases	Mu
Threat Eval.	Threat Detection	Missed threat	10	Threshold error	4	3	120	Validate logic	M.
Threat Eval.	Threat Detection	False RA	8	Input error	4	2	80	Data filter	M.
Threat Eval.	Priority Logic	Wrong priority	9	Logic flaw	3	2	90	Refactor logic	M.
Threat Eval.	Timing	RA too late	8	Computation delay	2	2	64	Optimize code	M.
Threat Eval.	TAU Calc.	Invalid TAU	7	Div/0 error	3	2	84	Add fallback	M.
Threat Eval.	Threat Data	Stale inputs	9	No refresh	4	2	90	Add timestamps	M.
Threat Eval.	Thresholds	Missing config	9	Bad setup	4	2	90	Validate config	M.
Advisory	Maneuver	Same RA	10	ID error	3	3	150	Add redundancy	Tabba
Advisory	RA Assign	Invalid maneuver	9	Altitude limit	3	2	90	Add checks	Tabba
Advisory	Display	RA not shown	8	Data drop	4	2	96	Force update	Tabba
Advisory	RA Logic	ID conflict	8	ID error	3	2	96	Add fallback	Tabba

2 STPA - TCAS System

2.1 Hazards

- **H1**: TCAS fails to detect the intruder aircraft.
- **H2**: TCAS tracks wrong position and velocity of the intruder aircraft.
- **H3**: TCAS detects the intruder aircraft too late for safe avoidance.
- **H4**: TCAS fails to detect a threat if one exists. (Output: -)

- **H5**: TCAS misclassifies level of threat (TA vs RA).
- **H6**: TCAS delays threat detection beyond acceptable time.
- **H7**: TCAS fails to issue an advisory when required.
- **H8**: TCAS issues incorrect advisory (Wrong Severity, Direction).
- **H9**: TCAS issues advisory too late for pilot to react.
- **H10**: TCAS gives conflicting or same maneuver to both aircraft.
- **H11**: TCAS fails to assign correct maneuver (Climb/Descend) to aircraft.
- **H12**: TCAS fails to evaluate RA condition when criteria are met.
- **H13**: TCAS fails to deliver advisory to UI/Radar/Audio Interface.
- **H14**: TCAS announces the advisory too late.
- **H15**: TCAS delays advisory or radar updates beyond human reaction time.

2.2 Unsafe Control Actions:

UCA	**Control Action**	**Unsafe when**	**Type of UCA**	**Related Hazard**
UCA 1	Compute Range, TAU	Position or velocity values are missing / out of bounds	Not Provided	H1, H2
UCA 2	Compute Relative Velocity	Range = 0 → Illegal Division	Provided Incorrectly	H1, H2
UCA 3	Calculate TAU	Relative Velocity = 0 → Invalid	Provided Incorrectly	H1, H2
UCA 4	Detects threat	No threat exists	Provided Incorrectly	H4
UCA 5	Detects TA	Threat should be RA	Provided Incorrectly	H5, H8
UCA 6	Detects RA	Threat should be TA	Provided Incorrectly	H5, H8
UCA 7	Compares Range/TAU	RA/DMOD threshold values are missing or undefined	Provided Incorrectly	H4, H5
UCA 8	Detects 'No Threat'	TAU or DMOD threshold is violated → Threat missed	Not Provided	H4
UCA 9	Detects threats	Too late for pilot to react	Provided Too Late	H6,H9,H15
UCA 10	Announces TA	Should have announced RA instead	Provided Incorrectly	H8
UCA 11	Announces RA	Should have announced TA instead	Provided Incorrectly	H8
UCA 12	Assign RA Maneuver	Same maneuver (Climb/Climb or Descend/Descend) to both aircraft	Provided Incorrectly	H10, H11
UCA 13	Assign Maneuver by ID	Aircraft IDs not valid / same / missing	Provided Incorrectly	H11
UCA 14	Assign climb Maneuver	Impossible for Aircraft to perform maneuver	Provided Incorrectly	H11
UCA 15	Assign descend Maneuver	Impossible for Aircraft to perform maneuver	Provided Incorrectly	H11
UCA 16	Display Advisory to Radar	Advisory generated but UI doesn't update	Not Provided	H13

2.3 Casual Scenarios:

UCA ID	Casual Scenario
UCA 1	Aircraft velocity / position input was unrealistic or outside expected bounds (ex: Velocity > 2180 km/h, Position < 0)
UCA 2	Both aircraft initialized at same position (x1 = x2, y1 = y2), making range = 0 → leads to division by zero when computing relative velocity.
UCA 3	Both planes have equal velocity vectors (both planes going in the same direction and at same velocity/speed a1.vx = a2.vx) leads to 0 relative velocity. System still tries to compute TAU → invalid operation.
UCA 4	Protection volume threshold (TAU/DMOD) were not set or set to default due to missing variables in script.
UCA 5, UCA6	Same protection thresholds were accidentally used for both TA and RA or RA/TA protection thresholds were used for TA/RA protection thresholds leading to misclassification of threats.
UCA 7	Researcher didn't define protection volume thresholds for TA/RA scenarios before simulation starts.
UCA 9	Thresholds were hardcoded based on low altitudes and not adjusted for high altitude scenarios like 42,000 ft.
UCA 10, UCA 11	If else logic incorrectly maps RA to TA or vice versa due to inverted condition or missing boundary check.
UCA 12	Both aircraft IDs are either missing or both have the same parity (even/even or odd/odd) which makes maneuver assignment ambiguous.
UCA 13	One or both aircraft have no assigned ID → maneuver logic cannot decide climb/descend.
UCA 14, UCA 15	Aircraft is already at minimum or maximum allowed altitude → cannot climb/descend but advisory is still issued.

2.4 Safety Constraints:

SC ID	SR	UCA	Component	SC
SC1	SR 1	UCA 1,2	Identify & Track	The system shall validate all aircrafts' data (position, velocity, IDs) before computing Range and TAU. If the inputs are missing or are out of bounds, simulation should update the radar with the error message for the pilot and should halt the simulation.
SC2		UCA 3	Identify & Track	The system shall pre check all divisions and mathematical operations such as (TAU = Range / Relative Velocity) and should avoid execution if the denominator is 0 or undefined.
SC3	SR1, SR4, SR5	UCA 4,5,6,7	Threat Evaluation	The system shall validate Protection threshold values. If protection threshold values are missing, out of bound or misconfigured (TA → RA or RA → TA), the system shall not generate any advisory.
SC4	SR2, SR3, SR6	UCA 9	Threat Evaluation	The system should automatically set the Protection Threshold values based on the aircrafts' altitude, according to the Sensitivity level.
SC5	SR5	UCA 10,11	Advisory Selection	The advisory module must validate that the threat level is correctly interpreted before issuing TA or RA. TA shall not be issued when RA conditions are met and vice versa. This must be ensured through distinct comparison logic for both TA and RA thresholds.
SC6	SR 5	UCA 12,13	Advisory Selection	The system should use redundant conditions such as Speed, Velocity while assigning a RA and should not solely depend on Aircrafts' IDs for assigning RA.
SC7	SR 2	UCA 14, 15	Advisory Selection	The system shall check if the altitude before giving a RA, making sure the maneuver could be executed properly.
SC8	SR7	UCA 16	UI/Radar	The UI should update the aircrafts' positions, threats and advisories in real time (1 sec) with visual makers and labels, clearly showing intruder identity and type of advisory.
SC9	SR6, SR7	-	UI/Radar	The advisory displayed must be accompanied by audio alert and should persist for at least 3 seconds to ensure pilot's acknowledgment.
SC10	SR1, SR7	-	UI/Radar	In case of system failure, data error or missing inputs, the radar must display 'System Error / Advisory Halted' warning so that the pilot is aware of advisory suspension.

3 STPA-SafeSec

3.1 Security Hazards:

- **SH1**: Unauthorized access to source code or project repository.
- **SH2**: Unauthorized modification of predefined input data or advisory logic without proper approval.
- **SH3**: Inability to trace changes made to source code or configuration due to lack of version control or commit documentation.
- **SH4**: External interference during simulation (ex: remote access, Wi-Fi/Bluetooth injection) that may halt/disrupt simulation.

3.2 UCA-Sec

UCA ID	Control Action	Unsafe When	Type	Related SH
UCA 1	Access project	Access is not granted to unauthorised person	Not Authorised	SH1
UCA 2	Modify logic or inputs	Changes made without team consensus or approval	Not Tracked	SH2
UCA 3	Run simulation	Logic was tempered by unauthorised person	Not Authorised	SH2,3
UCA 4	Edit Repository	No Git tracking or commit messages used	Not Authorised	SH3
UCA 5	Run Simulation while connected to network	WiFi or Bluetooth allows unauthorized interception	Not Authorised	SH4

3.3 Security Requirements:

- **Sec-R1**: The source code should be protected from unauthorised access and modification.
- **Sec-R2**: All source code changes must be tracked through version control (Git) with proper commit documentation. **Sec-R3**: Only Authorized team members should have access to code repository.
- **Sec-R4**: All purposed changes to source code shall require team approval prior to implementation.
- **Sec-R5**: During simulation execution, the system shall run in an offline environment to prevent external interferences.

3.4 SC-Sec:

SC-Sec ID	Component	Sec-Requirement	Constraint
SC-Sec 1	Source Code	Sec-R1	The source code shall reside in a private GitHub repository with restricted access.
SC-Sec 2	GitHub Repository Access	Sec-R3	Only authorized group members should be added as collaborators with commit/push permissions.
SC-Sec 3	Git Workflow	Sec-R4	All changes must be peer reviewed and approved before being committed to the repository.
SC-Sec 4	Version Control	Sec-R2	All commits must be documented with messages describing the change purpose.
SC-Sec 5	Laptop Runtime Environment	Sec-R5	During simulation runtime, Wifi, Bluetooth should be turned off to prevent remote interferences.