Fault Tree of the VaMEx-Navigation System used for the Iterative System Design presented at the DLRK 2024

Navigation System Loss — Nav.Sys. loss will result into an unsave state of the UAV and potential loss of the UAV itself

OR

Hazardous Missleading Sensorfusion Result — The estimated errourous state would lead to a loss of the Nav.Sys./UAV in the current flight segment

AND — The estimated errourous state was not fitered out by the sensorfusion watchdog and will lead to a loss of the Nav.Sys

Potential Missleading Sensorfusion Result

Sensorfusion Watchdog Failure

A potential desasterous measurment update is sent to the sensorfusion/ The SF update might fail due to a computational failure

OR

Nav.Sys/UAV would be lost as the as the initialization does not allow safe flight operation

Hazardous Missleading Initialization

No false positive

AND

- Initialization Watchdog Failure
- Potential Missleading Initialization Information

OR

- Sun Sensor Failure
- Beacon Failure

Hazardous Missleading Beacon Information

AND

- Beacon Watchdog Failure
- Beacon Failure

Hazardous Missleading TRN Information

AND

- TRN Watchdog Failure
- Potential Missleading TRN Information

OR

- Vis. Odometry Failure
- Camera Failure

Hazardous Missleading Altimeter Information

AND

- Potential Missleading Altimeter Information
- Altimeter Watchdog Failure

OR

- LiDAR Failure
- Altimeter Module Failure

Hazardous Missleading IMU Information — Faulty IMU measurments were not detected an will lead to an immidiat loss of the Nav. System and UAV

AND

- IMU Redundancy Watchdog Failure
- Potential Missleading IMU Information

OR

- IMU 1 Failure
- IMU 2 Failure
- IMU 3 Failure

Hazardous Missleading Sensorfusion Result — The estimated errourous state would lead to a loss of the Nav.Sys./UAV in the current flight segment

AND — The estimated errourous state was not fitered out by the sensorfusion watchdog and will lead to a loss of the Nav.Sys

Potential Missleading Sensorfusion Result

Sensorfusion Watchdog Failure

A potential desasterous measurment update is sent to the sensorfusion/ The SF update might fail due to a computational failure

OR

Hazardous Missleading TRN Information

AND

- TRN Watchdog Failure
- Potential Missleading TRN Information

OR

- Vis.Pos. Failure
- Vis. Odometry Failure
- Camera Failure

Hazardous Missleading Altimeter Information

AND

- Potential Missleading Altimeter Information
- Altimeter Watchdog Failure

OR

- LiDAR Failure
- Altimeter Module Failure

Computational Failure — E.G. bitflip, compute HW Failure etc

Phases

- Initialization
- Take off / landing
- Cruise / Mapping

AL_pos, scien. = 20m
AL_pos, = 100m