Hazard Analysis for DO178C

Referencing the lecture on Hazards, Risks and Failures:
"System design is about handling hazards, either by eliminating the state or removing/mitigating the potential for loss while in that state"

So, in regards to our minimal cut sets, we are trying to eliminate those states outlined or find ways to remove/mitigate the potential for loss while in the state.

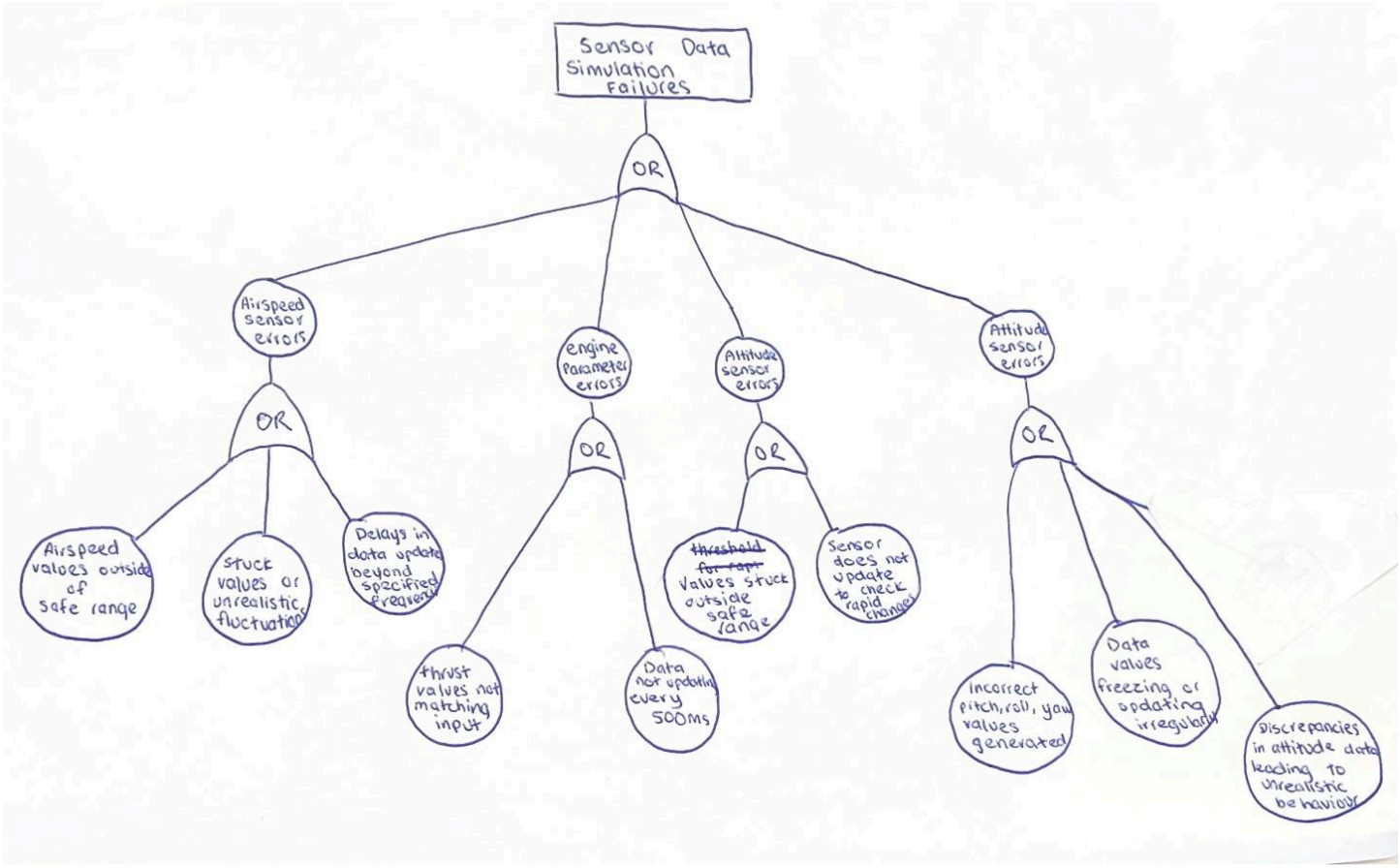
Hazard Analysis

Hazard Category	Hazards that may lead to faults in our avionics flight management and control system	Detail	Design Constraint	Where in our code is this design constraint evident (show the traceability)
Sensor Data Simulation Failures	Airspeed Sensor Simulation Errors	- Airspeed values generated outside of safe range. - Stuck values or unrealistic fluctuations. - Delays in data updates beyond the specified frequency.		
	Altitude Sensor Simulation Errors	- Altitude sensor does not update to detect rapid changes in altitude - Threshold for rapid changes will be >5 metres in a second - warning and >15 metres in a second is a automatic autopilot entry		
	Attitude Sensor Simulation Errors	- Incorrect pitch, roll, or yaw values generated, outside of the safe range. - Data values freezing or updating irregularly. - Discrepancies in attitude data leading to unrealistic aircraft behaviour.		
	Engine Parameter Simulation Errors	- Thrust values not matching the input commands. - Data not updating as frequently as required - every 500ms.		

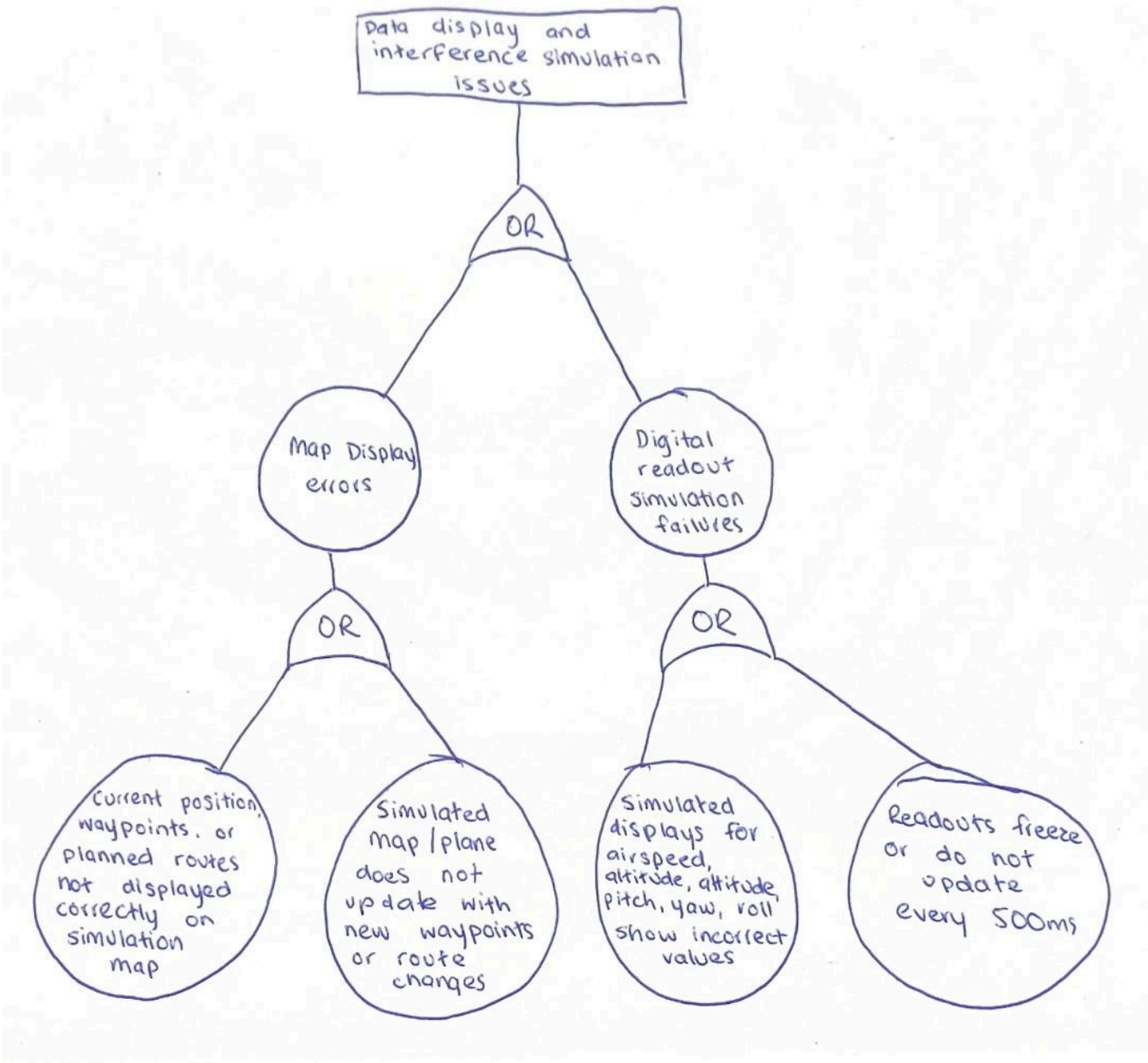
Autopilot System Simulation Failures	Autopilot Engagement/ Disengagement Issues	- Autopilot fails to engage when a simulated command is issued. - Autopilot disengages unexpectedly within the simulation. (Disengages without the command being given) - Status indicators for autopilot engagement are incorrect or delayed.		
	Manual Override Simulation Failures	- Delay or failure in reflecting manual control inputs. Manual altitude adjustment made is not reflected in simulation. - Manual speed adjustment made is not reflected in simulation. - Manual heading adjustment made is not reflected in simulation.		
	Control Signal Simulation Errors	- Control signals to control surfaces or engines are not simulated correctly. - Simulated control signals not verified within 200 milliseconds (signals delayed or lost). - Incorrect or no response to control signals in the simulation. (sensor data does not reflect the expected change from the control signal)		
Hazard Alerts Simulation Failures	Simulation of Alert System Malfunctions	- Simulated audible or visual alerts do not trigger correctly. - False hazard alerts generated in the simulation. - Emergency procedure checklists not displayed or incorrect in the simulation.		
Data Display and Interference	Map Display Errors	- Current position, waypoints, or planned routes not displayed correctly on the simulation map. - Simulated map does not update with new		

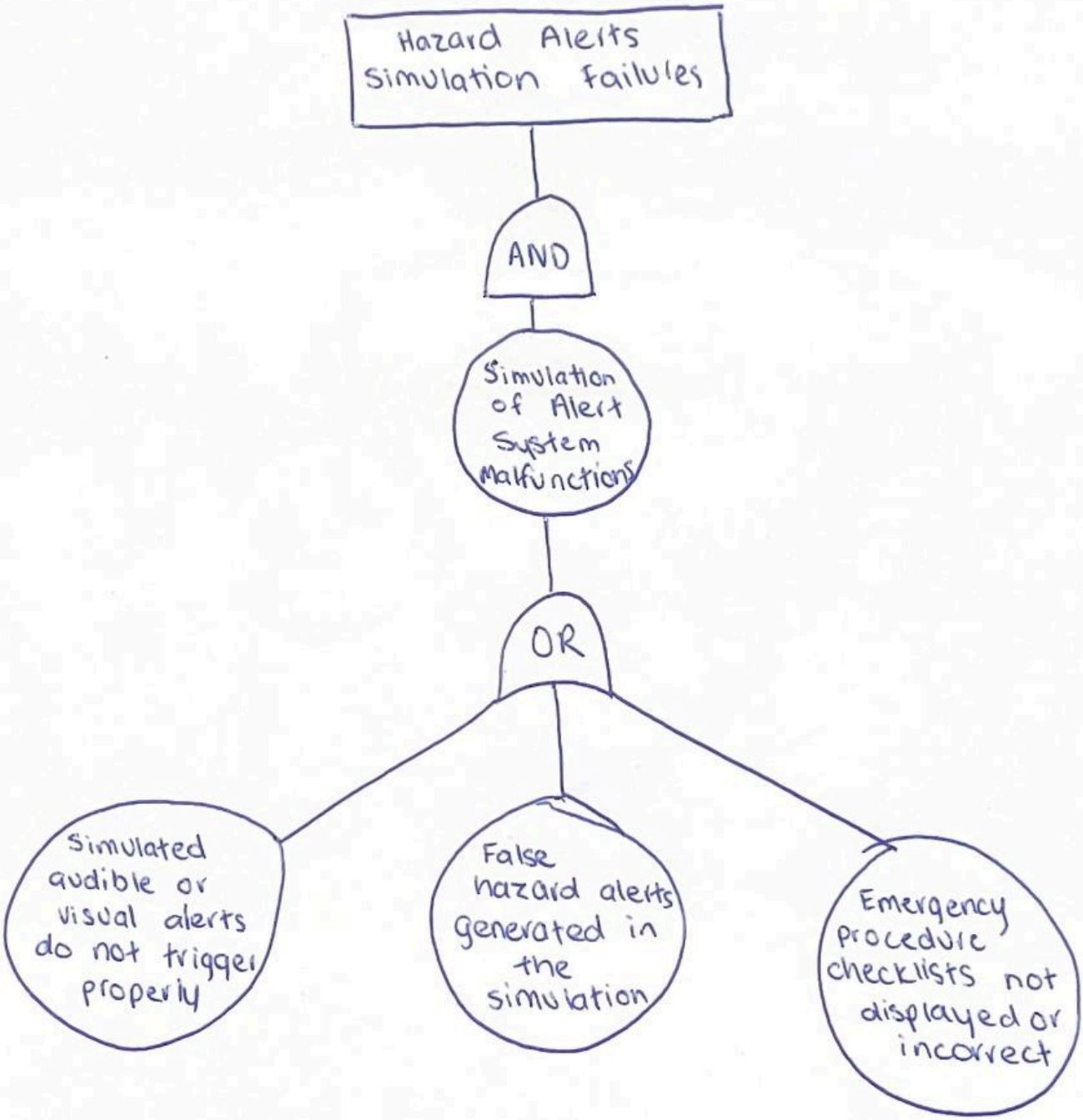
Simulation Issues		waypoints or route changes.		
	Digital Readout Simulation Failures	- Simulated displays for airspeed, altitude, pitch, roll, yaw, and engine parameters show incorrect values. - Readouts freeze or do not update at the specified frequency of 500 milliseconds.		
Control Signal Verification Failures	Simulation Execution Check Failures	- Simulation does not verify control signal execution correctly. - False negatives in execution check (signal executed correctly but marked as failed). - Multiple reattempts of failed signals in simulation causing errors.		
Redundant System Simulation Failures	2oo3 Redundant System Simulation Issues	- Incorrect logic decisions due to simulated sensor data discrepancies. - Failure in the simulated switch to backup sensors when the primary sensor fails.		
Miscellaneous Simulation Hazards	Software Bugs and Glitches in Simulation	- General software bugs causing the simulation to crash or freeze. - Interface glitches leading to incorrect data entry or data interpretation within the simulation.		

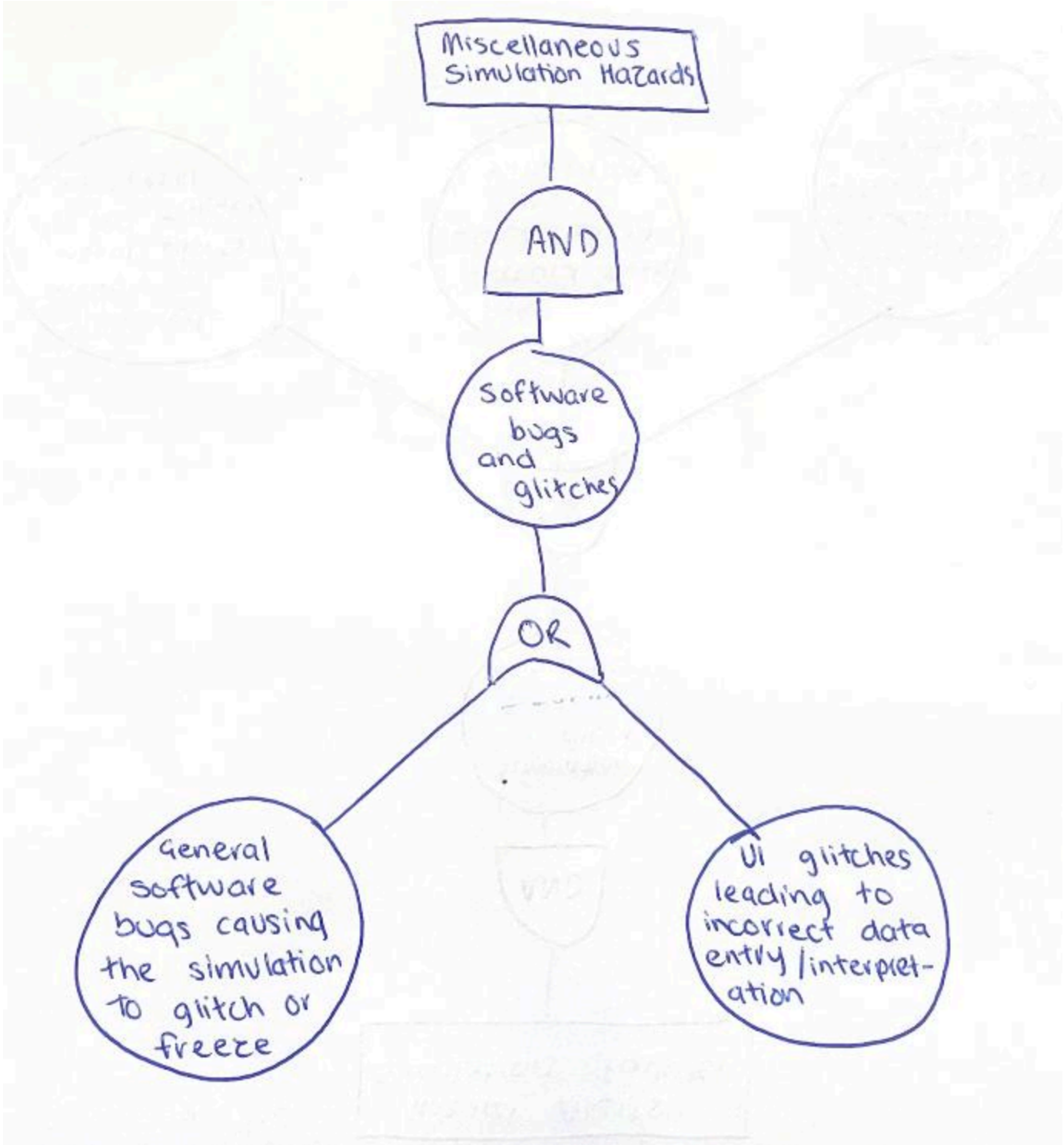
Fault Trees based on Hazards identified



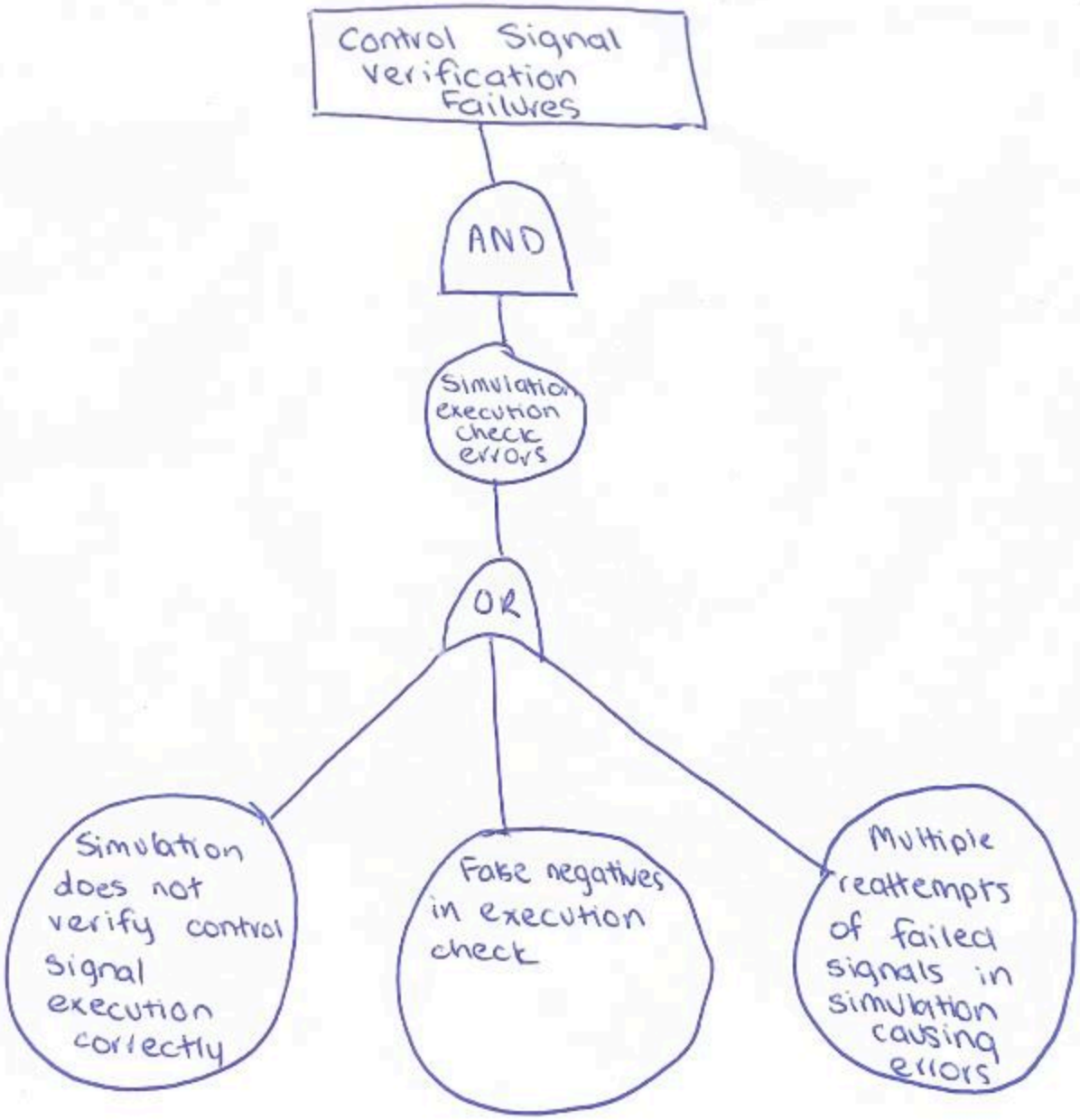

Autopilot System Simulation Failures
OR
Autopilot Engagement/ Dis Engagement Issues
Manual Override Simulation Failures
Control Signal Simulation Errors
OR
OR
OR
Autopilot fails to engage when command given
Autopilot disengages unexpectedly (without command being given)
Status indicators incorrect or delayed
manual altitude adjustment not reflected
manual heading adjustment not reflected
manual speed adjustment not reflected
Signals to control surfaces or engines not simulated correctly
controls not verified within 200ms
incorrect or no response to signals


Data display and interference simulation issues
OR
Map Display errors
Digital readout simulation failures
OR
OR
Current position, waypoints, or planned routes not displayed correctly on simulation map
Simulated map/plane does not update with new waypoints or route changes
Simulated displays for airspeed, altitude, altitude, pitch, yaw, roll show incorrect values
Readouts freeze or do not update every 500ms


Hazard Alerts Simulation Failules
AND
Simulation of Alert System Malfunctions
OR
Simulated audible or visual alerts do not trigger properly
False hazard alerts generated in the simulation
Emergency procedure checklists not displayed or incorrect


Miscellaneous Simulation Hazards
AND
Software bugs and glitches
OR
General software bugs causing the simulation to glitch or freeze
UI glitches leading to incorrect data entry / interpretation


Redundant System Simulation Failures
AND
2003 Redundant System Simulation Issues
OR
Incorrect logic decisions due to simulated sensor data discrepancies
Failure in the simulated switch to backup sensors when the primary sensor fails


Control Signal verification Failures
AND
Simulation execution check errors
OR
Simulation does not verify control signal execution correctly
False negatives in execution check
Multiple reattempts of failed signals in simulation causing errors

Minimal Cut Sets

The minimal cut sets that could cause our *Avionics Flight Management and Control System* to lead to a plane crash are:

1. Airspeed values outside of safe range **OR** stuck values/unrealistic fluctuations **OR** delays in data update beyond specified frequency
2. Thrust values not matching input **OR** data not updating every 500ms
3. Values stuck outside safe range **OR** sensor does not update to check rapid changes
4. Incorrect pitch, roll, yaw values generated **OR** data values freezing/updating irregularly **OR** discrepancies in attitude data leading to unrealistic behaviour
5. Autopilot fails to engage when command is given **OR** autopilot disengages unexpectedly **OR** status indicators incorrect/delayed
6. Manual altitude adjustment not reflected **OR** Manual speed adjustment not reflected **OR** Manual heading adjustment not reflected
7. Signals to control surfaces or engines not simulated correctly **OR** control signals not verified within 200ms **OR** incorrect/no response to signals
8. Current position, waypoints or planned routes not displayed correctly on simulation map **OR** simulated map/plane does not update with new waypoints or route changes
9. Simulated displays for airspeed, altitude, attitude, pitch, yaw, roll show incorrect values **OR** readouts freeze or do not update every 500ms
10. Simulated audible or visual alerts do not trigger properly **OR** false hazard alerts generated in simulation **OR** emergency procedure checklists not displayed or incorrect
11. General software bugs causing the simulation to glitch or freeze **OR** UI glitches leading to incorrect data entry/interpretation
12. Incorrect logic decisions due to simulated sensor data discrepancies **OR** Failure in the simulated switch to backup sensors when the primary sensor fails
13. Simulation does not verify control signal execution correctly **OR** false negatives in the execution check **OR** multiple reattempts of failed signals in simulation causing errors