Mälardalen University
M.Sc.Eng. Dependable Aerospace Systems
Västerås, Sweden

Project Course in Dependable Systems
22.5 credits

Safety Assessment

Responsible
Esaias Målqvist
emt21001@student.mdu.se

Contributors

Andrea Haglund
ahd20002@student.mdu.se

Yonatan Michael Beyene
yme21001@student.mdu.se

Claire Namatovu
cnu21001@student.mdu.se

Emily Zainali
ezi21001@student.mdu.se

Examiner: Luciana Provenzano

December 5, 2025

Title: Safety Assessment		ID: SM-05 Version: 1.1
Author: Esaias Målqvist	Role: Safety Manager	Page 1 of 7

DOCUMENT APPROVAL

Name	Role	Version	Date	Signature
Andrea Haglund	Chief Engineer	1.1	2025-12-05	
Yonatan Michael Beyene	Q&C Manager	1.1	2025-12-05	

DOCUMENT CHANGE RECORD

Version	Date	Reason for Change	Pages / Sections Affected
0.1	2025-11-10	Version for internal review	
1.0	2025-11-14	Version for first release	
1.1	2025-11-25	changed according to feedback	All

Contents

Glossary

ARP4761A
: Aerospace Recommended Practice (ARP) providing guidelines for conducting the safety assessment process on civil aircraft systems and equipment, covering techniques such as FHA, FMEA, and FTA to support system safety analysis throughout the development lifecycle. 3

FHA
: Functional Hazard Analysis. 3

FMEA
: Failure Modes and Effects Analysis. 3

FTA
: Fault Tree Analysis. 3

1 Introduction

This document is based on activites from ARP4761A and addresses four potential failures:

- Fatal ground collision
- Air collision with a third party
- Air collision with an agent
- Erroneous communication

A fault tree analysis (FTA) is used to illustrate the causal paths leading to each failure. To fully describe these failures, certain functions outside the scope of the protocol are included. These functions are shown in yellow in the fault trees, while functions related to the protocol are shown in blue. This distinction clearly illustrates the protocol's impact on system safety.
The FTAs are based on the current protocol design and may require updates if changes are made later.

1.1 Purpose

This document describes how failures may occur and how the protocol contributes to improving system safety. It is intended to serve as evidence that the system meets its safety goals.

1.2 Related Documents

Document ID	Document Title
SM-01	Safety Management Plan [1]
SM-06	Safety Goals & Requirements [2]

Table 1: Related documents

2 Failures

2.1 Fatal Ground Collision

This failure occurs when an agent collides with the ground and causes a fatal accident. It only applies in cases where a person is killed as a result of the crash.

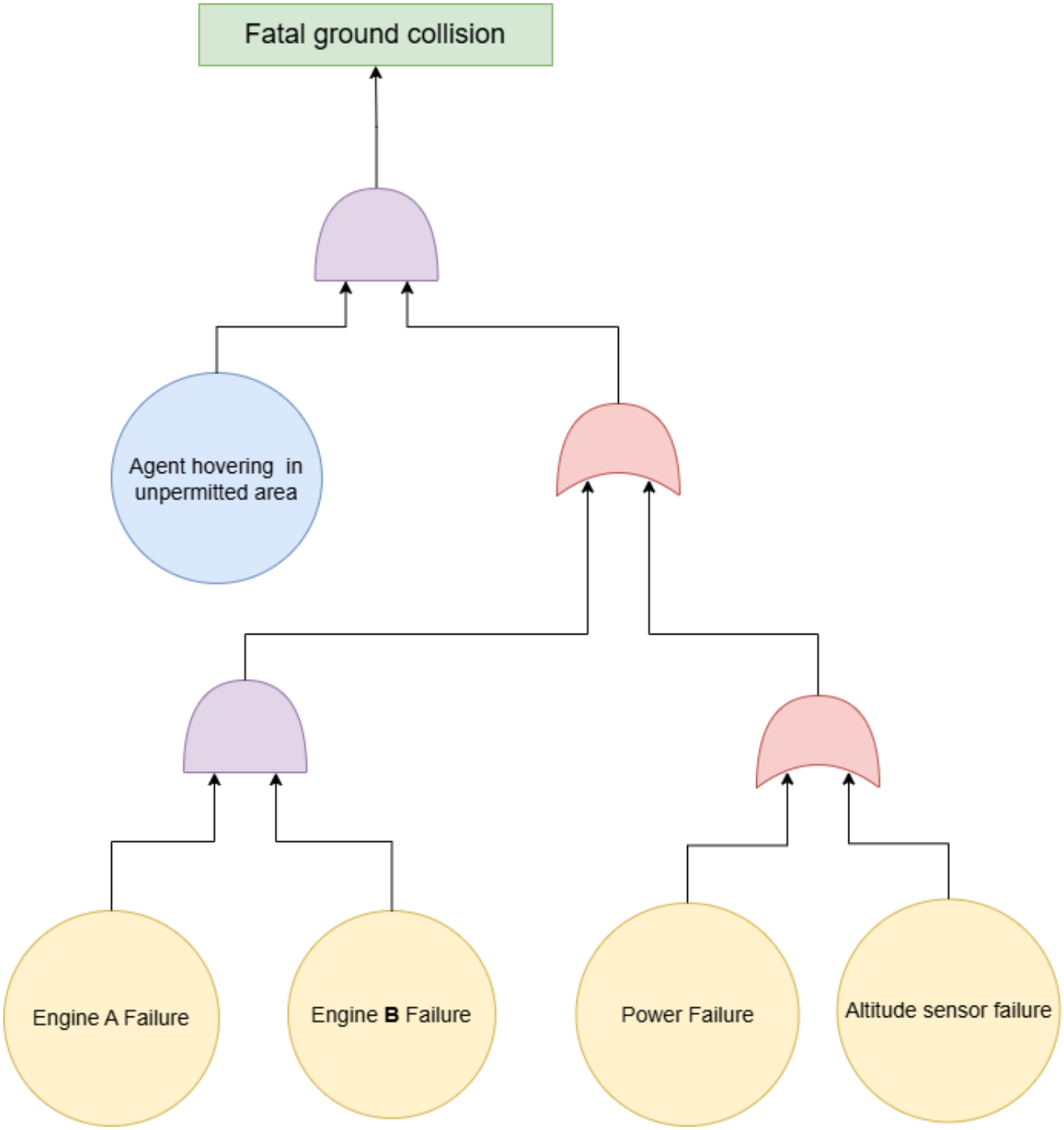

Figure 1: FTA for Fatal Ground Collision.

For a fatal ground collision to occur, the agent must experience a hardware failure severe enough to prevent it from remaining airborne. In addition, the agent must have entered a restricted area as defined by the protocol—such as above the subject, over non-rural areas, or at the starting location before evacuation is complete. Under these conditions, the system is protected from single-point failures.

2.2 Air Collision With Third Party

This failure occurs when an agent collides with a third-party aircraft, such as an aeroplane or helicopter.

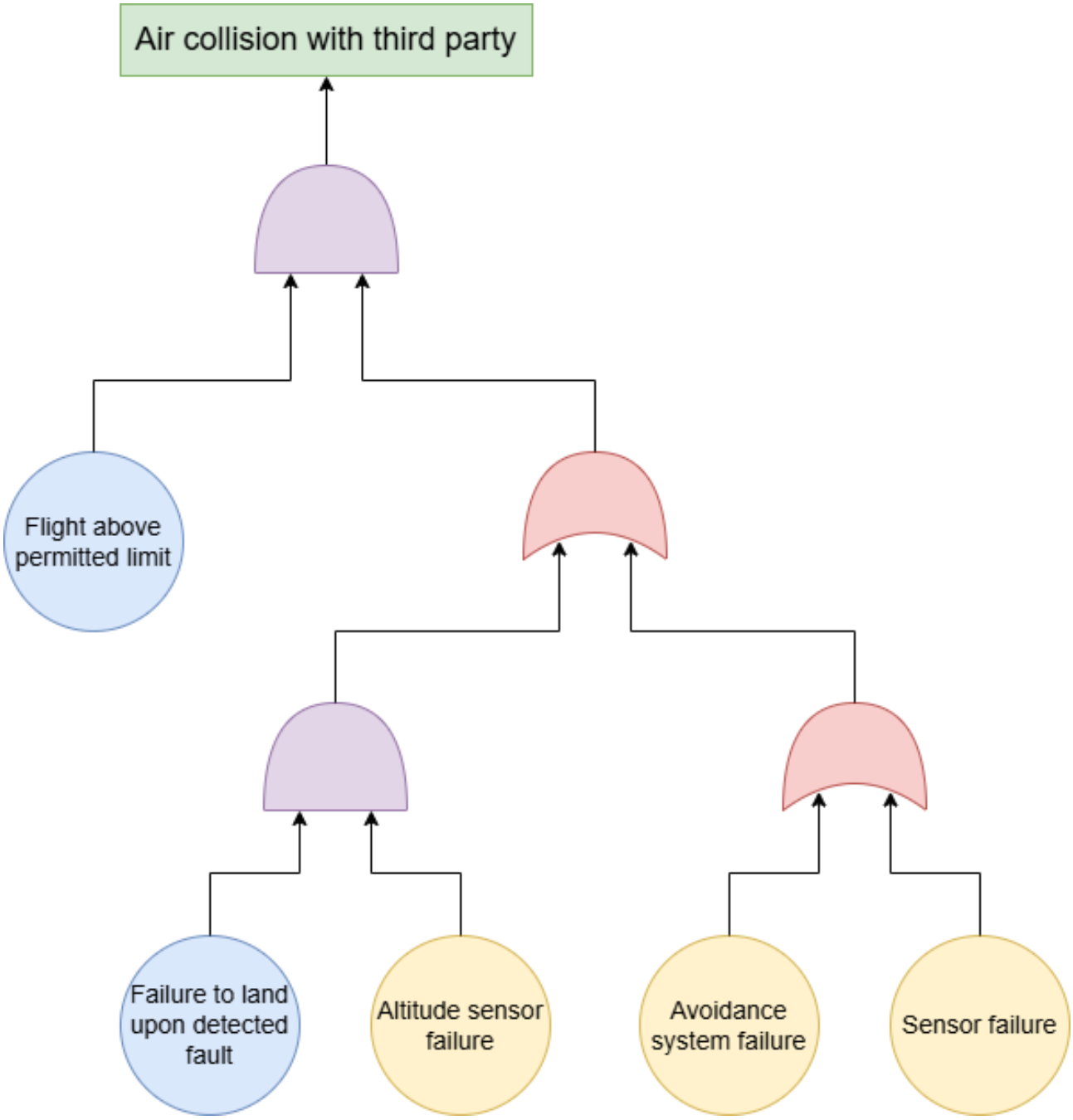

Figure 2: FTA for Third Party Air Collision.

For an air collision with a third party to occur, the agent must either lose its ability to detect and avoid obstacles due to a hardware malfunction while exceeding the maximum altitude defined in the safety requirements, or lose its ability to accurately determine its own altitude, fail to land, and subsequently fly above the permitted limit. Flying above this maximum altitude is a prerequisite for such a failure, as the altitude limit is set to match the lowest allowed operating altitude for manned aircraft in the intended use area (rural regions).

2.3 Air Collision With Agent

This failure occurs when 2 or more agents collide in the air.

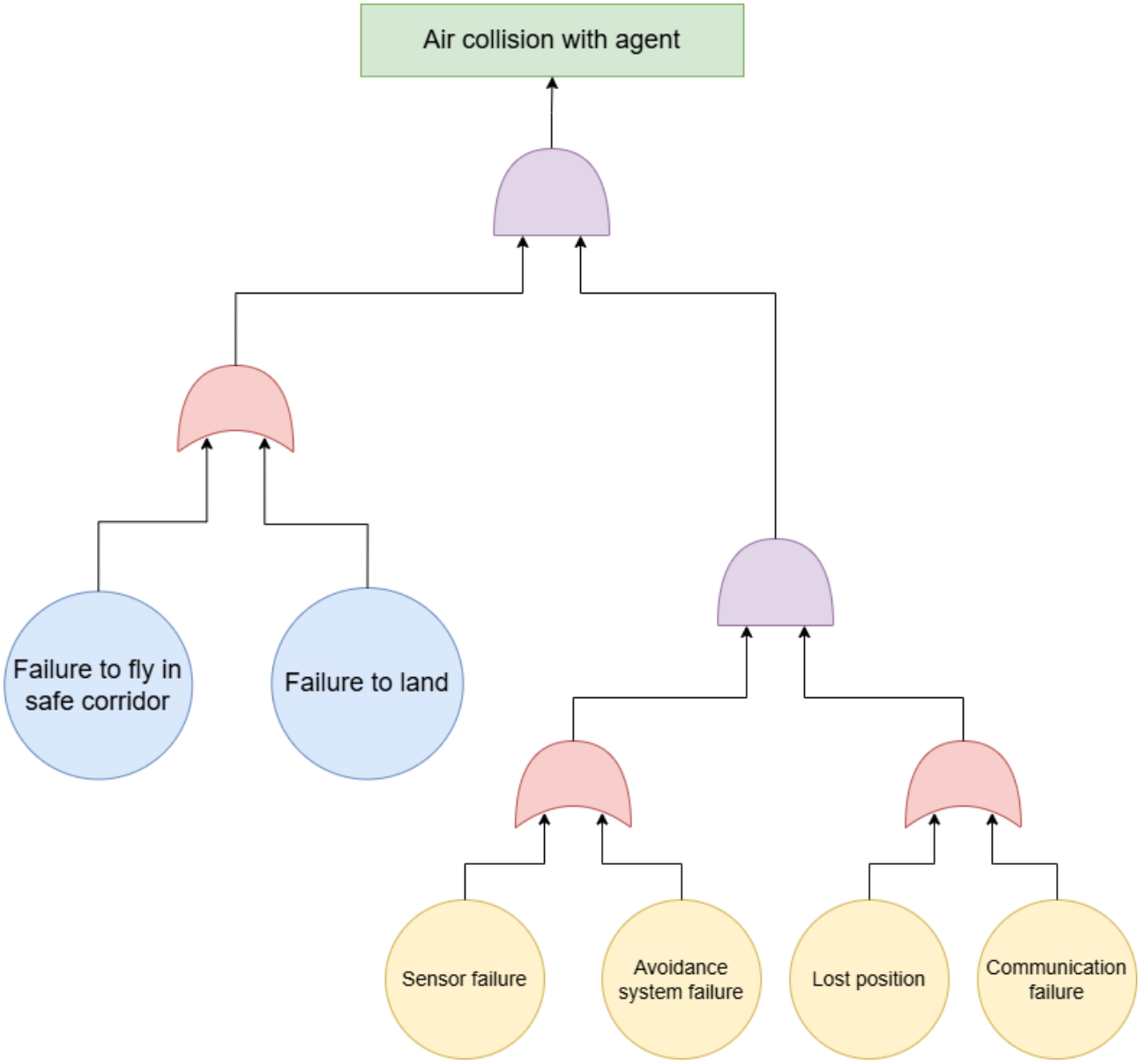

Figure 3: FTA for Air Collision With Agent.

A mid-air collision between agents can only occur if they are unaware of each other's positions. This situation may arise when the positioning system fails or when all communication between agents is lost. In addition, the sensors responsible for detection and avoidance must also be inoperative. Finally, a collision becomes likely if the agents do not execute their safety protocols—such as initiating an emergency landing upon detecting a positioning fault or returning to base via a designated safe corridor.

2.4 Erroneous Communication

Erroneous communication occurs when important information is wrong or misleading. Examples of this could be false positives, untrue status reports, and more.

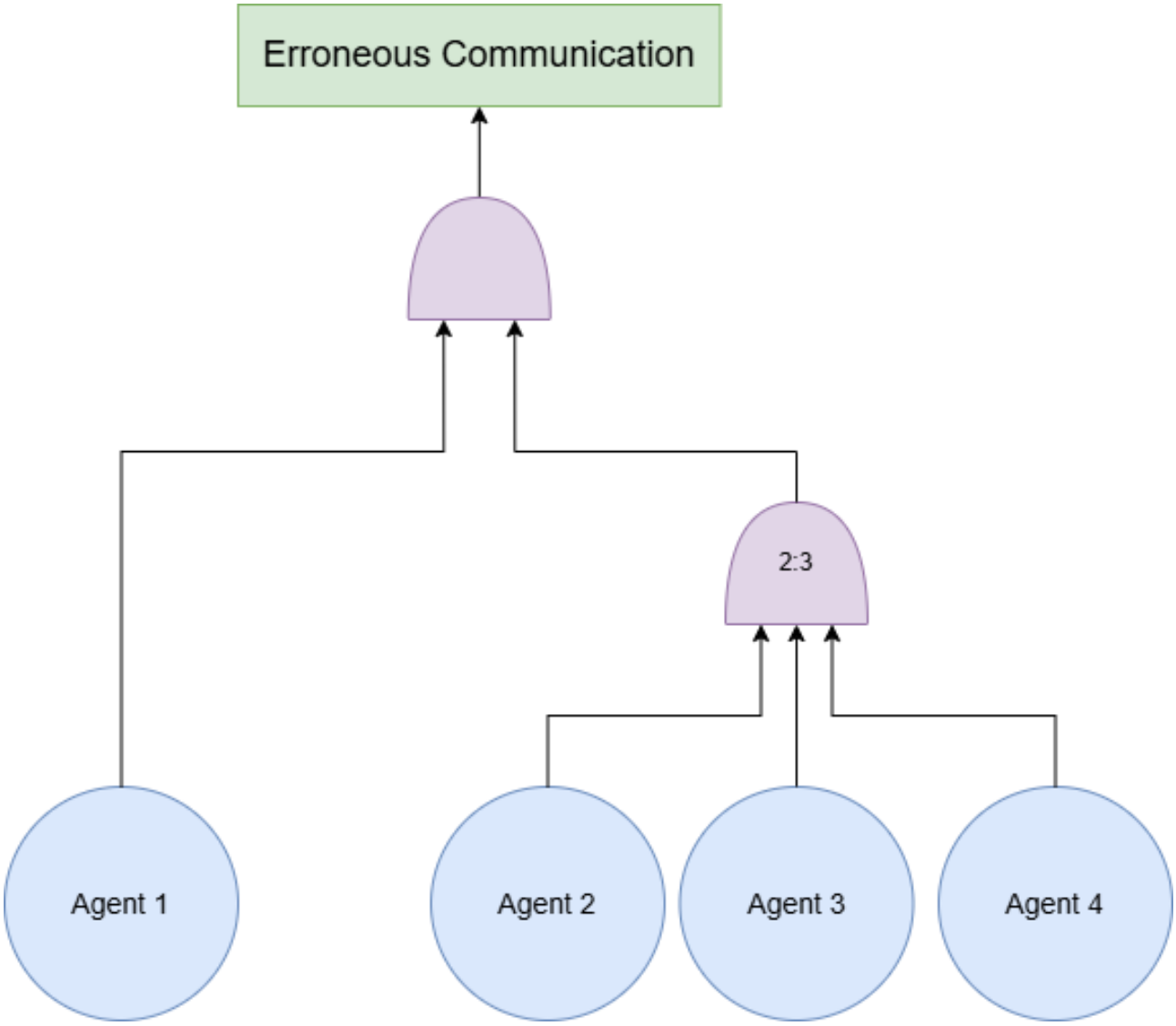

Figure 4: FTA for Erroneous Communication.

To prevent faulty messages from propagating throughout the swarm, a voting system is implemented. If an agent sends out an important message, at least 3 other agents must receive it and vote among each other on what message to relay to the rest of the swarm. If an agent sends a "subject found" message, at least 3 other agents must confirm the subject before the mission is complete.

References

[1] E. Målqvist, *Safety Management Plan*, Intelligent Replanning Drone Swarm, Oct. 4 2025, Version 1.0.
[2] ——, *Safety Goals And Requirements*, Intelligent Replanning Drone Swarm, Oct. 4 2025, Version 1.0.