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

Project Course in Dependable Systems
22.5 credits

Safety Assurance Case

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

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	YMB

DOCUMENT CHANGE RECORD

Version	Date	Reason for Change	Pages / Sections Affected
0.1	2025-11-12	Version for internal review	
0.2	2025-11-12	Spelling and grammar	All
1.0	2025-11-14	Release version	All
1.1	2025-11-25	Updated according to feedback	All

Contents

Glossary

ARC
initial Air Risk Class. 5

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. 4

FHA
Functional Hazard Analysis. 3, 5

FMEA
Failure Modes and Effects Analysis. 3

FSA
Flight Safety Assessment. 4

FTA
Fault Tree Analysis. 3, 5

GSN
Goal Structuring Notation. 2, 6

iGRC
intrinsic Ground Risk Class. 4

PDSSA
Preliminary Drone Swarm Safety Assessment. 5

PSA
Preliminary Safety Assessment. 5

SA
Safety Assessment. 5

SAC
Safety Assurance Case. 4

SAIL
Specific Assurance and Integrity Level. 5

SAR
Search and Rescue. 4

SORA
JARUS guidelines on Specific Operations Risk Assessment (SORA). SORA is a guideline for creating UAVs. 4

TMPR
Tactical Mitigation Performance Requirement. 5

UAV
Unmanned Aerial Vehicle. 4

1 Introduction

1.1 Purpose

The safety assurance case (SAC) will use documents produced throughout the project to demonstrate that the system is acceptably safe. The document will describe the system overview, safety objectives and arguments. The Safety case will be described using GSN argumentation.

1.2 Related Documents

Document ID	Document Title
SM-01	Safety Management Plan [1]
SM-03	Preliminary Safety Assessment [2]
SM-04	Flight Safety Assessment [3]
SM-05	Safety Assessment [4]
SM-06	Safety goals and requirements [5]
VVP-01	Test Case - Drone Swarm Requirements [6]
VVP-05	Verification - Safety Requirements [7]
VVP-06	Verification - Safety Goals [8]

Table 1: Related documents.

2 Safety Objectives

1) The system shall not cause unnecessary injury or bodily harm to people.
2) The system shall comply with the relevant requirements and processes defined in:
   - **SORA** (Specific Operations Risk Assessment), as applicable to operational risk and containment.
   - **ARP4761A**, for safety assessment processes and analysis methods.

3 System Description

The system under consideration is a communication and control protocol for a Unmanned Aerial Vehicle (UAV) operating collaboratively in Search and Rescue (SAR) missions.

The protocol governs:

- **Inter-drone communication**, including coordination and data exchange.
- **Behavioral logic**, including formation management, area coverage, and fault response.

4 Safety Objective

Goal: It is demonstrated that the system is acceptably safe for its intended operation.
Strategy: Safety will be demonstrated by:

1) The identified potential hazards through structured analysis.
2) The safety goals and safety requirements derived from the identified hazards.
3) The verification of the safety goals and requirements.
4) The effect of the safety requirements on the system.

5 Safety Activities to Identify Hazards

5.1 Activities Based on SORA

Relevant safety activities defined under SORA are documented in the Flight Safety Assessment (FSA). These include:

- intrinsic Ground Risk Class (iGRC) determination.

- initial Air Risk Class (ARC)determination.
- Tactical Mitigation Performance Requirement (TMPR) and robustness level assessment.
- Specific Assurance and Integrity Level (SAIL) determination.
- Containment requirements definition.

5.2 Activities Based on ARP4761A

Relevant safety activities derived from ARP4761A are documented in the Preliminary Safety Assessment (PSA), these include:

- Functional Hazard Analysis (FHA).
- Preliminary Drone Swarm Safety Assessment (PDSSA).

5.3 Safety Goal and Requirement Elicitation

Safety goals and requirements are documented in safety goals and requirement document (SM-06).

5.4 Verification

All verification can be found in these three documents:

- Test Case - Drone Swarm Requirements.
- Verification - Safety Requirements.
- Verification - Safety Goals.

5.5 Mitigation effects

The requirements' effect on the system is documented in the Safety Assessment (SA) document and mostly consists of Fault Tree Analysis (FTA).

6 Argumentation

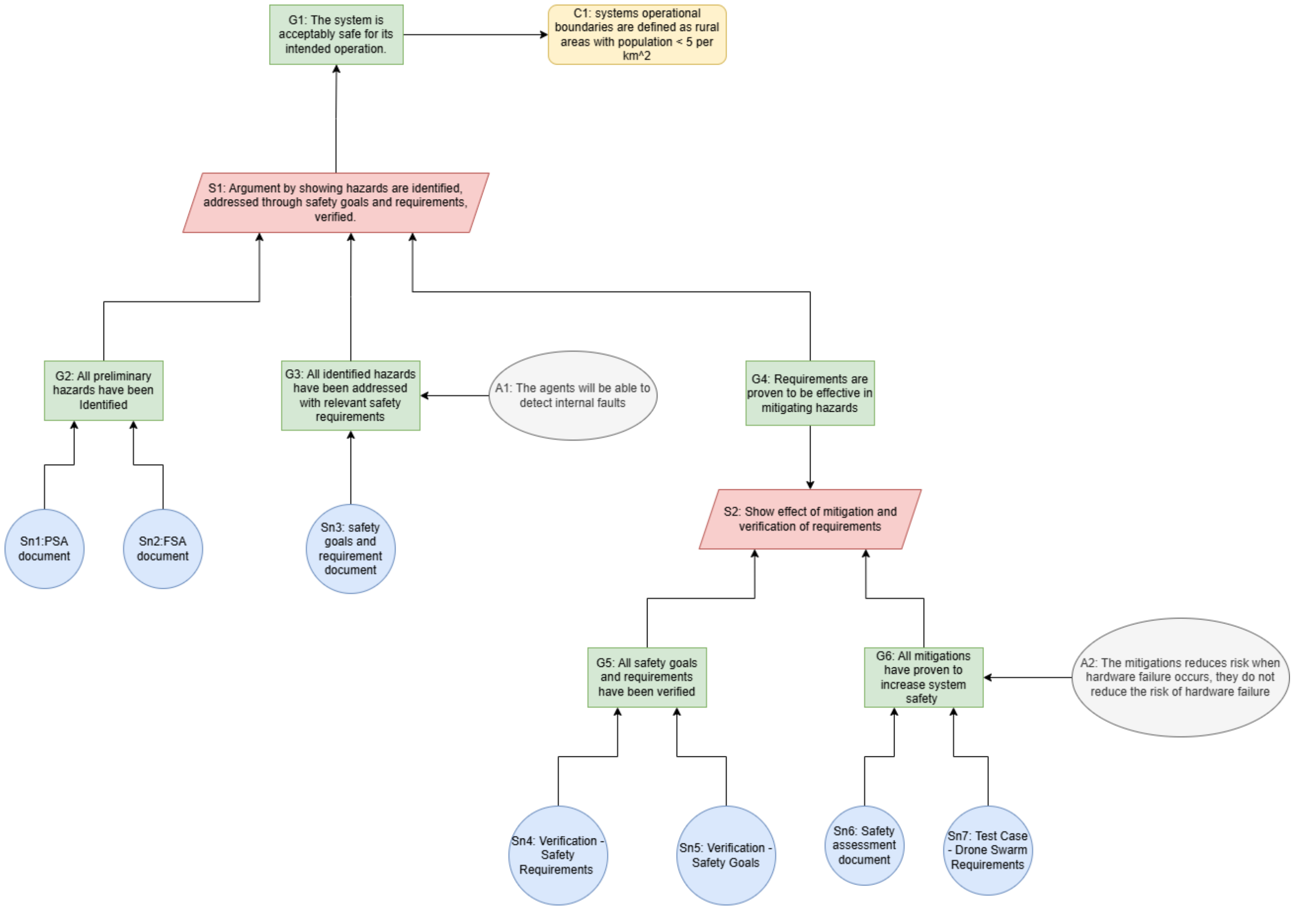
G1: The system is acceptably safe for its intended operation.
C1: systems operational boundaries are defined as rural areas with population < 5 per km^2
S1: Argument by showing hazards are identified, addressed through safety goals and requirements, verified.
G2: All preliminary hazards have been Identified
G3: All identified hazards have been addressed with relevant safety requirements
A1: The agents will be able to detect internal faults
G4: Requirements are proven to be effective in mitigating hazards
Sn1:PSA document
Sn2:FSA document
Sn3: safety goals and requirement document
S2: Show effect of mitigation and verification of requirements
G5: All safety goals and requirements have been verified
G6: All mitigations have proven to increase system safety
A2: The mitigations reduces risk when hardware failure occurs, they do not reduce the risk of hardware failure
Sn4: Verification - Safety Requirements
Sn5: Verification - Safety Goals
Sn6: Safety assessment document
Sn7: Test Case - Drone Swarm Requirements

Figure 1: GSN

6.1 Goal Structuring Notation (GSN) statements

6.1.1 Goals

- G1: The system is acceptably safe for its intended operation.
- G2: All preliminary hazards have been identified.
- G3: All identified hazards have been addressed with relevant safety requirements.
- G4: Requirements are proven to be effective in mitigating hazards.
- G5: All safety goals and requirements have been verified.
- G6: All mitigations have proven to increase system safety.

6.1.2 Strategy

- S1: Argument by showing hazards are identified, addressed through safety goals and requirements, verified.
- S2: Show effect of mitigation and verification of requirements.

6.1.3 Assumptions

- A1: The agents will be able to detect internal faults.
- A2: The mitigations reduces risk when hardware failure occurs, they do not reduce the risk of hardware failure.

6.1.4 Context

- C1: systems operational boundaries are defined as rural areas with population < 5 per km^2.

6.1.5 Solutions

- Sn1: PSA document [2].
- Sn2: FSA document [3].
- Sn3: Safety goals and requirement document [5].
- Sn4: Verification - Safety Requirements [7].
- Sn5: Verification - Safety Goals [8].
- Sn6: Safety assessment document [4].
- Sn7: Test Case - Drone Swarm Requirements [6].

References

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

[2] ——, *Preliminary Safety Assessment*, Intelligent Replanning Drone Swarm, Nov. 4 2025, Version 1.0.

[3] ——, *Flight Safety Assessment*, Intelligent Replanning Drone Swarm, Nov. 4 2025, Version 1.0.

[4] ——, *Safety Assessment*, Intelligent Replanning Drone Swarm, Nov. 4 2025, Version 1.0.

[5] ——, *Safety Goals And Requirements*, Intelligent Replanning Drone Swarm, Oct. 4 2025, Version 1.0.

[6] E. Zainali, *Test Case - Drone Swarm Requirements*, Intelligent Replanning Drone Swarm, Nov. 4 2025, Version 1.0.

[7] ——, *Verification - Safety Requirements*, Intelligent Replanning Drone Swarm, Nov. 4 2025, Version 1.0.

[8] ——, *Verification - Safety Goals*, Intelligent Replanning Drone Swarm, Nov. 4 2025, Version 1.0.