



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

---

Project Course in Dependable Systems
22.5 credits

# Preliminary Safety Assurance Case

**Responsible**
Esaias Målqvist
*emt21001@student.mdu.se*

---

**Contributors**

Andrea Haglund
*ahd20002@student.mdu.se*

Yonatan Michael Beyene
*yme21001@student.mdu.se*

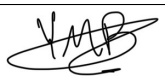
Claire Namatovu
cnu21001@student.mdu.se

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 |  |

# DOCUMENT CHANGE RECORD

| Version | Date | Reason for Change | Pages / Sections Affected |
|---|---|---|---|
| 0.1 | 2025-11-11 | Version for internal review | |
| 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. 4

**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. 5

**iGRC**
: intrinsic Ground Risk Class. 4

**PDSSA**
: Preliminary Drone Swarm Safety Assessment. 5

**PSA**
: Preliminary Safety Assessment. 4

**PSAC**
: Preliminary Safety Assurance Case. 4

**SA**
: Safety Assessment. 5

**SAIL**
: Specific Assurance and Integrity Level. 4

**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. 4

**UAV**
: Unmanned Aerial Vehicle. 4

# 1 Introduction

## 1.1 Purpose

This Preliminary Safety Assurance Case (PSAC) outlines the overall safety objectives for the system, the approach that will be used to achieve those objectives, and the evidence that will be developed to demonstrate compliance. It also provides a brief description of the system under consideration.

## 1.2 Related Documents

| Document ID | Document Title |
|---|---|
| SM-01 | Safety Management Plan [1] |

Table 1: Related documents.

# 2 Safety Objectives

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 swarm of 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 Preliminary Safety Argument

**Goal:** The system shall be demonstrated to be acceptably safe for its intended operation.
**Strategy:** Safety will be demonstrated by:

1) Identifying potential hazards through structured analysis.
2) Addressing identified hazards via safety goals and derived requirements.
3) Verifying the implementation and effectiveness of mitigations.

# 5 Planned Safety Activities

## 5.1 Activities Based on SORA

Safety activities defined under SORA will be 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

Safety activities derived from ARP4761A will be 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 derived requirements will be captured and maintained in the **requirements management database** to ensure traceability.

## 5.4 Safety Verification

Verification activities will be documented in the Safety Assessment (SA) document and mostly consists of Fault Tree Analysis (FTA).

# 6 Safety Evidence Plan

Planned safety evidence will include results from the following assessments:

## Preliminary Safety Assessment (ARP4761A-based):

- FHA results.
- PDSSA results.

## Flight Safety Assessment (SORA-based):

- iGRC determination results.
- ARC determination results.
- TMPR and robustness assessment results.
- SAIL determination results.
- Containment requirements results.

## Additional Documentation:

- Safety goals and requirements.
- Verification evidence (FTA, test reports).

# 7 Preliminary Safety Case Structure (GSN Overview)

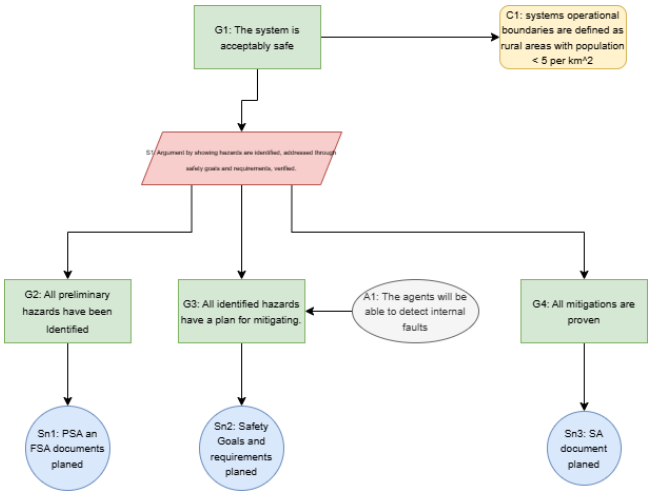



Figure 1: Goal Structuring Notation (GSN).

# References

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