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

Project Course in Dependable Systems
22.5 credits

Safety Management Plan

Responsible
Esaias Målqvist
emt21001@student.mdu.se

Contributors

Andrea Haglund
ahd20002@student.mdu.se

Yonatan Michael Beyene
yme21001@student.mdu.se

Examiner: Luciana Provenzano

December 5, 2025

DOCUMENT APPROVAL

Name	Role	Version	Date	Signature
Andrea Haglund	Chief Engineer	1.1	2025-11-14	
Yonatan Michael Beyene	Q&C Manager	1.1	2025-11-14	

DOCUMENT CHANGE RECORD

Version	Date	Reason for Change	Pages / Sections Affected
0.1	2025-09-30	Version for internal review	
0.2	2025-10-03	Version for review	
1.0	2025-10-05	Version for public release	All
1.1	2025-10-05	Updated for changes during the project	All

Contents

Glossary

ARC
initial Air Risk Class. 2, 9–11

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. 6

CE
Chief Engineer. 8

CoFFE
Combined Functional Failure Effects. 10

DSSA
Drone Swarm Safety Assessment. 2, 9, 11

Excel
Microsoft's spreadsheet software for organising, analysing, and visualising data. 7

FHA
Functional Hazard Assessment. 2, 3, 9, 10

FMEA
Failure Modes and Effects Analysis. 3, 9, 10

FSA
Flight Safety Assessment. 6, 10, 11

FTA
Fault Tree Analysis. 3, 9, 11

iGRC
intrinsic Ground Risk Class. 2, 9–11

IRDS
Intelligent Replanning Drone Swarm. 5, 6

latex
A mark up language specially suited for scientific documents. 7

PDSSA
Preliminary Drone Swarm Safety Assessment. 2, 9, 10

PSA
Preliminary Safety Assessment. 6, 9, 10

QCM
Quality & Configuration Manager. 8

RM
Requirements Manager. 8

SA
Safety Assessment. 6, 11

SAIL
Specific Assurance and Integrity Level. 2, 9, 11

SAR
Search and Rescue. 5

SM
Safety Manager. 6, 8

SMP
Safety Management Plan. 5

SORA
JARUS guidelines on Specific Operations Risk Assessment (SORA). A structured methodology to assess and mitigate risks for specific UAS operations, ensuring safe conduct in complex or beyond-visual-line-of-sight environments. 6, 7

TMPR
Tactical Mitigation Performance Requirement. 2, 9, 11

UA
Unmanned Aircraft. 10

UAS
Unmanned Aircraft System. 4

UAV
Unmanned Aerial Vehicle. 5, 6, 11

V&V
Validation & Verification. 5, 7, 11

VVM
Validation & Verification Manager. 8

1 Introduction

This Safety Management Plan (SMP) defines the framework for conducting safety evaluations within the Intelligent Replanning Drone Swarm (IRDS) project. It specifies the standards to be applied, the safety assessment techniques to be used, and the deliverables to be produced in order to systematically address safety throughout the project lifecycle.

This plan follows the guidelines of ARP4754A (system development safety framework) [1] and JARUS SORA (operational safety framework for Unmanned Aerial Vehicle (UAV)s) [2]. Together, these standards provide the basis for identifying hazards, classifying risks, and determining the level of assurance required.

This document is part of the project's set of management plans (Requirements, Validation & Verification (V&V), Quality, and Configuration). While those plans govern related processes, this plan focuses specifically on safety management and how safety evidence will be produced, documented, and reviewed.

1.1 Purpose

The purpose of this plan is to define how safety will be managed, analysed, and documented throughout the project, establish responsibilities, activities, and review points to ensure safety considerations are integrated into requirements, design, testing, and assurance activities, provide a consistent framework for deriving safety goals and requirements, and for collecting the evidence needed to support Preliminary and Final Safety Assurance Cases, and serve as a reference for project members and stakeholders on how safety will be assured in both the UAV swarm and its Search and Rescue (SAR) operations.

1.2 Related Documents

Document ID	**Document Title**
PP-01	Project Plan [3]
CM-01	Configuration Management Plan [4]
QM-01	Quality Management Plan [5]
RM-01	Requirements Management Plan [6]
VV-01	Validation & Verification Management Plan [**?**]
SORA	JARUS guidelines on Specific OperationsRisk Assessment [2]
ARP4761A	AEROSPACE RECOMMENDED PRACTICE revision A [7]

Table 1: Related documents.

2 Scope

This plan applies to all activities and deliverables of the IRDS project that concern system and operational safety. It covers the identification, analysis, and mitigation of hazards, as well as the derivation and validation of safety goals and requirements.

This plan applies to:

- Development activities (hazard analysis, safety assessment, and assurance argumentation).
- Operational aspects relevant to Search and Rescue (SAR) missions, including swarm behaviour, task reallocation, and containment.
- Safety artefacts (hazard log, analyses, goals, requirements, and assurance cases) produced and controlled within the project.

This plan does not cover:

- Hardware manufacturing safety aspects beyond simulation (e.g., propeller integrity, battery handling).
- Regulatory certification of UAVs for commercial flight.
- Non-safety dependability aspects (e.g., performance, maintainability), which are addressed in other plans.

2.1 Objectives

The objectives of this plan are to:

- Ensure that safety risks are systematically identified, analysed, and mitigated.
- Guarantee that all safety goals and requirements are documented, traceable, and verifiable.
- Provide quantified safety objectives as benchmarks to guide hazard analysis and risk classification.

System safety objectives are:

- No single failure shall lead to loss of life.
- Probability of a fatal crash shall be less than 1E-6 fatalities per flight hour.
- Probability of a mid-air collision with third parties shall be less than 1E-9 per flight hour.

2.2 Deliverables

The safety documents that shall be produced throughout the project are the following:

ID	Title	Description	Responsible
SM-01	Safety Management Plan	Outlines the activities and deliverables to be produced to ensure the safety of the project.	Safety Manager (SM)
SM-02	Preliminary Safety Assurance Case	Early arguments for safety.	SM
SM-03	Preliminary Safety Assessment (PSA)	Focuses on activities outlined in ARP4761A [7]. The PSA's goal is to identify potential hazards, both internal and external, that could pose risks to search target(s) or third parties.	SM
SM-04	Flight Safety Assessment (FSA)	Focuses on the potential risks that the UAV swarm may pose to third parties. The FSA's goal is to define the flight boundaries. The activities follow SORA [2] guidelines.	SM
SM-05	Safety Assessment (SA)	Assesses the safety of the system implementation. Its focus is on identifying flaws in the implementation. The document is based on activities outlined in ARP4761A [7].	SM
SM-06	Safety Goals & Requirements	Used to compile safety goals derived from other safety activities.	SM
SM-07	*(Final)* Safety Assurance Case	Builds on the Preliminary safety assurance case with more argumentation and evidence.	SM

Table 2: Deliverables.

3 Methodology

The safety management activities in this project are based on ARP4754A [1], ARP4761A [7], and the JARUS SORA methodology [2].

SORA provides a structured approach to evaluating risks to third parties in the air and on the ground, and will be used to determine risk classifications (iGRC, ARC, TMPR, SAIL) and containment requirements. While SORA does not directly address the safety of the person being searched for, this aspect will be considered within the project's own hazard analysis.

ARP4761A provides techniques such as Functional Hazard Analysis (FHA), Fault Tree Analysis (FTA), and Failure Modes and Effects Analysis (FMEA), which will be applied to identify potential system-level weaknesses, including risks arising from communication protocols and navigation failures.

ARP4754A ensures that safety assessment results are systematically integrated into system development, requirements definition, and verification activities.

Safety analyses and documentation will be prepared in latex, with hazard logs initially captured in Excel.

To ensure consistency, safety goals and safety requirements will be transferred to the project's requirements database (SQLite, as defined in RM-01 [6]). This allows hazards, safety goals, requirements, and V&V test cases to be linked with full traceability.

Each hazard entry will be assigned a unique ID and shall trace to at least one safety goal, one requirement ID, and one V&V test case.

This methodology ensures that both operational safety (via SORA) and system-level safety (via ARP4754A/ARP4761A) are addressed in a structured and traceable way, with safety evidence captured in a form that supports the Safety Assurance Cases.

4 Safety Organisation & Responsibilities

Role	Responsibilities	Authority
Safety Manager (SM)	Lead hazard analyses. Define safety goals and requirements. Maintain hazard log and safety case documentation. Coordinate with RM, VVM, and QCM for traceability and assurance evidence.	Can propose new safety requirements and mitigation strategies; drafts Preliminary and Final Safety Assurance Cases.
Chief Engineer (CE)	Ensure safety is integrated into system design and architecture. Provide system-level input for hazard analysis.	Approves all safety deliverables before baseline; has final authority to accept or reject safety artefacts.
Validation & Verification Manager (VVM)	Define and execute test cases linked to safety requirements. Ensure safety requirements are verifiable and tested under realistic conditions (e.g., fault injection).	Can accept or reject test evidence for safety requirements; collaborates with SM to confirm requirement coverage.
Quality & Configuration Manager (QCM)	Audit and review safety artefacts for compliance with quality standards. Ensure all safety documents and logs are version-controlled and baselined.	Can block release of safety artefacts that fail quality or configuration control; ensures reviews are documented.
Requirements Manager (RM)	Translate safety goals into formal requirements in the requirements database. Maintain traceability between hazards, goals, requirements, and design artefacts.	Can create, update, and baseline safety requirements; collaborates with SM to ensure completeness.

Table 3: Project roles and their safety related responsibilities and authorities.

5 Activities

The safety analysis will use the following activities:

Project Plan Ref.	Title
TR-02	Functional Hazard Assessment (FHA)
TR-03	Preliminary Drone Swarm Safety Assessment (PDSSA)
TR-04	Determination of the intrinsic Ground Risk Class (iGRC)
TR-05	Determination of the initial Air Risk Class (ARC)
TR-06	Tactical Mitigation Performance Requirement (TMPR) and Robustness Levels
TR-07	Specific Assurance and Integrity Level (SAIL) determination
TR-08	Determination of Containment requirements
TR-09	Drone Swarm Safety Assessment (DSSA)
-	Preliminary Safety Assurance Case
(TR-09)	Failure Modes and Effects Analysis (FMEA)
(TR-09)	Fault Tree Analysis (FTA)
(TR-09)	Safety Assurance Case
TR-01	Safety Goals & Safety Requirements
(TE-03)	Final Safety Report (Comprehensive Portfolio)

Table 4: Activities.

5.1 Functional Hazard Assessment

The main focus of the FHA is to identify faults that could compromise the mission of finding the lost person. Artefact needed is Hazard Log (entries with severity levels), and deliverables are FHA Report and updated Hazard Log.

The FHA shall be completed in three steps:

1) Identify all functions of the drone swarm (e.g., the ability to fly). Once the main functions are identified, all sub-functions shall be determined. This process shall be conducted through discussion and documented according to table 5.
2) Determine the effects of total and partial loss of each function, as well as the malfunctions that could cause these losses. This step shall also be conducted through discussion and documented according to table 6.
3) Using the information from step 2, assess the effects on the swarm, the target, and the severity of each scenario [7], and document according to table **??**.

The results of these steps shall be documented according to tables 5, 6, and **??** within the Preliminary Safety Assessment (PSA) document.

ID	Function

Table 5: Functions

Function	Total loss	Partial loss	Malfunction

Table 6: Function Loss

Function ID	Function	Loss Phase	Operational Phase	Malfunction	Effect on Swarm	Effect on Subject	Severity of one (1) Agent failure	Severity of 50% of Agents in Swarm failing	Assumptions, Comments, Rationale

Table 7: FHA

5.2 Preliminary Drone Swarm Safety Assessment

The objective of the PDSSA is to identify faults that could compromise the mission of finding the lost person. Artefact needed is updated Hazard Log, and deliverable is the PDSSA document.

The PDSSA shall be conducted in three sequential steps:

1) **Function and System Identification**: Using information from system requirements and the FHA, determine the functions of the drone swarm, associated failure conditions, and all systems involved in each function. This uses the function table and FHA table. Record the findings in the Interdependence table (table 8).
2) **Failure Modes and Effects Analysis**: Based on the results of step 1, evaluate all potential failure scenarios and their effects. For example, case 1 may correspond to the total loss of all systems supporting a function, while case 2 may correspond to the partial loss of systems. Document the outcomes in the Combined Functional Failure Effects (CoFFE) table (table 9) [7].

All tables, analyses, and results shall be compiled in the PSA document.

			System 1		System 2	
Function	Function ID	Failure condition	System function 1	System function 2	System function 1	System function 2

Table 8: Interdependence table.

Case ID	System 1	System 2	Drone swarm result	Does it result in failure?

Table 9: CoFFE

5.3 Intrinsic Ground Risk Class

The operational geography and population within the area shall be defined, together with the characteristics of the Unmanned Aircraft (UA). Deliverable from this activity is the iGRC Report.

The iGRC shall be calculated according to SORA, based on UA characteristics such as size and maximum speed in relation to operational geography.

The operational volume for each drone in the swarm shall be established, and an appropriate ground buffer shall be specified.

The results of this activity shall be documented in a table (table 10 included in the FSA document [2].

Intrinsic UAS Ground Risk Class	#
Max population	
UAV size	#
UAV speed	#

Table 10: iGRC results (# means a number).

5.4 Initial Air Risk Class

This activity is to identify air collision risks with third parties. This does not include other drones in the swarm. This will be done using the following steps:

1) Identify the drones max height.
2) Identify the sensors max detection range.
3) Identify the height of any potential third parties in the area of operation.
4) Decide a maximum operational height for the drones.
5) Create a protocol for when a drone exceeds the maximum operational limit.

The deliverables for this activity are the ARC report, a protocol for returning to operational height and a table of height information (see table 11) recorded in the flight safety assessment document [2].

Max height	#
Max sensor height	#
Traffic height	#

Table 11: Heights.

5.5 TMPR & Robustness Levels

The SORA methodology shall be used to determine the TMPR within the operational environment. This assessment shall be performed to evaluate the likelihood of air collisions. Once the likelihood has been established, it shall be used to develop an air avoidance protocol [2]. The deliverables of this activity are Tactical Mitigation Performance Requirement (TMPR) and Robustness Report, which shall be documented in the FSA document.

5.6 Specific Assurance and Integrity Level Determination

In this step, use the deliverables from iGRC and ARC to find the SAIL level. The SAIL level will later be used to create requirements. The deliverable from this activity is the SAIL Determination Report, which shall be documented in the flight safety assessment document [2].

5.7 Determination of Containment Requirement

This activity shall follow SORA Main #8 and Annex E to determine the ground clearance height and the buffer zone around the operational area. The required values shall be based on the UAV's size and maximum speed [2]. Deliverable from this activity is Containment Requirement Document, which shall be documented in the FSA document.

5.8 Drone Swarm Safety Assessment

The safety assessment shall utilise Fault Tree Analysis (FTA) to demonstrate that the safety requirements have been satisfied [7].
Deliverable from this activity is the DSSA document, which shall be documented in the SA document.

5.9 Preliminary Safety Assurance Case

Develops a structured argument showing how to argue using the documents produced. The preliminary safety assurance case will structure a GSN using PSA, FSA, SA and safety goals and requirement as planed evidence for the Safety Assurance Case.

5.10 Safety Goals & Safety Requirements

The safety goals and requirements shall be updated as each activity is completed. The updated safety goals and requirements shall be compiled in the Safety Goals and Requirements Document and subsequently translated into the project's requirements database.

5.11 Safety Assurance Case

Provides the complete argument with all hazards, goals, requirements, and V&V evidence included. The safety assurance case will be based on the preliminary safety assurance case. It will present all documents as prof of reaching the goal.

6 Activity list

The timeline presented in this plan (figure 1) describes only the sequence of activities. For the time allocated to each activity and their relation to other activities, refer to the project plan [3].

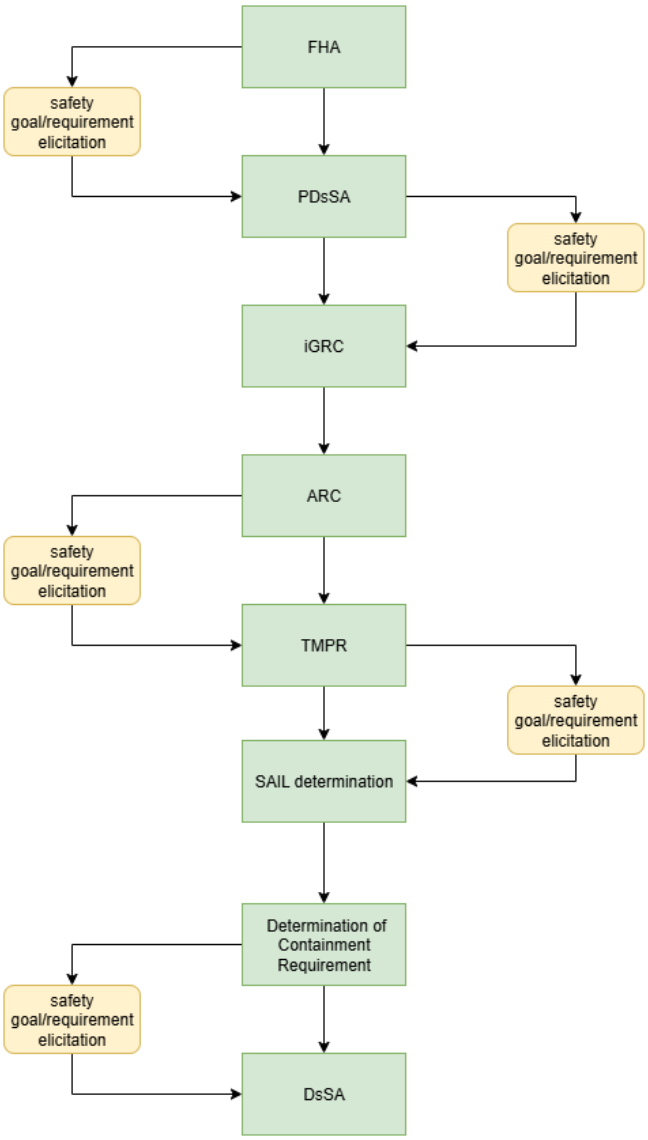

Figure 1: Sequence of Safety Activities.

References

[1] SAE International, *Guidelines for Development of Civil Aircraft and Systems*, ARP 4754A, Dec. 2010. [Online]. Available: https://www.sae.org/standards/arp4754a-guidelines-development-civil-aircraft-systems

[2] Joint Authorities for Rulemaking on Unmanned Systems (JARUS), *JARUS guidelines on Specific Operations Risk Assessment (SORA)*, JAR-DEL-SRM-SORA-MB-2.5, May 2024, Accessed: Sep. 30, 2025. [Online]. Available: https://jarus-rpas.org/wp-content/uploads/2024/06/SORA-v2.5-Main-Body-Release-JAR_doc_25.pdf

[3] A. Haglund, *Project Plan*, Intelligent Replanning Drone Swarm, Oct. 4 2025, Version 1.0.

[4] Y. M. Beyene, *Configuration Management Plan*, Intelligent Replanning Drone Swarm, Oct. 4 2025, Version 1.0.

[5] ——, *Quality Management Plan*, Intelligent Replanning Drone Swarm, Oct. 4 2025, Version 1.0.

[6] C. Namatovu, *Requirements Management Plan*, Intelligent Replanning Drone Swarm, Oct. 4 2025, Version 1.0.

[7] SAE International, *Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment*, ARP4761A, Dec. 2023. [Online]. Available: https://www.sae.org/standards/arp4761a-guidelines-conducting-safety-assessment-process-civil-aircraft-systems-equipment