Mälardalens universitet

INTELLIGENT
REPLANNING DRONE SWARM

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

Project Course in Dependable Systems
22.5 credits

Safety Goals & Requirements

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

graphicx

Title: Safety goals & Requirements		ID: SM-06 Version: 1.1
Author: Esaias Målqvist	Role: Safety Manager	Page 1 of 6

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	2025-11-14	Version for internal review	
1.0	2025-11-14	Release version	All
1.1	2025-11-14	Updated based on feedback	All

Contents

Glossary

ARC
initial Air Risk Class. 4

FHA
Functional Hazard Analysis. 4

FSA
Flight Safety Assessment. 4

iGRC
intrinsic Ground Risk Class. 4

PSA
Preliminary Safety Assessment. 4

1 Introduction

This document will list all safety goals, safety requirements and system safety requirements. All safety requirements and goals can also be found in the database. The requirements are derived from the safety activities done in the preliminary safety assessment and flight safety assessment documents.

1.1 Purpose

This document will be used as evidence that the hazards have been properly identified and mitigated through corresponding requirements. The document is also used to display safety goals and requirements independent from other requirements.

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]

Table 1: Related documents.

2 Safety goals

ID	Goal	derived from
SG-1	All staff must be safe in all operational phases.	FHA (PSA)
SG-2	Agents should avoid posing any threat to the subject.	ARC (FSA)
SG-3	Agents should avoid collisions with each other, minimum distance from each other 30 m.	containent requirements (FSA)
SG-4	Agents should avoid collisions with ground or ground obstacles, minimum altitude 15m.	ARC (FSA)
SG-5	Agents should avoid collisions with third parties in the air, max altitude above ground 50 m	ARC (FSA)
SG-6	The swarm should only fly in rural areas.	iGRC (FSA)
SG-7	Damaged agent should return home if damage is critical or battery low.	FHA (PSA)
SG-8	The agents should move at different altitudes depending on the task, searching 15-20m, moving from one sector to another, 25-40m.	containent requirements (FSA)
SG-9	The probability of the failure condition “UA leaving the operational volume” shall be less than 10-3/Flight Hour (FH).	containent requirements (FSA)
SG-10	When the UA leaves the operational volume, an immediate end of the flight must be initiated through a combination of procedures/processes and/or available technical means.	containent requirements (FSA)
SG-11	The Ground Risk Buffer must at least adhere to the 1:1 principle.	containent requirements (FSA)

Table 2: Safety Goals.

3 Safety Requirements

ID	requirement	traceability
SR-1	When the staff is at least 20m away from the swarm, the swarm shall proceed with startup sequence.	SG-1
SR-2	When the staff is in the landing area, the swarm shall hover at a distance of at least 40m away from the landing area.	SG-1
SR-3	When the swarm finds the subject, agents shall avoid flying above the subject.	SG-2
SR-4	When the subject is confirmed to be found, the swarm shall fly at least 50m away from the subject.	SG-2
SR-5	When the mission is in progress, swarm agents shall send location updates periodically to other agents in the same swarm.	SG-3
SR-6	Agents shall have a 25m buffer zone around them.	SG-3
SR-7	If agents' buffer zones overlap, the agents whose zones overlap shall move away from each other.	SG-3
SR-8	If position data of an agent is delayed, that agent shall increase its buffer zone by at least 20m.	SG-3
SR-9	If position data of an agent is uncertain, that agent shall increase its buffer zone by at least 20m.	SG-3
SR-10	If the flight capacity of an agent decreases, that agent shall increase its buffer zone by at least 20m.	SG-3
SR-11	If communication of an agent is delayed, that agent shall increase its buffer zone by at least 20m.	SG-3
SR-12	Agents shall fly a minimum of 15m above ground.	SG-4
SR-13	Agents shall avoid obstacles.	SG-4
SR-14	When the mission is in progress, agents shall use sensors to detect stationary obstacles (situational awareness).	SR-13
SR-15	When the mission is in progress, agents shall use sensors to detect air obstacles (situational awareness).	SR-13
SR-16	The swarm shall operate in areas with a population < 5 people per km2.	SG-6
SR-17	If communication is lost, the agent shall return to base.	SG-7
SR-18	If an agent's power unit is degraded, the agent shall return to base if possible.	SG-7
SR-19	If an agent's battery power is below 50%, the agent shall return to base.	SG-7
SR-20	If an agent's flight is unstable, the agent shall return to base.	SG-7
SR-21	While an agent is in searching state, it shall fly at an altitude between 15–20m above ground.	SG-8
SR-22	While an agent is in transition state, it shall fly between 25–40m above ground.	SG-8
SR-23	The operational volume shall add 50m to all sides as a buffer zone.	SG-11
SR-24	If an agent enters the operational area's buffer zone, it shall return to the operational area.	SG-9
SR-25	If an agent leaves the operational area's buffer zone, the agent shall land.	SG-10
SR-26	Agents shall fly a maximum of 50m above ground.	SG-5

Table 3: Safety Requirements.

4 System Safety Requirements

ID	system requirement	traceability
SSR-1	The protocol module shall define the procedures that will be taken so that all agents start in a safe way.	SR-1
SSR-2	The protocol module shall define the procedures that agents shall take when approaching the landing area.	SR-2
SSR-3	The protocol module shall define the distance from the landing area when staff are present.	SR-2
SSR-4	The protocol module shall define the procedures that agents shall take when the subject is found.	SR-3
SSR-5	The protocol module shall define the distance from the subject when the subject is found.	SR-4
SSR-6	The protocol module shall define the rules for agents broadcasting their position.	SR-5
SSR-7	The protocol module shall define the buffer zone for all agents.	SR-6
SSR-8	The protocol module shall define the procedures that will be taken when agent buffer zones overlap.	SR-7
SSR-9	The protocol module shall define the procedures that will be taken when agent position data is delayed.	SR-8
SSR-10	The protocol module shall define the procedures that will be taken when agent position data is uncertain.	SR-9
SSR-11	The protocol module shall define the procedures that will be taken when agent flight capacity is decreased.	SR-10
SSR-12	The protocol module shall define the procedures that will be taken when agent communication is delayed.	SR-11
SSR-13	The protocol module shall define the minimum height above ground for all agents.	SR-12
SSR-14	The protocol module shall define the procedures that agents shall take when avoiding stationary obstacles.	SR-14
SSR-15	The protocol module shall define the procedures that agents shall take when avoiding air obstacles.	SR-15
SSR-16	The protocol module shall define the operational volume based on input.	SR-16
SSR-17	The protocol module shall define the procedures that agents shall take when agent communication is lost.	SR-17
SSR-18	The protocol module shall define the procedures that agents shall take when an agent's power unit is degraded.	SR-18
SSR-19	The protocol module shall define the procedures that agents shall take when an agent's battery is below 50%.	SR-19
SSR-20	The protocol module shall define the procedures that agents shall take when an agent's flight is unstable.	SR-20
SSR-21	The protocol module shall define the maximum and minimum altitudes for searching state.	SR-21
SSR-22	The protocol module shall define the maximum and minimum altitudes for transition state.	SR-22
SSR-23	The protocol module shall define the buffer zone of the operational volume.	SR-23
SSR-24	The protocol module shall define the procedures that agents shall take when entering the operational volume buffer zone.	SR-24
SSR-25	The protocol module shall define the procedures that agents shall take when leaving the operational volume's outer buffer boundary.	SR-25
SSR-26	The protocol module shall define the maximum height above ground for all agents.	SR-26

Table 4: System Safety Requirements.

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.