



SAIL III Means of Compliance with OSO#18
“Envelope Protection”

Doc. No. : MOC OSO#18-01

Issue : 1

Date : 18 December 2023

Proposed

Final

SUBJECT	Automatic Protection of the flight envelope from human error
REQUIREMENTS incl. Amdt.	Annex E of AMC 1 to Article 11 of Regulation 2019/947
ASSOCIATED IM/MoC	Yes <input type="checkbox"/> / No <input checked="" type="checkbox"/>
ADVISORY MATERIAL	N/A

List of acronyms

CMU	control and monitoring unit
EPS	envelope protection function
HW/SW	hardware / software
MoC	means of compliance
OA	Operational Authorization
SAIL	specific assurance and integrity level
UA	unmanned aircraft
UAS	unmanned aircraft system

Table of contents

1. Introduction.....	2
2. Definitions	2
3. General Means of Compliance for OSO#18 (low robustness).....	3
4. Guidance.....	4

 <p>EASA European Union Aviation Safety Agency</p>	<p>SAIL III Means of Compliance with OSO#18</p> <p>“Envelope Protection”</p>	<p>Doc. No. : MOC OSO#18-01</p> <p>Issue : 1</p> <p>Date : 18 December 2023</p> <p>Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/></p>
--	--	--

1. Introduction

UAS without automatic protection function are susceptible to incorrect remote-pilot control inputs (human errors) which can result in loss of the UA if the performance or structural limits of the aircraft are exceeded.

To mitigate this risk, UA are required to have an automatic protection of the flight envelope from human errors when operated in the specific category.

This MoC covers the flight envelop protection as required by OSO#18 for SAIL III operations where the levels of integrity and assurance are accepted to be low.

The criteria for low integrity are described as:

The UAS incorporates automatic protection of the flight envelope to prevent the remote pilot from making any single input under normal operating conditions that would cause the UA to exceed its flight envelope or prevent it from recovering in a timely fashion.


The criteria for low assurance are described as:

- *The automatic protection of the flight envelope has been developed in-house or out of the box (e.g. using Commercial Off The Shelf elements), without following specific standards*

2. Definitions

For these MoC the following definitions are established:

- a) *Flight envelope*: the flight envelope as associated by the UA design limits or as defined by the manufacturer as limit flight envelope and as associated with operational limitations.
- b) *Exceedance of the flight envelope or prevent it from recovering in a timely fashion*: a condition that would result in a loss of control or where it cannot be expected that the aircraft can reliably return to normal operation, without imposing risk on the ground and in the air.
- c) *“Loss of control”* situations where the control is considered to be lost are e.g.:
 - crash of the UA with the ground/infrastructure/people;
 - unrecoverable loss of controllability;
 - activation of flight termination system/parachute/other M2 mitigation due to emergency situation;
 - erroneous activation of flight termination system/parachute/other M2 mitigation;
 - loss of payload (detachment of a part or a load heavy enough to create a risk for people on ground).

 <p>EASA European Union Aviation Safety Agency</p>	<p>SAIL III Means of Compliance with OSO#18 “Envelope Protection”</p>	<p>Doc. No. : MOC OSO#18-01</p> <p>Issue : 1</p> <p>Date : 18 December 2023</p> <p>Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/></p>
--	---	--

d) *single input*: any pilot interaction manipulating a single control of the human machine interface (HMI) for a period of time within which it cannot be assumed that the pilot is detecting and correcting his error.

normal operating condition: operations within established limits for normal operations and related foreseeable environmental conditions.

3. General Means of Compliance for OSO#18 (low robustness)

Any declaration to comply with the criteria of low robustness should specify the supporting evidence available to substantiate each of the following claims:

- a) A limit flight envelope under normal operating conditions is established by the designer as associated with the UA design limits and/or associated with operational limitations defined by the designer to enable safe and controllable manoeuvring.
- b) The flight parameters relevant for the protection of the established limit flight envelope, and their allowed variability range, should be identified as appropriate for the kind of aircraft, phase of flight and type of manoeuvre. The analysis considers parameters and their combinations, such as:
 - speed (horizontal/vertical);
 - angle of attack;
 - accelerations;
 - aircraft attitude, yaw, pitch and roll rates;
 - power settings.
- c) The envelope protection is implemented in the flight control system onboard of the UA.
- d) The automated protection is demonstrated by flight test, analysis, simulation, or a combination thereof under anticipated operating conditions for any identified parameter or critical combination of parameters.
- e) The system is providing the necessary feedback to the pilot and is enabling the pilot to regain control.

Note: When it is demonstrated that a flight envelope parameter is protected by inherent characteristics of the UA (e. g. through a stall resistant design and/or limited control authority) it is not expected that additional automated protection functions are addressed.

 <p>EASA European Union Aviation Safety Agency</p>	<p>SAIL III Means of Compliance with OSO#18</p> <p>“Envelope Protection”</p>	<p>Doc. No. : MOC OSO#18-01</p> <p>Issue : 1</p> <p>Date : 18 December 2023</p> <p>Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/></p>
--	--	--

Documentation and record-keeping

Designers need to declare that they achieve the integrity criteria and base the declaration on evidence, which is the documentation of appropriate testing, analysis, simulation, inspection, design review or operational experience or a combination thereof.

Delivery of such evidence to the authority may not be required in the frame of a declaration of compliance to OSO#18, however, declaring compliance, applicants are responsible to determine, collect, record such evidence, and make it available in case the authority should so require.

Related procedures, limitations and information including required pre-flight checks and maintenance instructions are established and provided to the operator.

Link with other OSO’s:

If the UAS includes specific means to meet containment requirements, the envelope protection system should not negatively affect the operation of these means.

Any automated function needs to be designed considering system safety and reliability iaw. OSO #5.

OSO #11 - Safe recovery from Human Error addresses the risk of human errors that may affect the safety of the operation that are not related to the protection of the flight envelope.

OSO #15 “Human Factors evaluation” requires that the UAS information and control interfaces are clearly and succinctly presented and do not confuse, cause unreasonable fatigue, or contribute to remote crew error that could adversely affect the safety of the operation

4. Guidance


The following examples are conceptual considerations with guidance on how to comply. They are by no means a comprehensive list of required compliance demonstrations.

a) Limiting “rate of descent”

For certain aircraft configuration a sudden reduction in vertical thrust leads to high rates of descent that may result in a loss of control and subsequent structural damage.

An automated function providing sufficient thrust to protect the UA from a critical rate of descent or critical flight vector is implemented in the flight control system.

The established limit as well as the proper engagement and efficiency of the automated protection is demonstrated (by flight test, analysis, simulation, etc).

 <p>EASA European Union Aviation Safety Agency</p>	<p>SAIL III Means of Compliance with OSO#18</p> <p>“Envelope Protection”</p>	<p>Doc. No. : MOC OSO#18-01</p> <p>Issue : 1</p> <p>Date : 18 December 2023</p> <p>Proposed <input checked="" type="checkbox"/> Final <input type="checkbox"/></p>
--	--	--

b) Protecting structural loads of a fixed wing UA

Limit loads for the structure are identified and appropriate combinations of flight parameters ensuring protection of the structural limits are established with adequate margins.

An automated function to limit pilot inputs that are expected to result in flight parameters beyond the established limits is implemented.

The established limit as well as the proper engagement and the function of the automated protection is demonstrated (by flight test, analysis, simulation, or a combination).

Engagement of the EPS is indicated to the pilot (e.g. a caution light) when not obvious and the pilot is able to regain control with normal pilot inputs.

c) Credit for inherent protection characteristics (e.g. fixed wing UA)

A naturally stable fixed wing aircraft with stall resistant design is equipped with a 2-axis-flight control system that is achieving limited roll or pitch rates. Pilot errors can be easily identified when the aircraft is approaching indicated or visible turn- and bank angles and after timely stopping any pilot input the aircraft is recovering with appropriate margin from structural limits.

d) Protection of parameter selection, switches and data loading

The pilot should be prevented from selection of parameters that would directly lead to a loss of control of the operation. This may include parameters/values such as

- selection of non-active C2 link leading to non-timely recovery or Loss of Control
- de-activation of any function required for safe operation (autoflight, stabilization,)
- activation of flight termination system in normal operation
- erroneous release of external payload

The prevention of inadvertent activation or switch may be achieved through various means such as required dual action, in-activation of a selected value or automatic checking of the pilot’s input.