Safety recommendation no. 589

Date of the publication	06.06.2023
Number of the final report	2390
Safety deficit	About one minute after take-off at the University of Zurich (UZH) Irchel, the M2 V9 drone automatically triggered the flight termination system (FTS) and initiated an emergency descent with a parachute. After ejecting the parachute, the connecting rope broke and the drone hit the forest floor without deceleration and was destroyed. As the investigation showed, the applied firmware of the flight controller based on the software version ArduCopter 3.5.0-rc5 was only capable of using two of the three available inertial measurement units (IMU) for the flight control of the drone. As a result, the flight controller's software lacked the ability, known as resilience, not to fail completely in the event of malfunctions or the failure of individual components, but to maintain control of the drone. Only from software version 3.6.12 onwards was it possible to achieve this resilience with the corresponding configuration of the safety-critical parameter ("EK2_IMU_MASK = 7"), as published in a discussion forum of the flight controller manufacturer as Service Bulletin SB 0000002. In the case of the accident involving the largely identical drone SUI-9909 on 25 January 2019 (cf. summary report), the FTS was also immediately triggered due to a loss of the GPS signal. As the investigation showed, the drone's flight attitude was still stable at this time and thus a landing under engine power, either manually controlled on sight or autonomously, would not have been fundamentally impossible. When operating under extreme climatic conditions, corresponding flight-critical parameters such as ambient temperature and humidity are not included in practice. This would allow a flight mission to be aborted early or not carried out at all under certain conditions.
Safety recommendation	The Federal Office of Civil Aviation (FOCA) should ensure that the manufacturer revises the conditions for triggering the automatic flight termination system so that suitable measures (contingency procedures) are taken to achieve a controlled flight abortion before the parachute is triggered and the drone descends to the ground in an uncontrolled manner.
Addressees	BAZL Bundesamt für Zivilluftfahrt
Stage of the implementation	Implemented – In a letter dated 29 September 2023, the Federal Office of Civil Aviation (FOCA) commented as follows: "The Federal Office of Civil Aviation supports Safety Recommendation (SE) No. 589 in principle. The roles and responsibilities of the competent authorities are defined in the Implementing Regulation (EU) 2019/947 [3], or the Applicable Means of Compliance (AMC) 1, Art. 11, para. 1.5 (f): 'According to Regulation (EU) 2018/1139 (the EASA 'Basic

Regulation'), EASA is the authority competent in the European Union to verify compliance of the UAS design and its components with the applicable rules, while the authority that is designated by the Member State is competent to verify compliance with the operational requirements and compliance of the personnel's competency with those rules.'
This safety recommendation relates to drone manufacturers and design considerations; therefore, the European Union Aviation Safety Agency (EASA) is the competent authority for monitoring design compliance.
In addition, SE 589 is already fully considered by the risk-based approach according to SORA (Art. 11 of Implementing Regulation (EU) 2019/947) [3].
SORA requires the definition of operational procedures in the event of technical problems with unmanned aircraft systems (UAS) and the handling of malfunctioning systems to ensure the safe operation of UAS. In doing so, the FOCA is guided by the operational safety objectives (OSO) as currently set out in Regulation (EU) 2019/947 and the associated AMC [3].
In particular, considering the following points, it should be ensured that a controlled flight termination is achieved in abnormal / emergency situations [1, Annex E].
- OSO #08 "Operational procedures [reg. technical issue with the UAS] are defined, validated and adhered to",
- OSO #11 "Procedures [reg. deterioration of external systems supporting UAS operations] are in-place to handle the deterioration of external systems supporting UAS operations",
- OSO #14 "Operational procedures [reg. human error] are defined, validated and adhered to" and
- OSO #21 "Operational procedures [reg. adverse operating conditions] are defined, validated and adhered to"
For operations at "SAIL II" level [4] (and beyond, i.e. SAIL III, SAIL IV etc.), the above-mentioned OSOs are at a "Medium Robustness Level" [5], which involves the FOCA in accordance with [1, Annex E].

In practice, this means that contingency procedures and emergency procedures are already being assessed and validated by both the operator and the FOCA as part of the SORA process, and the FOCA hereby considers Safety Recommendation No. 589 to be fully implemented and completed."

____

[1] JARUS Guidelines on Specific Operations Risk Assessment (SORA). JAR-DEL-WG6-D.04; Joint Authorities for Rulemaking of Unmanned Systems; 30 January 2019, Edition No. 2.0, http://jarus-rpas.org/wp-content/uploads/2023/07/jar_doc_06_jarus_sora_v2.0.pdf
[2] FOCA Authorisation to Matternet Operations GmbH to operate unmanned aircraft systems, 20 August 2021
[3] Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and (EU)
2019/945), European Union, September 2021, https://www.easa.europa.eu/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulation-eu
[4] The SAIL (Specific Assurance and Integrity Level) is an index that ranges from one to six and indicates the guarantee and integrity of the measures to be applied, i.e. the robustness. We can therefore say that a low value of SAIL means a low value for the robustness of the remedial actions to be applied, which corresponds to a low-risk operation. Conversely, a higher SAIL value means a higher robustness, as the risk of the operation is correspondingly higher.
[5] According to the SORA methodology, the robustness of the mitigation measures is defined by the level of integrity that each of the mitigations provides (e.g. the safety improvement) and the level of safety assurance that the mitigations have been able to achieve

	(e.g. the method by which this is demonstrated). Robustness level = integrity level + reliability level. There are therefore 3 types of robustness level: Low Robustness, Medium Robustness and High Robustness.
Investigation report concerning the safety recommendation	Zwischenbericht Schlussbericht Final report Vorbericht

Swiss Transportation Safety Investigation Board STSB
CH-3003 Berne
Tel.: +41 58 466 33 00, Fax.: +41 58 463 33 01
info@sust.admin.ch
www.sust.admin.ch