Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizerische Sicherheitsuntersuchungsstelle SUST

Untersuchungsdienst

Sicherheitsempfehlung Nr. 589

Ausgabedatum der Sicherheitsempfehlung	06.06.2023
Nummer Schlussbericht	2390
Sicherheitsdefizit	Rund eine Minute nach dem Start bei der Universität Zürich (UZH) Irchel löste die Drohne M2 V9 automatisch das Flugabbruchsystem (Flight Termination System – FTS) aus und leitete einen Notabstieg mit Fallschirm ein. Nach dem Ausstossen des Fallschirms riss die Verbindungsleine, und die Drohne schlug ungebremst auf den Waldboden auf und wurde zerstört. Wie die Untersuchung zeigte, war die angewandte Firmware des Flugreglers auf Basis des Softwarestandes ArduCopter 3.5.0-rc5 lediglich in der Lage, zwei der drei zur Verfügung stehenden Trägheitsmesseinheiten (Inertial Measurement Units – IMU) zur Flugsteuerung der Drohne zu verwenden. Dadurch fehlte der Software des Flugreglers die als Resilienz bezeichnete Fähigkeit, bei Störungen oder bei Ausfällen einzelner Komponenten nicht vollständig auszufallen, sondern die Steuerung der Drohne aufrechtzuerhalten. Erst ab der Software-Version 3.6.12 konnte diese Resilienz mit der entsprechenden Konfiguration des sicherheitskritischen Parameters («EK2_IMU_MASK = 7»), wie dies in einem Diskussionsforum des Herstellers des Flugreglers als Service Bulletin SB 0000002 publiziert wurde, erlangt werden. Auch beim Unfall der weitgehend baugleichen Drohne SUI-9909 vom 25. Januar 2019 (vgl. summarischer Bericht) wurde aufgrund eines Verlustes des GPS-Signals umgehend das FTS ausgelöst. Wie die Untersuchung zeigte, war zu diesem Zeitpunkt die Fluglage der Drohne noch stabil und eine Landung unter Motorkraft wäre somit, entweder manuell gesteuert auf Sicht oder autonom, nicht grundsätzlich ausgeschlossen gewesen. Beim Einsatz unter extremen klimatischen Bedingungen werden in der Praxis entsprechende flugkritische Parameter wie z.B. der Umgebungstemperatur und der Luftfeuchtigkeit nicht einbezogen. Dies würde es erlauben, unter gewissen Bedingungen einen Flugeinsatz frühzeitig abzubrechen oder erst gar nicht durchzuführen.
Sicherheitsempfehlung	Das Bundesamt für Zivilluftfahrt (BAZL) sollte sicherstellen, dass der Hersteller die Bedingungen für das Auslösen des automatischen Flugabbruchsystems (Flight Termination System) dahingehend überarbeitet, dass durch geeignete Massnahmen (contingency procedures) eine kontrollierte Flugbeendigung erwirkt wird, bevor es zum Auslösen des Fallschirms kommt und die Drohne unkontrolliert zu Boden sinkt.
Adressaten	BAZL Bundesamt für Zivilluftfahrt
Stand der Umsetzung	Umgesetzt – Mit Schreiben vom 29. September 2023 nimmt das

Schweizerische Sicherheitsuntersuchungsstelle SUST
3003 Bern
Tel.: +41 58 466 33 00, Fax.: +41 58 463 33 01
info@sust.admin.ch
www.sust.admin.ch

Bundesamt für Zivilluftfahrt (BAZL) wie folgt Stellung:
«Das Bundesamt für Zivilluftfahrt unterstützt die Sicherheitsempfehlung (SE) Nr. 589 grundsätzlich.
Die Rollen und Verantwortlichkeiten der zuständigen Behörden werden in der Durch-führungsverordnung (EU) 2019/947 [3], bzw. den Applicable Means of Compliance (AMC) 1, Art. 11, Abs. 1.5 (f), festgelegt:
'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.'
Diese Sicherheitsempfehlung bezieht sich auf Drohnenhersteller und Designüberlegungen, dementsprechend ist für die Überwachung der Regelkonformität bezüglich Konstruktion (design) die Agentur der Europäischen Union für Flugsicherheit (EASA) die zuständige Behörde.
Darüber hinaus wird die SE 589 bereits vollumfänglich durch den risikobasierten Ansatz gemäss SORA (Art. 11 der Durchführungsverordnung (EU) 2019/947) [3] berücksichtigt.
SORA verlangt die Bestimmung von betrieblichen Verfahren für den Fall eines Auftretens technischer Probleme bei unbemannten Luftfahrzeugen (unmanned aircraft systems, UAS) sowie den Umgang mit gestörten Systemen, um den sicheren Betrieb von UAS zu gewährleisten. Das BAZL richtet sich hierbei nach den Anforderungen an den Betrieb (operational safety objectives, OSO), wie sie heute in der Verordnung (EU) 2019/947 respektive im dazugehörigen AMC [3] festgehalten werden.
Insbesondere soll unter Berücksichtigung der nachfolgenden Punkte sichergestellt werden, dass in abnormalen / Notfallsituationen eine kontrollierte Flugbeendigung erwirkt wird [1, Annex E].
- OSO #08 "Operational procedures [reg. technical issue with the UAS] are defined, validated and adhered to" (Betriebsverfahren [beim Auftreten von technischen Problemen] werden definiert, validiert und befolgt),
- OSO #11 "Procedures [reg. deterioration of external systems supporting UAS operations] are in-place to handle the deterioration of external systems supporting UAS operations"(Verfahren für den Umgang mit gestörten Systemen, die den sicheren Betrieb von UAS unterstützen, sind vorhanden,
- OSO #14 "Operational procedures [reg. human error] are defined, validated and adhered to" (Betriebsverfahren [bei menschlichem Versagen] werden definiert, validiert und befolgt) sowie
- OSO #21 "Operational procedures [reg. adverse operating conditions] are defined, validated and adhered to" (Betriebsverfahren [für ungünstige Betriebsbedingungen] werden definiert, validiert und befolgt)
Für den Betrieb auf Stufe «SAIL II» [4] (und darüber hinaus, d.h. SAIL III, SAIL IV etc.) sind die obgenannten OSOs auf einem «Medium Robustness Level» (Mittlere Robustheit) [5] angesiedelt, wodurch gemäss [1, Annex E] das BAZL involviert ist.
In der Praxis bedeutet dies, dass Verfahren zur Bewältigung von Ausnahmesituationen (contingency procedures) und solche zur Bewältigung von Notfallsituationen (emergency procedures) bereits heute im Rahmen des SORA-Prozesses sowohl durch den Betreiber als auch vom BAZL bewertet respektive validiert werden.Das BAZL erachtet die Sicherheitsempfehlung Nr. 589 hiermit als vollständig umgesetzt und abgeschlossen.»

_____

[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 Authorization 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] Der SAIIL (Specific Assurance and Integrity Level) ist ein Index, der von eins bis sechs reicht und die Garantie und Integrität der anzuwendenden Maßnahmen, d.h. die Robustheit, angibt. Wir können also sagen, dass ein niedriger Wert von SAIL einen niedrigen Wert für die Robustheit der anzuwendenden Abhilfemaßnahmen bedeutet, was einem Betrieb mit geringem Risiko entspricht. Umgekehrt bedeutet ein höherer SAIL-Wert eine höhere Robustheit, da das Risiko der Operation entsprechend höher ist. [5] Nach der SORA-Methodik wird die Robustheit der Abschwächungsmaßnahmen durch den Grad der Integrität definiert, den jede der Abschwächungen bietet (z. B. die Sicherheitsverbesserung), sowie durch den Grad der Sicherheitsgewährleistung, der durch die Abschwächungen erreicht werden konnte (z. B. die Methode, mit der dies nachgewiesen wird). Robustheitsgrad = Integritätsgrad + Zuverlässigkeitsgrad. Es gibt also 3 Arten von Robustheitsstufe: Geringe Robustheit, Mittlere Robustheit und Hohe Robustheit.
Untersuchungsberichte zur Sicherheitsempfehlung	Zwischenbericht Schlussbericht Final report Vorbericht

Schweizerische Sicherheitsuntersuchungsstelle SUST
3003 Bern
Tel.: +41 58 466 33 00, Fax.: +41 58 463 33 01
info@sust.admin.ch
www.sust.admin.ch