

ÜBERWACHUNGSINSTANZ ZUR TRENNUNG DES MISSIONSSYSTEMS UND DES FLUGKONTROLLSYSTEMS IN DEM UNBEMANNTEN LUFTFAHRTSYSTEM SAGITTA

A. Frey, T. Hanti; Technische Hochschule Ingolstadt, Esplanade 10, 85049 Ingolstadt, Germany

Zusammenfassung

Im diesem Paper werden die Ziele und das Konzept einer Überwachungsinstanz für ein autonomes unbemanntes Luftfahrtsystem als mögliche Lösung zur Trennung eines nicht nach sicherheitskritischen Anforderungen entwickelten Missionssystems und des Flugkontrollsystems vorgestellt. Die Überwachungsinstanz überprüft die Ausgaben des Missionssystems auf Fehler und verhindert eine Ausführung, bevor kritische Flugbewegungen ausgeführt werden.

Durch die Fehler würde ein zumindest temporärer Ausfall des Missionssystems hervorgerufen. Während autonom durchgeführter Flugphasen, in denen kein menschlicher Bediener zur Verfügung steht, besteht damit die Anforderung an die Überwachungsinstanz einen Ausfall des Missionssystems für das Flugkontrollsystem zu maskieren. Dies schließt das Generieren eigener Anweisungen an das Flugkontrollsystem ein.

Zunächst werden primär die derzeit durch den menschlichen Bediener durchgeführten Überwachungen analysiert und in der Überwachungsschicht implementiert. Darauf folgend werden die für den Fall eines erkannten Fehlers durch die Überwachungsinstanz generierten Anweisung erläutert. Die Anweisungen gewährleisten eine vorab und zu jedem Zeitpunkt des Fluges ein bekanntes und nachvollziehbares Verhalten des unbemannten Luftfahrtsystems.

Zum Abschluss wird die Entwicklungs- und Testumgebung für die Überwachungsinstanz, sowie die Planung für die Flugerprobung, vorgestellt.

1. EINLEITUNG

Das experimentelle unbemannte Luftfahrtsystem Sagitta dient als Erprobungsträger für eine Vielzahl von neuen Technologien, welche von Forschungseinrichtungen für spätere Anwendung entwickelt und unter Führung der Industrie integriert werden. Damit steht Sagitta explizit auch zur Erprobung von in anderen Forschungsprojekten entwickelten Funktionalitäten zur Verfügung. Das mit dem Sagitta zu erprobende Missionssystem soll einen autonomen Flug ermöglichen durch den der menschlichen Bediener weitestgehend entlastet werden soll. Der Einsatz hochinnovativer Systeme, welche nicht nach sicherheitskritischen Anforderungen zugelassen werden können, erhöht die Fehleranfälligkeit des Systems und erfordert insbesondere in der Interaktion mit sicherheitskritischen Subsystemen weitergehende Maßnahmen um die Sicherheit zu gewährleisten. Ein Teil der Überwachungsaufgaben, die derzeit von einem menschlichen Bediener am Boden wahrgenommen werden, müssen somit an Bord des unbemannten Luftfahrtsystems transferiert werden.

2. ZIEL DER ÜBERWACHUNGSINSTANZ

Primäres Ziel zur Entwicklung einer Überwachungsinstanz ist die Erhöhung der Sicherheit im Betrieb von unbemannten Luftfahrtsystemen.

Die Überwachungsinstanz muss sicherstellen, dass keine kritischen Flugbewegungen ausgeführt werden und der Flug sicher fortgesetzt wird, auch wenn abschnittsweise kein menschlicher Bediener zur Verfügung steht.

In dem experimentellen unbemannten Luftfahrtsystem Sagitta sollen zwei Aspekte der Überwachungsinstanz nachgewiesen werden.

1) Die Überwachungsinstanz kann selbständig Fehler des Missionssystems erkennen. Im Fehlerfall kann der Flug auch ohne den Eingriff eines menschlichen Bedieners, nach vordefinierten Regeln, sicher bis zur Rückkehr auf den Flugplatz fortgesetzt werden.

2) Eine Entscheidung über eine Übernahme der Kontrolle des unbemannten Luftfahrtsystems durch einen menschlichen Bediener ist damit nicht ad hoc erforderlich und kann ressourcenabhängig erfolgen.

3. KONZEPT EINER ÜBERWACHUNGSINSTANZ

Das Konzept der Überwachungsinstanz ist aus der Analyse des bisherigen Betriebes unbemannter Luftfahrtsysteme und den Anforderungen eines steigenden Autonomiegrades entstanden. Für den steigenden Autonomiegrad werden künstliche kognitive Systeme [1] zugrunde gelegt, bei denen die Missionssteuerung auf Basis eines komplexen

Planungsprozesses mit Situationsauswertung und Zielebestimmung erfolgt. Die Interaktion mit dem unbemannten Luftfahrtsystem wird auf einer ähnlichen Ebene durchgeführt, als ob es von einem Menschen gesteuert wird. In dem unbemannten Luftfahrtsystem Sagitta wird ein solches System erprobt [2].

In den hochkomplexen Szenarien in der Luftfahrt wird auch in einem bemannten Luftfahrtsystem eine Vielzahl von Vorgängen hochautomatisiert durchgeführt. Der menschliche Bediener an Bord steuert und überwacht diese Vorgänge und greift notfalls korrigierend ein. Durch die Eingriffsmöglichkeit eines menschlichen Bedieners reduziert sich die formale Verfügbarkeitsanforderung und die Anforderung an die Fehlerfreiheit der berechneten Ergebnisse.

Bei unbemannten Luftfahrtsystemen wurde dieses Überwachungskonzept konsequent fortgeführt. Der menschliche Bediener am Boden steuert und überwacht analog zu dem Piloten an Bord eines bemannten Luftfahrtsystems die hochautomatisierten Vorgänge und greift notfalls korrigierend ein. Dabei ist es unerheblich, ob die hochautomatisierten Vorgänge an Bord des unbemannten Luftfahrtsystems durchgeführt werden, oder am Boden. In jedem Fall ist eine ständige Kommunikation mit dem unbemannten Luftfahrtsystem und die ständige Verfügbarkeit des menschlichen Bedieners erforderlich.

Zukünftige Ansätze sehen die gleichzeitige Führung mehrerer unbemannter Luftfahrtsysteme durch einen einzigen menschlichen Bediener vor [3]. Die ständige Verfügbarkeit eines menschlichen Bedieners für die Überwachung und den möglicherweise erforderlichen Eingriff für ein individuelles unbemanntes Luftfahrtsystem ist damit nicht gewährleistet. Die Überwachungsaufgabe des menschlichen Bedieners muss an Bord des unbemannten Luftfahrtsystems verlagert werden. Das zu überwachende Missionssystem wird als Black Box betrachtet, dessen interne Zustände für den menschlichen Bediener nicht transparent sind. Zudem können die internen Zustände aufgrund des Konzeptes und der Komplexität des eingesetzten Missionssystems nicht während der Entwicklungs- Integrations- und Testphase vollständig überprüft werden. Die Integration solcher Black Box oder Off-the-Shelf Systemkomponenten in sicherheitsrelevanten Systeme kann softwaretechnisch durch eine Überwachungsinstanz gelöst werden welche die Ausgaben des zu überwachenden Systems prüft und nur spezifikationskonforme Ausgaben zulässt [4].

In unbemannten Luftfahrtsystemen muss selbst im Falle eines Fehlers im Missionssystem ein weiterer autonomer Betrieb sichergestellt sein, bis der menschliche Bediener zur Verfügung steht. Für bestimmte, unverzichtbare Funktionen des

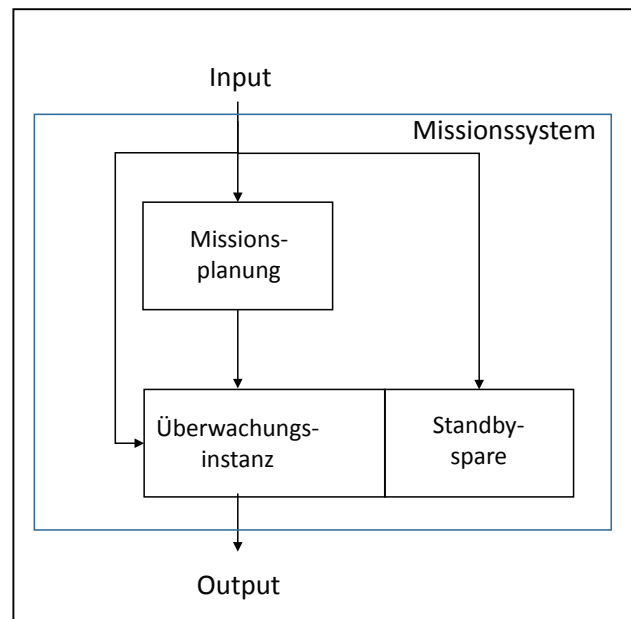


BILD 1 Konzept einer Überwachungsinstanz

Missionssystems muss eine alternative, aus sicherheitstechnischer Sicht bewertbare, Implementierung vorliegen. Die alternative Implementierung wird nur bei einem erkannten Fehler in der Ausgabe des zu überwachenden Missionssystems ausgeführt. Die Überwachungsinstanz implementiert z.B. Funktionen für einen sicheren Rückflug zum Flugplatz und fungiert in diesem Fall als „standby-spare“ [5].

3.1. Überwachungen

Ein gefährlicher Fehler im Missionssystem stellt einen internen Zustand dar, der zu einem Versagen führt, welches die Sicherheit des unbemannten Luftfahrtsystems gefährdet. Im Falle des prinzipiell funktionsfähigen Missionssystems kann dies eine falsche Anweisung sein. Als falsch werden Anweisungen eingestuft, welche, würde das Flugkontrollsystem diese ausführen, gegen vorgegebene Randbedingungen der Mission verstoßen. Ebenso ist ein gefährlicher Fehler eine Anweisung die mit dem Luftfahrtsystem nicht umsetzbar ist. Gleichermaßen gefährlich wird das Ausbleiben einzelner Anweisungen eingestuft, welche zwingend erfolgen müssen, damit die Sicherheit des unbemannten Luftfahrtsystems nicht gefährdet wird, wie z.B. die ausbleibende Richtungsänderung vor Verletzung der Missionsgrenze und dem damit verbundenen Verlust des unbemannten Luftfahrtsystems.

Als eigene Kategorie ist der Ausfall des Missionssystems zu sehen, durch den überhaupt keine weiteren Anweisungen an das Flugkontrollsystem gegeben werden.

Um das Versagen des Missionssystems zu erkennen werden für die einzelnen Fälle folgende Überwachungen umgesetzt:

a) *Senden von falschen oder keinen Anweisungen*

Umgesetzte Überwachung

- Einhaltung der Missionsgrenzen
- Erreichbarkeit und Position der Wegpunkte
- Verbleibende Flugzeiten

b) *Ausfall des Missionssystems*

Umgesetzte Überwachung

- Zustandsnachrichten oder Fehlermeldungen des Missionssystems

3.1.1. Einhalten der Missionsgrenzen

Der Flugweg des unbemannten Luftfahrtsystems wird permanent in Bezug auf die Missionsgrenzen überwacht. Die Entfernung des unbemannten Luftfahrtsystems zu den Grenzen des Missionsgebietes muss zu jeder Zeit größer sein, als der Kurvenradius, der zum Abdrehen vor der Missionsgrenze erforderlich ist. Ein Flug parallel zu der Missionsgrenze wäre direkt an der Missionsgrenze möglich, während bei einer Annäherung in einem rechten Winkel vorher abgedreht werden muss. Die Betrachtung schließt komplexe Konstellationen der Missionsgrenzen und daraus resultierende Einschränkungen für die zu erfolgende Kurve mit ein (Bild 2).

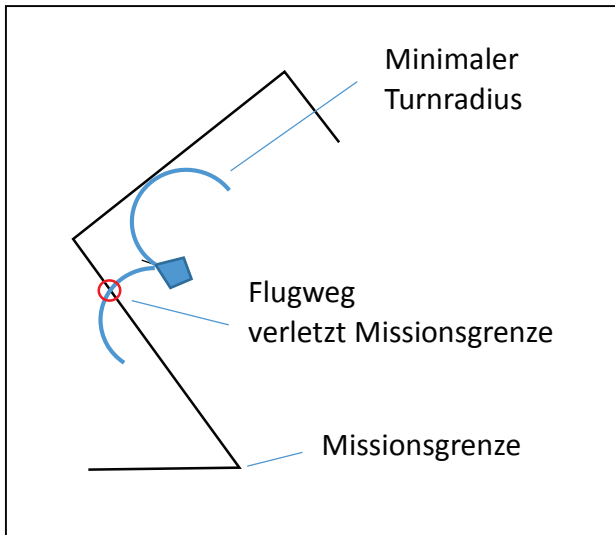


BILD 2 Beispiel für Annäherung an eine Missionsgrenze

3.1.2. Erreichbarkeit und Position der Wegpunkte

Die Position der Wegpunkte muss einen definierten lateralen Abstand voneinander einhalten, der gewährleistet, dass das Flugkontrollsystem die Wegpunkte direkt anfliegen kann. Bei Wegpunkten, die eine engere Kurve, als der minimale Kurvenradius

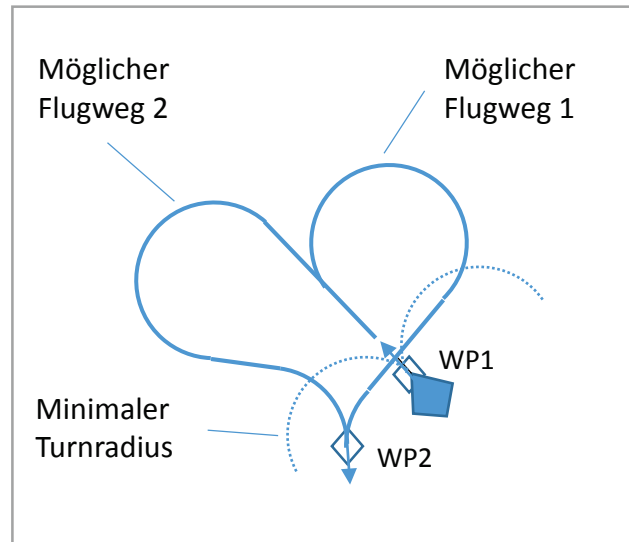


BILD 3 Beispiel für Flugwegplanung bei nicht direkt anfliegaren Wegpunkten

des unbemannten Luftfahrtsystems erfordern, wird das Flugkontrollsystem entweder den Wegpunkt nicht anfliegen, oder eine komplexe Flugroute planen, um den Wegpunkt zu erreichen (Bild 3). Das Flugkontrollsystem berücksichtigt bei der Flugwegplanung keine missionspezifischen Einschränkungen, so dass eine unbeabsichtigte Verletzung der Missionsgrenze erfolgen könnte.

Der vertikale Abstand der Wegpunkte darf außerdem die Steigfähigkeit/Sinkfähigkeit des unbemannten Luftfahrtsystems nicht überschreiten. Zusätzlich wird überwacht, dass die absolut vorgegebenen Missionsgrenzen eingehalten werden. Hierzu werden die mit den Wegpunkten angegebenen Attribute, wie z.B. Höhen und Geschwindigkeiten, überprüft.

3.1.3. Verbleibende Flugzeiten

Die verbleibende Flugzeit wird hinsichtlich des verfügbaren Treibstoffs überwacht. Der Treibstoffverbrauch zur Rückkehr zum Flugplatz entlang einer sicheren und möglichst kurzen Flugroute wird ständig mitgerechnet. Ist der für einen sicheren Flug erforderliche Treibstoff gerade noch vorhanden und es erfolgt keine Anweisung für einen Rückflug zu dem Flugplatz, wird das Missionssystem als fehlerhaft eingestuft.

3.1.4. Zustandsnachrichten oder Fehlermeldung des Missionssystems

Das Missionssystem sendet eine periodische Zustandsnachricht. Ist der Zustand fehlerhaft, bleibt die Zustandsnachricht aus, oder enthält die Zustandsnachricht eine Fehlermeldung, dann wird das Missionssystem als fehlerhaft eingestuft.

3.2. Systemarchitektur des unbemannten Luftfahrtsystems Sagitta

Die Überwachungsinstanz im experimentellen unbemannten Luftfahrtsystem Sagitta muss an der Schnittstelle zwischen dem Missionssystem (Mission Management System MMS) und dem Flugkontrollsystem (FCS) angeordnet sein, um fehlerhafte Ausgaben des Missionssystems erkennen zu können. Um die flugkritischen Anteile von den missionspezifischen Anteilen zu trennen, enthält das Flugkontrollsystem kein missionspezifisches Wissen. Die Überwachungsinstanz ist damit Teil des Mission Management Systems. Sowohl das Flugkontrollsystem, als auch das Missionssystem sind über Funkverbindungen mit jeweiligen Bodenstationen verbunden, an denen der Status verfolgt werden kann, als auch Anweisungen an das unbemannte Luftfahrtsystem gegeben werden können. Der menschliche Bediener an der Bodenstation des Flugkontrollsystems autorisiert das Flugkontrollsystem zur Ausführung von Wegpunkten des Missionssystems.

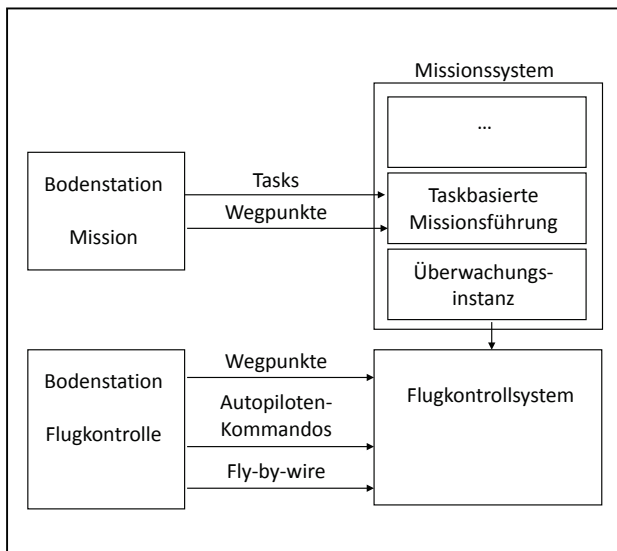


BILD 2 Schnittstellen des Flugkontrollsystems und des Missionssystems

Die Statusanzeige der Überwachungsinstanz wird sowohl auf der Bodenstation zur Missionsüberwachung, als auch auf der Bodenstation zur Flugkontrolle angezeigt.

Die Softwarebestandteile des Missionssystems werden aufgrund der Fehlerreduzierung, der verteilten Entwicklung und Verantwortlichkeiten auf getrennten Computerboards gerechnet. Dies ermöglicht eine Isolierung von Fehlern der experimentellen Softwarebestandteile. Diese Computerboards werden als System in einem Gehäuse zusammengefasst, das als Missionscomputer bezeichnet wird.

Die Überwachungsinstanz unterliegt wie das gesamte Missionssystem des experimentellen

Luftfahrtsystems Sagitta keinen formalen Anforderungen an die Betriebssicherheit. Aufgrund der expliziten Auslegung als Überwachungsinstanz soll aber eine hohe Zuverlässigkeit und Fehlerfreiheit erreicht werden.

4. REAKTION DER ÜBERWACHUNGSINSTANZ BEI ERKANNTEN FEHLERN

Die Überwachungsinstanz stellt für einen autonomen Flug eine zusätzliche Sicherheit vor fehlerhaften Anweisungen des Missionssystems dar. Falls die Überwachungsinstanz einen Fehler im Missionssystem erkannt hat, dann maskiert die Überwachungsinstanz die Fehler durch Generierung von Anweisungen an das Flugkontrollsystem, um einen sicheren autonomen Flug des unbemannten Luftfahrtsystems zum Flugplatz zu gewährleisten.

4.1. Konzept

Die Anweisungen sind wiederum an den Regeln des menschlichen Bedieners angelehnt, welche dieser im Fehlerfall heranzieht. Die Anweisungen sollen ein bekanntes und nachvollziehbares (deterministisches) Verhalten des unbemannten Luftfahrtsystems gewährleisten. Hierzu werden die erforderlichen Randbedingungen vor dem Flug definiert, wie z.B. die Flugroute für einen sicheren Rückflug zum Flugplatz, und der Überwachungsinstanz während der Initialisierung mitgegeben. Für einen Flug entlang dieser Flugroute muss das Missionssystem nicht aktiv sein. Die Überwachungsinstanz in Verbindung mit dem Flugkontrollsystem ist ausreichend für einen Flug entlang der vorgeplanten Route. Die Route endet an einem vordefinierten Punkt (Missionsendpunkt), an dem der menschliche Bediener für den eigentlichen Anflug des Flugplatzes und die Integration in den Flugplatzverkehr die Kontrolle übernehmen muss. Bis der menschliche Bediener die Kontrolle übernimmt wartet das unbemannte Luftfahrtsystem an dem Endpunkt der Route.

4.2. Generierung von Anweisungen

Als zeitkritischen Anteil muss die Überwachungsinstanz die Wegpunkte ab dem erkannten Fehler bis zum Erreichen der vordefinierten Route erstellen. Im Falle einer unmittelbaren Gefährdung des unbemannten Luftfahrtsystems wird zunächst ein Wegpunkt erstellt, den das Flugkontrollsystem direkt anfliegt. Die Position des Wegpunktes ist so zu wählen, dass sich das unbemannte Luftfahrtsystem von der unmittelbaren Gefährdung entfernt. Hierzu muss die Flugleistungsplanung des Flugkontrollsystems berücksichtigt werden, damit die Reaktion des unbemannten Luftfahrtsystems rechtzeitig vor Eintritt der Gefahr eingeleitet wird. Darauf folgend wird von diesem Wegpunkt der am nächsten liegende Punkt der vorab definierten Flugroute für die sichere Rückkehr zum Flugplatz direkt angefliegen. In BILD 3 sind mögliche Positionen

und die jeweiligen nächstliegenden Punkte auf der vorab definierten Flugroute angegeben. Die Flugroute ist entsprechend festgelegt, so dass von jedem Punkt des Missionsgebietes ein direktes Anfliegen dieser Flugroute möglich ist. Der Flug wird mit der im Flughandbuch hinterlegten Geschwindigkeit für größte Reichweite durchgeführt. Der Planungsvorgang in der Überwachungsinstanz ist somit auf ein Minimum beschränkt und jederzeit vorhersag- und kontrollierbar. Die Überwachungsinstanz liefert einen Status an den menschlichen Bediener.

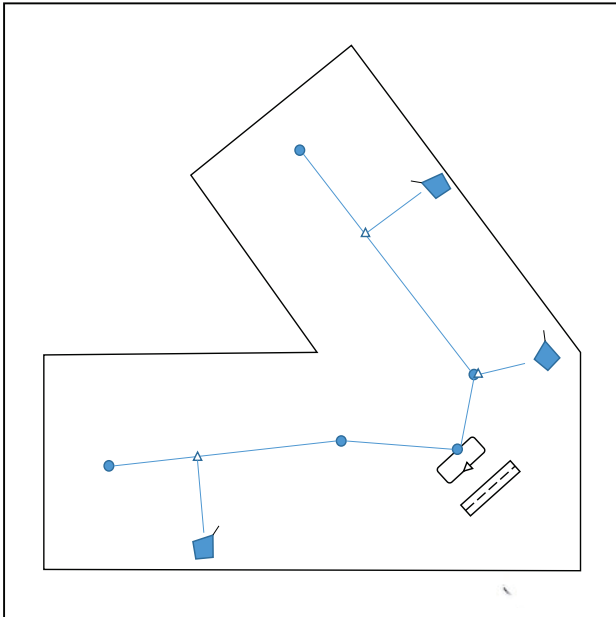


BILD 3 Vorgeplante Route für einen sicheren Rückflug zum Flugplatz

Eine Übernahme der Kontrolle des unbemannten Luftfahrtsystems durch einen menschlichen Bediener ist zu jedem Zeitpunkt des Fluges möglich und kann ressourcenabhängig erfolgen. Die Übernahme durch den menschlichen Bediener erfolgt direkt über das Flugkontrollsystem. In diesem Fall wird das Flugkontrollsystem jegliche Kommunikation an der Schnittstelle zum Missionssystem ignorieren. Die manuelle Übernahme durch den menschlichen Bediener setzt je nach Eingriffsebene eine stabile Kommunikation mit dem unbemannten Luftfahrtsystem voraus.

Prinzipiell ist ein automatisierter Start und Landung unter Führung durch das Missionssystem möglich. In dem experimentellen Luftfahrtsystem Sagitta wird dies aus Sicherheitsgründen zunächst direkt über das Flugkontrollsystem gesteuert erfolgen.

5. ENTWICKLUNGS- UND TESTUMGEBUNG

Die Überwachungsinstanz wird während der Entwicklungszeit des Sagitta Luftfahrtsystems in verschiedenen Testebenen überprüft. Jede Softwareänderung wird zunächst lokal getestet. Hierzu werden Software-in-the-Loop (SiL) Tests und Hardware-in-the-loop (HiL) Tests in verschiedenen Integrationsstufen und an verschiedenen Integrationstestplätzen durchgeführt. Die Integrationstestplätze sind entsprechend dem jeweiligen Absicherungsziel unterschiedlich aufgebaut. Jeweils nicht im Original vorhandene Komponenten werden als Simulation integriert.

Neben der Funktion der Software wird an den Integrationstestplätzen die Funktionsfähigkeit der Hardware nachgewiesen. Zusätzlich dienen die Integrationstestplätze und das fertig integrierte unbemannte Luftfahrtsystem Sagitta auch als Simulator für das Training der Bediener.

Die Flugerprobung findet in verschiedenen Phasen statt.

In Phase 1, welche für September 2015 geplant ist, wird die Inbetriebnahme und Basiserprobung des unbemannten Luftfahrtsystems Sagitta durchgeführt. Das Ziel ist der Nachweis der Leistung im Flug und das Sammeln von Daten zur Erweiterung des operativen Flugbereiches.

Parallel werden die Flüge zur Überprüfung der bereits installierten Komponenten des Missionssystems, wie z.B. der Sensoren, des Missioncomputers und der Datenfunkverbindung genutzt. Das Missionssystem wird in der Phase 1 nicht zur Führung des unbemannten Luftfahrtsystems eingesetzt. Explizite Testfälle für das Missionssystem sind nicht geplant. Die Möglichkeiten zur Erprobung des Missionssystems sind während der Phase 1 damit sehr eingeschränkt.

Die Erprobung des Missionssystems ist im Rahmen einer Phase 2 in 2016 geplant. Die Überwachungsinstanz wird während dieser Flugversuche in Verbindung mit der taskbasierten Missionsführung erprobt. Hierfür muss eine explizite Fehlersituation als Experiment herbeigeführt werden. Die kontrollierte Auslösung der Fehlersituation wird an der Missionsbodenstation durchgeführt. Hierfür werden für das jeweilige Experimente eigene Schnittstellen eingeführt, um eine entsprechende Fehlfunktion in der Missionsplanung auszulösen. Die Experimente werden explizit in Flugtestkarten mit Anweisungen für alle beteiligten Bediener beschrieben. Bei einer unerwarteten Reaktion des unbemannten Luftfahrtsystems muss das Experiment abgebrochen werden und der menschliche Bediener an der Flugkontrollbodenstation muss einen sicheren Zustand herstellen.

Die Experimente für die Überwachungsinstanz dienen des Nachweises der in 3.1 definierten Überwachungen. Um sicherzustellen, dass das unbemannte Luftfahrtsystem während der Experimente die Missionsgrenzen nicht verletzt, werden virtuelle Missionsgrenzen definiert, welche für die Nachweise der Überwachungsinstanz dienen. da das Missionsgebiet auch bei Experimenten nicht verlassen werden darf.

Die Auswertung der Flugversuche wird anhand einer Datenaufzeichnung durchgeführt. Die Datenaufzeichnung erfolgt über einen Flight Test Recorder (FTI), der den Datenverkehr der Bussysteme aufzeichnet und dezentrale Aufzeichnungen, welche darüber hinaus interne Ereignisse aufzeichnen.

6. ZUSAMMENFASSUNG UND AUSBLICK

Unbemannte autonome Luftfahrtsysteme erfordern einen hohen Autonomiegrad. Aufgrund der nicht durchgängig gewährleisteten Überwachung durch einen menschlichen Bediener ist eine hohe Zuverlässigkeit und Fehlerfreiheit auch des Missionssystems erforderlich. Die hier eingesetzten Missionssysteme können nicht nach den Standards für sicherheitsrelevante Systeme verifiziert werden. Um die Betriebssicherheit zu erhöhen können die Ausgaben des Missionssystems überprüft und eventuelle Fehler maskiert werden. Die bisher durch einen menschlichen Bediener am Boden durchgeführte Überwachungsaufgabe wird nun in der Überwachungsinstanz an Bord des unbemannten Luftfahrtsystems ausgeführt um einen autonomen Flug ohne menschlichen Bediener zu gewährleisten. Falls erforderlich wird ein „standby-spare“ aktiviert, der anhand der gleichen Regeln, wie der menschliche Bediener auch einen sicheren Flug zum Flugplatz ermöglicht. Die Überwachungsinstanz wird in dem experimentellen unbemannten Luftfahrtsystem Sagitta implementiert werden und in Flugversuchen erprobt.

7. LITERATUR

[1] H. Putzer and R. Onken, "COSA - A generic cognitive system architecture based on a cognitive model of human behavior," *Cognition, Technology & Work*, vol. 5, no. 2, pp. 140–151, 2003.

[2] Gerrit Kahn, Nikolaus Theißing, Axel Schulte. „Cognitive Automation based Guidance and Operator Assistance for semi-autonomous Mission Accomplishment of the UAV Demonstrator SAGITTA“; In: *61. Deutscher Luft- und Raumfahrtkongress 2012*. Berlin, Deutschland. 10.-12. September 2012

[3] Johann Uhrmann & Axel Schulte. Task-based Guidance of Multiple UAV Using Cognitive Automation. In: *The Third International Conference on Advanced Cognitive Technologies and*

Applications. COGNITIVE 2011. Rome, Italy. 25-30 September 2011.

[4] J. Voas; „An Approach to Certifying Off-the-Shelf Software Components“; *IEEE Computer*; 31(6): 53-59; Juni 1998

[5] B. Randell, "System Structure for Software Fault Tolerance", *IEEE Transactions on Software Engineering*, vol. SE-1, pp. 220-232, Juni, 1975