Journal of Systems Architecture 90 (2018) 94–108

Contents lists available at ScienceDirect

Journal of Systems Architecture

journal homepage: www.elsevier.com/locate/sysarc

Architectural design of a Safe Mission Manager for Unmanned Aircraft Systems

Hector Usach[a,*], Juan A. Vila[a], Christoph Torens[b], Florian Adolf[b]

[a] Universitat Politècnica de València, Camí de Vera s/n, València 46022, Spain
[b] German Aerospace Center (DLR), Institute of Flight Systems, Dept. Unmanned Aircraft, Lilienthalplatz 7, Braunschweig 38108, Germany

ARTICLE INFO

Keywords:
Software architecture
Automated Contingency Management
Formal methods
Partitioning
UAS

ABSTRACT

Civil Aviation Authorities are elaborating a new regulatory framework for the safe operation of Unmanned Aircraft Systems (UAS). Current proposals are based on the analysis of the specific risks of the operation as well as on the definition of some risk mitigation measures. In order to achieve the target level of safety, we propose increasing the level of automation by providing the on-board system with Automated Contingency Management functions. The aim of the resulting Safe Mission Manager System is to autonomously adapt to contingency events while still achieving mission objectives through the degradation of mission performance. In this paper, we discuss some of the architectural issues in designing this system. The resulting architecture makes a conceptual differentiation between event monitoring, decision-making on a policy for dealing with contingencies and the execution of the corresponding policy. We also discuss how to allocate the different Safe Mission Manager components to a partitioned, Integrated Modular Avionics architecture. Finally, determinism and predictability are key aspects in contingency management due to their overall impact on safety. For this reason, we model and verify the correctness of a contingency management policy using formal methods.

1. Introduction

Unmanned Aerial Systems (UAS) have been developing very quickly, thus presenting a challenge to traditional aviation. The European Aviation Safety Agency (EASA) is elaborating a new regulatory framework for the operation of UAS. The current proposal establishes three categories of UAS operation according to their risk levels [1,2]. The *open category* is for low risk operations where safety is ensured through compliance with operational limitations, mass limitations, product safety requirements and a minimum set of operational rules. Authorization from a National Aviation Authority (NAA) is not required. The *specific category* is for medium risk operations and requires NAA authorization based on a risk assessment performed by the operator. A manual of operations lists the risk mitigation measures. Finally, the *certified category* is for large UAS flying in non-segregated airspace, the requirements for which are comparable to those for manned aviation. The International Civil Aviation Organization (ICAO) addresses this category in Doc. 10019 AN/507 [3]. According to that document, "only unmanned aircraft that are remotely piloted could be integrated alongside manned aircraft in non-segregated airspace and at aerodromes". This work is focused on Remotely Piloted Aircraft Systems (RPAS), a subclass of UAS.

The specific risks of an RPAS operation as compared to manned aviation are: *(1)* reduced situational awareness of the remote pilot, and *(2)* risk of losing the communication & control (C2) link between the remote pilot and the unmanned aircraft. In the former case, reduced situational awareness means that remote pilots, unlike pilots of manned aircraft in visual conditions, have reduced perception of environmental elements and events, which results in complex decision-making, especially during an emergency. In the latter case, the C2 link loss is a degradation or failure of the communication channel, which may result in the aircraft "flying not under command" [3].

UAS that aim to operate within the specific category, and ultimately within the certified category, are required to mitigate the aforementioned specific risks in order to achieve the *target level of safety*. This can be accomplished through several complementary approaches, such as setting the aforementioned operational limitations and even imposing certain functional requirements onto the on-board equipment. For example, some special technical equipment is often required to compensate for the reduced situational awareness, mainly Detect and Avoid (DAA) devices [3]. Another approach relies on operational flight planning and development of operations manuals with provisions for contingency handling.

In general, the functional requirements imposed on the on-board equipment exemplify the need for increased autonomous flight capabilities in RPAS. This is a focus of this paper. The software framework under development by the German Aerospace Center (DLR) for its research

* Corresponding author.
E-mail address: hecusmo@doctor.upv.es (H. Usach).

https://doi.org/10.1016/j.sysarc.2018.09.003
Received 14 May 2018; Received in revised form 24 August 2018; Accepted 11 September 2018
Available online 12 September 2018

fleet of unmanned aircraft enables high level autonomous behaviors. One of its key software components is the automated Mission Planner and Execution (MiPlEx) system. MiPlEx performs real-time mission plan execution, 3-D world modeling, as well as algorithms for combinatorial motion planning and task scheduling [4,5]. The Technical University of Valencia (UPV) is also developing a similar component based on the same architectural principles [6]. However, both *Mission Manager* implementations have so far only made use of operational limitations to achieve the target level of safety, e.g. operating in Very Low Level (VLL) or segregated airspace. As a collaboration between the two institutions, the goal is to safely increase the level of automation to develop a *Safe Mission Manager* System. This concept expands on the current Mission Manager by incorporating Automated Contingency Management (ACM) functions. The resulting system is expected to adapt autonomously to *contingencies*, while still achieving mission objectives by allowing some degradation on mission performance.

In this paper, we discuss the architectural design of the proposed Safe Mission Manager System. In addition, we also discuss how to allocate the different software components of the resulting system to an Integrated Modular Avionics (IMA) architecture. Finally, we propose using formal methods for specifying and verifying the contingency management policy. The rest of the paper is organized as follows: Section 2 presents related works in bibliography; Section 3 describes the initial Mission Manager System; Section 4 identifies the need for contingency management in RPAS; Section 5 discusses architectural considerations for integrating ACM functions into the previous Mission Manager; Section 6 presents the safety aspects relating to the software development of the resulting system; Section 7 develops the contingency management policy using formal methods; and finally, Section 8 concludes the paper.

2. Related work

The main topics of this paper are contingency management architectures, with special emphasis on UAS specific contingencies, and the use of formal methods in the software development process.

The primary guidelines for contingency management can be found in the proposals of regulatory frameworks for operating UAS currently being drawn up by Civil Aviation Authorities. These guidelines define risks and propose some risk mitigation procedures, among other things. UAS regulation in Europe is led by EASA, which has published the *Introduction of a regulatory framework for the operation of unmanned aircraft* [1], and the *Roadmap for the Integration of Remotely Piloted Aircraft Systems into the European Navigation System* [7]. A similar effort has been undertaken by the Unmanned Aircraft Systems Registration Task Force of the Federal Aviation Administration (FAA) in the United States [8,9]. In addition, the ICAO has published the *Manual on RPAS* [3] to provide guidance on technical and operational issues applicable to the integration of RPAS in non-segregated airspace and at aerodromes.

There is an important research effort behind the regulatory proposals. The main research frameworks are the SESAR program in Europe [10] and the NextGen program in the United States. Some of the projects falling within these initiatives are also related to this work. One of the most relevant is the *Automated Contingency Management* (ACM) [11–13], which is a NASA-led research project in collaboration with Impact Technologies, LLC and Georgia Tech. ACM is designed to improve the reliability and survivability of safety-critical aerospace systems. The approach of ACM differs from the one presented in this paper in its focus on control optimization techniques rather than on the use of formal methods. One interesting extension to this approach is the work in [14] where human-machine interface considerations in contingency management are discussed. Another NASA project on drones is the Unmanned Aircraft System (UAS) Traffic Management (UTM). The UTM concept [15] was proposed as a traffic management scheme to enable civilian low-altitude UAS operations. This work's most relevant proposal with regard to contingency management is the level of automation. The proposed scheme ranges from a completely manual process relying on the operator (Build 1) to fully automatic, large-scale, system-wide contingency handling (Build 4).

The DLR has also conducted important research in the field of RPAS in the WASLA-HALE project for the High Altitude Long Endurance domain. Some research work focuses on the procedures and techniques for integrating UAS into controlled airspace [16,17]. The proposed procedures are mainly related to C2 link failure conditions and communication with ATC. Another interesting aspect is the use of formal descriptions for enabling automatic reasoning on the consistency and correctness of the model requirements and the generation of on-line monitoring checks [18]. Case studies show that the process of formally writing down requirements is extremely helpful in understanding the domain inherent concepts [19].

The introduction of a Safety Monitor like the one in this paper is also suggested in [20]. The goal of the referenced work, however, is to expand the operational range and raise the autonomy level, rather than contingency handling. The work in [21] presents a predictive alerting method that uses multiple hypothesis prediction. It integrates all the onboard sensors and information sources with a stochastic estimator to obtain an accurate and reliable estimation of the aircraft state, which is key for contingency detection.

Regarding contingency management policies, C2 link loss is one of the most difficult to handle since any other contingency may also occur after it. The work in [22] presents a method for computing optimal lost-link policies for unmanned aircraft conducting surveillance alongside manned aircraft in a wildfire scenario. Another contingency handling policy especially important to UAS is collision avoidance. The work in the NextGen and SESAR programs led to the definition of a new Airborne Collision Avoidance System (ACAS) based on new logics, namely ACAS X. Its definition contains two particular variations: ACAS Xa for large aircraft, and ACAS Xu for unmanned aircraft. The work in [23] describes the specificities and challenges to the ACAS Xu system.

3. Initial Mission Manager architecture

The Mission Manager is the core system for performing the automatic guidance and control of the RPAS. Its functionality is based on the definition of a *Mission Plan* that basically specifies the RPAS route and payload actions. Both the MiPlEx framework and the Mission Manager developed at the UPV implement a software architecture based on the ideas of the three-tier (3T) architecture [24]. In general, a 3T architecture separates the intelligent control problem into three interacting layers named *Deliberative layer, Sequencing layer*, and *Reactive layer*. In this approach, the 3T concept has been applied from a flight guidance and control perspective, and the three layers have been renamed as *Path Planner, Guidance System*, and *Flight Director*, respectively, shown in Fig. 1.

The *Path Planner* is the high level component that has the ability to generate a reference trajectory for the Guidance System. As it is shown in Fig. 1, there exist multiple path planners that provide different path planning policies. The "Mission Planner" is a path planner that generates this trajectory based on the directives of the Mission Plan. In this approach, the Mission Plan is specified as a sequence of *flight legs* that implement the ARINC 424 *path terminators* [25]. Thus, the role of the Mission Planner is to provide each flight leg to the Guidance System in a sequential manner. In parallel to the Mission Planner, there exist some other *Task Specific Planners* for special tasks, such as the exploration of unknown terrain. From an abstract point of view, both the Mission Planner and the Task Specific Planners belong to a same class of objects with the ability to provide instructions for the Guidance System based on different criteria. The remote pilot should select the required Task Specific Planner manually in accordance with the current operational condition.

The *Guidance System* determines how to fly the reference trajectory provided by the active Path Planner and then activates the appropriate control modes of the Flight Director. To do so, the Guidance System uses a library of elemental maneuvers in the lateral plane (LNAV) and in