Reliability Engineering and System Safety 167 (2017) 383–393

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Unmanned aerial vehicle safety assessment modelling through petri Nets☆

P. Gonçalves[a,*], J. Sobral[b,c], L.A. Ferreira[d]

[a] Portuguese Air Force Development and Innovation Research Centre (CIDIFA), Academia da Força Aérea, Av. Leite de Vasconcelos, N.° 4 2614-506 Amadora, Portugal
[b] Mechanical Engineering Department, ISEL – Instituto Superior de Engenharia de Lisboa, Rua Conselheiro Emídio Navarro, 1, 1959-007 Lisboa, Portugal
[c] Centre for Marine Technology and Engineering (CENTEC), Instituto Superior Técnico, Universidade de Lisboa, Av. Rovisco Pais, 1049-001 Lisboa, Portugal
[d] Faculty of Engineering of University of Porto (FEUP), Universidade do Porto, Rua Dr. Roberto Frias, s/n 4200-465 Porto, Portugal

ARTICLE INFO

Keywords:
Petri Nets
UAV
UAS
Safety assessment

ABSTRACT

Currently we are facing an increasing trend of use of Unmanned Aerial Vehicles (UAV) in various activities both civilian and military. Although there is no legal framework for the operation of these systems, regulatory authorities require the demonstration of a safety level equivalent to manned aircraft. It is known the high vulnerability of the UAV not only to unexpected failures of their systems but also to the environment. The purpose of this paper is to present a safety assessment process modelling of a UAV by Petri Nets, that can be accepted by certifying bodies, considering the recommendations of STANAG 4671 UAV Airworthiness Requirements Specification (USAR) for analysis of fault conditions that lead to the most feared events. It is intended to show through the use of Petri Nets the frequency that the UAV enters the identified states described as most feared events; the ability of the UAV to react after being in a fault situation to the inputs of the operating crew in order to enhance trust and to facilitate the operation authorization process in UAV operations.

The results obtained allowed to identify and to define critical areas and corrective actions that will lead to an acceptable level of risk for the regulatory authority.

1. Introduction

Nowadays, Unmanned Aerial Vehicles (UAV) or Unmanned Aerial Systems (UAS) are employed in several areas such as complex military missions, maritime surveillance, border surveillance, environmental monitoring, agriculture and many other applications.

Despite the tremendous efforts made by the UAV manufacturers and operators they encounter a huge difficulty to overtake the mistrust feeling around these systems operations.

In order to produce a higher level of confidence in the UAV and on their operations and to facilitate the operational authorization process, the regulatory authorities require the presentation of a Safety Assessment process, usually developed in the design phase which among others aspects identifies potential failure conditions in operation of a particular UAV, their consequences and all mitigation measures implemented to reduce the severity of the identified failures.

However, and in accordance to the recommendations presented in Article 8 of the Convention on International Civil Aviation (ICAO) [1], "*No aircraft capable of being flown without a pilot shall be flown without a pilot over the territory of the contracting State without special authorization by que State and in accordance with the terms of such authorization* …". This assumption stems from the need that regulators have to make the integration of various types of aircraft (manned and unmanned) in the National Airspace System [2,3]. Thus, although there is still no regulatory framework suitable for the UAV, it is assumed that manned or unmanned aircraft share a high degree of commonality related to the airworthiness [1,4–6]. Therefore, most airworthiness analysis probably are based on those which are currently prescribed for manned aircraft: "*UAV certification will be based on a determination of equivalence with the existing Certification Specifications (CS) developed for manned aircraft, wherever possible*" [4].

Abbreviations: ARP, Aerospace Recommended Practice; CMA, Common Mode Analysis; Comms Fails, Communications Fails; FAA, Federal Aviation Administration; FHA, Functional Hazard Assessment; Fght Fails, Flight Controls Fails; FMEA, Failure Mode and Effects Analysis; GRIF, Graphical Interface for Reliability Forecasting; Land Pred Site, Land Predetermined Site; Loss UAV MNV, Loss UAV Maneuver; Loss UAV Ctrl, Loss UAV Control; MFE, Most Feared Events; PN, Petri Nets; Prop, Propulsion System Fail; PSSA, Preliminary System Safety Assessment; RTCA, Radio Technical Commission for Aeronautics; SAE, Society of Automotive Engineers; SF, System Fail; SSA, System Safety Assessment; SR, System Recovered; STANAG, Standard Agreement; Total Loss UAV Ctrl, Total Loss UAV Control; UAS, Unmanned Aerial Systems; UAV, Unmanned Aerial Vehicles; UAV Ctrl, UAV Control; UAV MNV, UAV Maneuver; UnP Land Site, Unplanned Land Site; USAR, Unmanned Aerial Vehicles Systems Airworthiness Requirements.

☆ This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

* Corresponding author.
E-mail addresses: pagoncalves@academiafa.edu.pt (P. Gonçalves), jsobral@dem.isel.ipl.pt (J. Sobral), lferreir@fe.up.pt (L.A. Ferreira).

http://dx.doi.org/10.1016/j.ress.2017.06.021
Received 1 June 2016; Received in revised form 12 June 2017; Accepted 18 June 2017
Available online 21 June 2017
0951-8320/

One of the essential elements in a UAV airworthiness certification process is the Safety Assessment, because the results of such analysis will determine the inherent level of safety [6].

Several regulators like Federal Aviation Administration (FAA), the European Aviation Safety Agency (EASA) or the Civil Aviation Authority (CAA) accept the use of Unmanned Systems Airworthiness Requirements (USAR) developed by the French Military Authorities that were later updated by NATO FINAS group to produce the STANAG 4671, as a reference for defining the basis for the airworthiness certification process as long as the applicable airworthiness codes are identified [4].

Safety Assessment of an aircraft is based on a set of safety requirements and on a system model that includes both nominal behaviour and failure mode behaviours [7]. It is a comprehensive and thorough analysis where an evaluation of the possible failure modes, and their consequences, is performed for each aircraft function and their systems. Also, the mitigation measures required to reduce the risk in operation to an acceptable level are outlined.

1.1. Problem statement

At the beginning of the UAV operation, and during the airworthiness certification process, exists an uncertainty about the response of new aircrafts towards feared events, despite the identification of system vulnerabilities and the development of mitigation measures at the Safety Assessment process.

To reduce this perception of uncertainty, it is mandatory to have access to tools to provide logical assertions about the operation of a given aircraft (e.g. a bad state will never be reached). Moreover, it is also desirable to compute quantitative metrics about the mission Safety Assessment such as the probability that a failure condition will affect the aircraft operation and formal notations should be able to describe system models as well as failure modes.

Due to the current lack of a well-established model, the analysis is usually performed in an empirical way, based on real flight data and safety requirements defined in the reference literature.

Different strategies have been proposed regarding to the Safety Assessment of unmanned aircraft. NASA [8] conducted a study in which it is addressed the definition and classification of hazards for unmanned systems, and also how these definitions could be applied in the preliminary functional hazard assessment of a generic Unmanned Aircraft System. It describes the hazard assessment process used in civil aviation, and how that process may be tailored to address unique aspects of a UAV. A Preliminary Functional Hazard Assessment (FHA) of a generic UAV was presented, with a functional decomposition through listing the high-level functions required for the safe and routine flight of a generic UAV. Trigos et al [9] formalized a model and failure diagnoser and applied it to Unmanned Aerial Vehicles. The model and diagnoser uses a hybrid Petri Net.

In this work we propose a new comprehensive model intended to detect the critical failures that could lead to the cancellation of the flight mission or an emergency landing. This paper addresses the Safety Assessment process applied to UAV through the real dynamics of the UAV modelling. It is considered that the failure conditions referred as Most Feared Events in STANAG 4671 are evident to UAV crew.

The Petri Nets (PN) were used to build the model because it is an excellent tool that allows performing statistical and logical analysis. The Safety Assessment model presented in this paper begins with the definition of the PN model for all flight phases considered for an UAV, for each failure condition and for each Most Feared Event defined. At the end the integration model is performed. It is part of a certifying process for UAV's, which model is described in a previous paper [10].

Given a particular type of Unmanned Aerial Vehicles (waypoint navigation, path defined by a set of points in the map), the focus is the identification of failure conditions that may lead to the feared events as they are defined in USAR [11], during normal operation, using PN. The problem statement is defined on the following questions about an UAV:

1. Will it ever get in a certain particular state, (e.g. one of the most feared events)?
2. Will it have the ability to react to inputs?
3. Will it be able to achieve a desired state?

The proposed model encompasses the UAV Safety Assessment issue from this perspective, where the real dynamics of the UAV is modelled in presence of the failure condition that lead to Most Feared Events, contributing to the development of evidence that demonstrate and strengthen the confidence in the reliability and the safety of UAV operations, which is extremely important in the airworthiness certification process.

The remainder of the paper is as follows. Section 2 briefly describes the Safety Assessment process related to UAV. Section 3 resumes the theory of Petri Nets and Section 4 emphasizes the assumptions and UAV operating concepts. Section 5 presents the construction of the Safety Assessment of an UAV model. Finally, Section 6 presents the analysis and the conclusions of this work related to the Safety Assessment of UAV flight, a situation that would greatly facilitate operators and regulators in the demonstration process of evidences of reliability and safety of UAV operations.

2. Safety assessment

The Safety Assessment process encompasses the development and verification of the requirements underlying the inherent activities in the design phase of an aircraft. This process provides a methodology to evaluate the functions of the aircraft and the design of the systems that will perform those functions, in order to determine whether the identified potential hazards have been properly handled. To perform a safety assessment for an UAV, it is necessary to address other aspects than the aircraft itself. It should include control ground station, data links, mission planning, interoperability with Air Traffic Control and others aircrafts, operation environments, mission types, operator's competences and their procedures, level of autonomy and its predictability, emergencies and abnormal flight conditions [11]. For most aircraft, the Safety Assessment process that is most widely accepted in the aeronautics industry is qualitative. When quantitative, it consists in conducting a Functional Hazard Assessment (FHA), a Preliminary System Safety Assessment (PSSA), and a System Safety Assessment (SSA) [11].

The Functional Hazard Assessment of aircraft functions is performed to identify and classify the failure conditions of those functions according to their severity [11].

The Preliminary System Safety Assessment is a systematic evaluation of the proposed system architecture and its implementation is based on the FHA and the classification of failure conditions in order to be achieved the requirements for all items [11].

The System Safety Assessment is a systematic evaluation of the implemented systems in order to demonstrate that the prevailing requirements are met [11].

For UAV, the Safety Assessment requirement is presented in various airworthiness military standards such as STANAG 4671, STANAG 4702 and STANAG 4703. Such standards address the airworthiness requirements for UAV which are intended to operate in non-segregated airspace.

According to STANAG 4671, Unmanned Aerial Vehicles Systems Airworthiness Requirements (USAR), the UAV must be designed to reduce the risk to people, the UAV crew and third parties at levels that are acceptable to regulators [12]. Such requirements present a risk reference system which is a combination of severity and frequency. The minimum acceptable level of safety for UAV equipment, systems and their installations are shown through the risk reference presented in Table 1.

In this sense, it is important to understand the failure conditions concept. *Failure Conditions: A condition having an effect on either the airplane or its occupants, or both, either direct or consequential, which is caused or contributed to by one or more failures or errors considering flight phase and*