Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 128 (2015) 54 – 63

Procedia Engineering

www.elsevier.com/locate/procedia

3rd European STAMP Workshop, STAMP EU 2015

The integration of drones in today's society

Mitchel Pappot[a], Robert J. de Boer[a]*

[a]*Amsterdam University of Applied Sciences, Aviation Academy, Weesperzijde 190, 1097 DZ Amsterdam, the Netherlands*

Abstract

The integration of Remotely Piloted Aircraft Systems (RPAS) in today's society depends on the ability of their operators to demonstrate safety. RPAS operators use risk matrices, as required by the Dutch government, to indicate the safety level. Key issues with this approach include the lack of available component reliability data for determining the risk factors, and the exclusion of human interactions. This study aims to determine the competence of the Systematic Theoretic Process Analysis (STPA) to demonstrate the safety of RPAS operations. It is concluded that the STPA is a comprehensive method to demonstrate the safety of RPAS operations.

Keywords: civil RPAS; civil Drones; STPA; STAMP; safety; systems theory; risk matrices

1. Introduction

Remotely Piloted Aircraft Systems (RPAS) are increasingly used for private and business needs. Because of recent developments in regulations related to the operation of business RPAS, the market now sees a great potential in the use of RPAS for commercial and civil purposes. However, the permission to use professional RPAS is highly dependent on the ability of the operator to demonstrate the safety of these operations to the authorities, and therefore on the type of operation. RPAS operated within the borders of the European Union (EU) are divided into two weight categories: 'Light' RPAS with a gross weight up to 150 kg which are controlled by local government authorities in the specific country of operation; and 'heavy' RPAS with a gross weight above 150 kg that are regulated by the EASA [1]. Light RPAS have been found to be particularly suitable for civil operations. RPAS have already been used for

* Corresponding author. Tel.: +31618561188
E-mail address: M.K.Pappot@hva.nl

doi:10.1016/j.proeng.2015.11.504

aerial cinematography, ground mapping, crop inspections and the inspection of windmill blades. Other applications, such as crowd control, surveillance, chemical detection and firefighting are of interest for commercial RPAS manufacturers and operators but are severely restricted in the interest of public safety.

Current safety assessment techniques used to determine the safety of RPAS in civil operations are based upon the identification of hazards and classification of the risk for each identified hazard. The current methodology mainly reasons from the failure or inadequate functioning of individual components that might result in accidents. Human errors, software errors and external disturbances are generally not considered during the analysis. However, new methods based on systems thinking have recently become available that do incorporate interactions between system components and potentially identify flaws in human performance, in software and due to external disturbances. One such approach is Systematic Theoretic Process Analysis (STPA).

The aim of this study is to investigate the ability of STPA to demonstrate the safety of light RPAS operations for business and determine whether the STPA is a more preferable analytical method compared to the current hazard identification and risk matrix safety analysis method used by the RPAS industry. To do so, the STPA and the current methodology are applied to case studies in the context of civil RPAS operations.

2. Background

2.1. STAMP / STPA

STAMP is a safety model based on systems theory. Unlike the traditional safety assessment methodologies STAMP does not use a chain of event model to describe the occurrence of accidents [2]. Instead, safety models based on systems theory consider accidents as a result of interactions between components; they do not represent a single cause for an accident, but reveal multiple factors - variables that collectively contribute to an accident [3]. STAMP views safety as a control problem and supports that accidents do not merely occur from component failures. Instead, accidents occur because of inadequate enforcement of safety constraints, inadequate control of system components or external disturbances considering the interactions between people, organizational structures, and the physical system components [4]. STAMP contemplates the system to be in a state of dynamic equilibrium. The equilibrium state is established by the control and feedback links among components. Viewing the process as a dynamic state means that the system adapts to internal and environmental changes. STAMP is based on three stages: defining the safety constraints, generating a hierarchical control structure and developing a systemic process model [5].

2.1.1. Safety constraints

STAMP embeds the concept of imposing constraints on a system's degrees of freedom [6]. An accident or loss is the result of inadequate enforcement of safety constraints rather than a single failure resulting in a loss or accident. Constraints can be applied during the design and operation of a system, to ensure safe system behaviour. Constraints are derived from the purpose and functions of a system. Enforcement of safety constraints is necessary to prevent the system moving towards a hazardous state. A person or organisation that places constraints on another level of the system also needs some form of feedback to be able to reflect on the effectiveness of the safety constraints [4].

2.1.2. Hierarchical control structure

A system can be represented graphically as a hierarchical control structure. The aim of a hierarchical control structure is to identify the system components, facilitate the generation of safety constraints and depict the feedback loops within the system [2]. Each level in the hierarchical control structure imposes constraints on the level below it. Constraints for each level of the structure can include design, process, operational, manufacturing and managerial constraints [7]. Constraints - when related to safety - specify the relationships between system variables that contribute to the safe state of the system [6]. The hierarchical control structure consists of two basic structures with communication links between them. The first part consists of the system development structure, where levels impose constraints on the design and development of the system. The second part of the structure is dedicated to the operation of the system [8]. Although a basic hierarchical control structure consists of the development and operational control structure, additional structures can be added to the model when these carry the responsibility of enforcing the safety