This file set is a supporting material for our paper [1].

The abstract of this paper is: In order to handle undesirable failures of a multicopter which occur in either the pre-flight process or the in-flight process, a failsafe mechanism design method based on supervisory control theory is proposed for the semi-autonomous control mode. Failsafe mechanism is a control logic that guides what subsequent actions the multicopter should take, by taking account of real-time information from guidance, attitude control, diagnosis, and other low-level subsystems. In order to design a failsafe mechanism for multicopters, safety issues of multicopters are introduced. Then, user requirements including functional requirements and safety requirements are textually described, where functional requirements guide to model a general multicopter plant, and safety requirements cover the failsafe measures dealing with the presented safety issues. Based on these requirements, several multicopter modes and events are defined. On this basis, the multicopter plant and control specifications are modeled by automata. Then, a supervisor is synthesized by Supervisory Control Theory (SCT). In addition, we present three examples to demonstrate the potential conflicting phenomenon due to inappropriate design of control specifications. Also, we discuss the properties of the obtained supervisor. The formal method based on SCT increases our confidence on the correctness of the designed failsafe mechanism. Finally, based on the obtained supervisor, an implementation method suitable for multicopters is presented, in which the supervisor is transformed into decision-making codes.

This paper presents the procedure of applying SCT to an engineering problem, from requirement analysis to supervisor synthesis, and finally to implementation on a real time flight simulation platform of quadcopters developed by MATLAB. Supplement materials will include:

(1) A supplement file to describing the other specification modeling because of space limitation for the submitted paper (File fold: Support document.zip);

(2) Source files of TCT and Supremica (File fold: Source files of TCT and Supremica);

(3) A function to export the transition matrix based on the output file of software (File fold: MATLAB files for processing XML file from Supremica);

(4) A video to show the failsafe mechanism on a real-time flight simulation platform of quadcopters developed by MATLAB (File fold: Video).

[1] Quan Quan, Zhiyao Zhao, Liyong Lin, Peng Wang, Walter Murray Wonham, and Kai-Yuan Cai. Failsafe Mechanism Design of Multicopters Based on Supervisory Control Theory. https://arxiv.org/abs/1704.08605.