Support Material of Manuscript "Failsafe Mechanism Design of Multicopters Based on Supervisory Control Theory"

Quan Quan*, Zhiyao Zhao, Liyong Lin, Peng Wang, Walter Murray Wonham, *Life Fellow*, *IEEE*, and Kai-Yuan Cai

Abstract

This is a support material of manuscript "Failsafe Mechanism Design of Multicopters Based on Supervisory Control Theory". In this material, it contains three contents: 1) control specifications for the 'in air' component of *Plant*; 2) input of the plant and control specifications to *TCT* software; 3) supervisor synthesis by decentralized supervisory control and supervisor reduction.

A. Control specifications for the 'in air' component of Plant

For the 'in air' component of *Plant*, safety requirements *SR2-SR13* restrict what actions the user wants the multicopter to perform under specific situations when it is in air. Thus, we design 24 specifications to cover all possible strings in the 'in air' component of *Plant*. The traversal relation between the designed specifications and the structure of the 'in air' component of *Plant* is shown in Figure 1.

1) Specification 2: This control specification is obtained by partially transforming "safety requirements *SR2-SR6*" to an automaton model. As shown in Figure 2, *Specification 2* contains 13 states (S_0-S_{12}), 33 events and 129 transitions. Here, the states S_0,S_1 are marker

Q. Quan, P. Wang and K.-Y. Cai are with School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China (e-mail: qq_buaa@buaa.edu.cn, wp2204@gmail.com, kycai@buaa.edu.cn). Z. Zhao was with School of Automation Science and Electrical Engineering, Beihang University and is now with School of Computer and Information Engineering, Beijing Technology and Business University, Beijing 100048, China (zhaozy@btbu.edu.cn). L. Lin and W. M. Wonham are with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: liyong.lin@utoronto.ca,wonham@control.utoronto.ca). The corresponding author Q. Quan is also with the Department of Electrical and Computer Engineering, University of Toronto as a visiting professor.

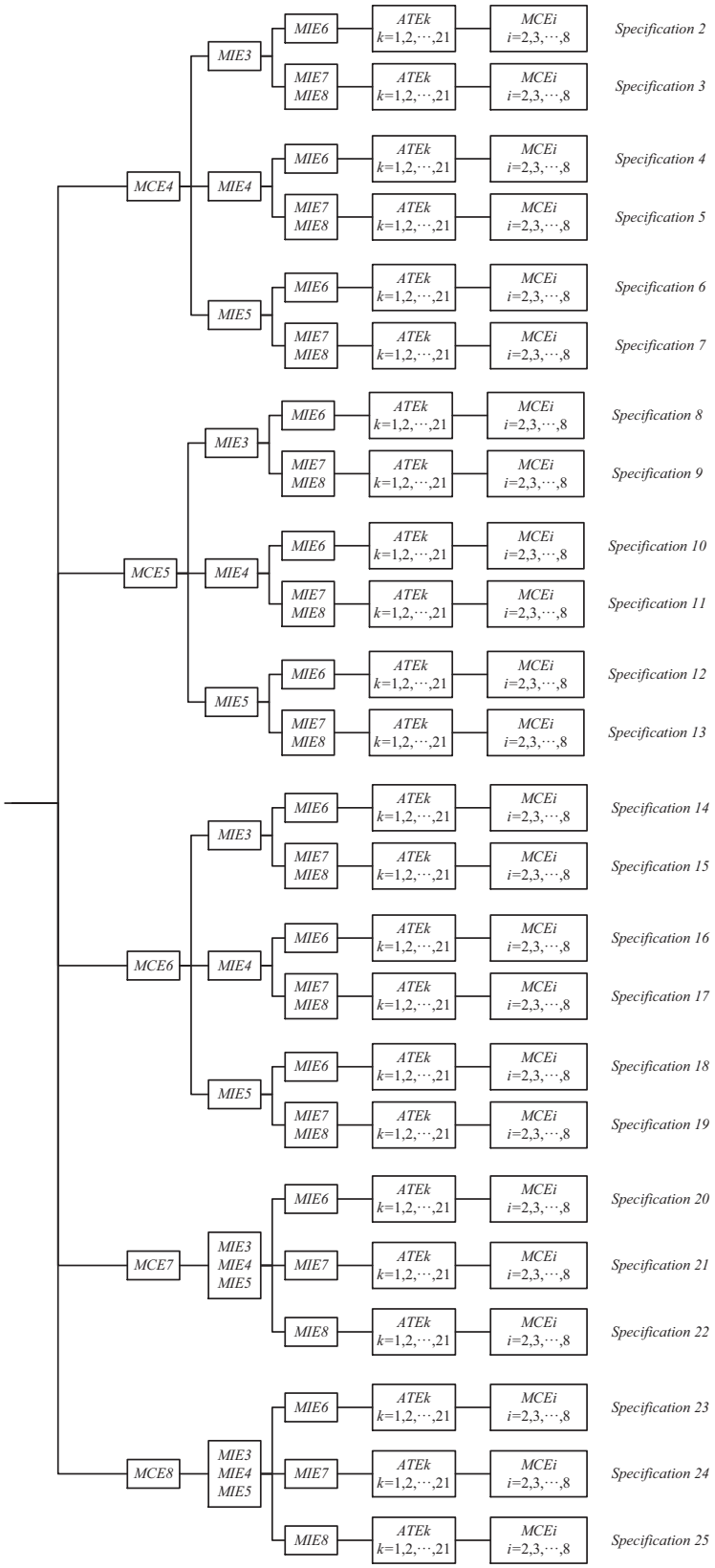

Fig. 1. Traversal relation between 24 control specifications and the structure of the 'in air' component of *Plant*

states. The state S_1 represents LOITER MODE, and the state S_0 integrates other multicopter modes.

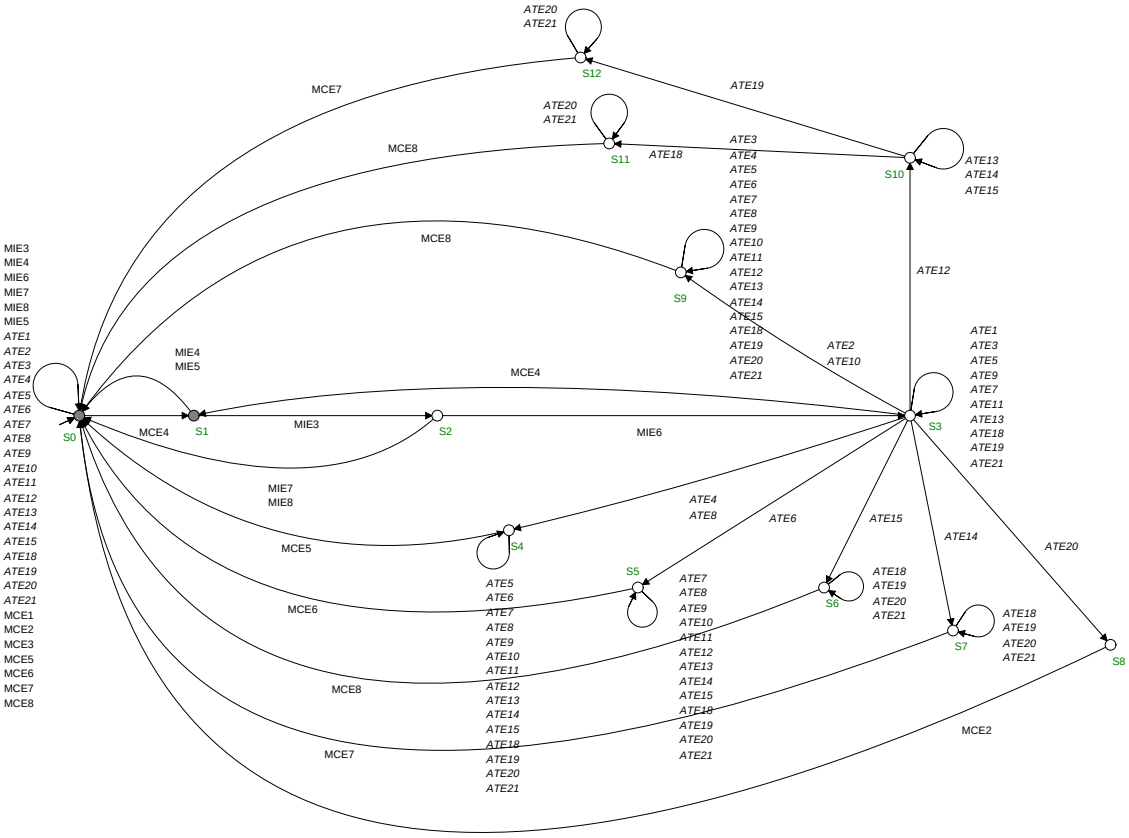

Fig. 2. Automaton model of *Specification 2*. *Specification 2* is triggered under the three successive conditions: i) the multicopter is in LOITER MODE (*MCE4* occurs); ii) the remote pilot executes an arm action (*MIE3* occurs); and iii) the flight mode switch is on the position of "normal flight" (*MIE6* occurs). In this case, if the GPS or compass is unhealthy (*ATE4* or *ATE8* occurs), the multicopter enters ALTITUDE-HOLD MODE (*MCE5* occurs); if the barometer is unhealthy (*ATE6* occurs), the multicopter enters STABILIZE MODE (*MCE6* occurs); if the INS or propulsors are unhealthy (*ATE2* or *ATE10* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the connection to the RC transmitter is abnormal (*ATE12* occurs), and the multicopter's distance from the base is less than a given threshold (*ATE18* occurs), then the multicopter enters AL MODE (*MCE8* occurs); if the connection to the RC transmitter is abnormal (*ATE12* occurs), and the multicopter's distance from the base is not less than a given threshold (*ATE19* occurs), then the multicopter enters RTL MODE (*MCE7* occurs); if the battery's capacity is inadequate but the multicopter is able to perform RTL (*ATE14* occurs), the multicopter enters RTL MODE (*MCE7* occurs); if the battery's capacity is inadequate and the multicopter is unable to perform RTL (*ATE15* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), the multicopter enters STANDBY MODE (*MCE2* occurs); otherwise, the multicopter stays in LOITER MODE (*MCE4* occurs).

2) Specification 3: This control specification is obtained by partially transforming "safety requirements *SR7* and *SR8*" to an automaton model. As shown in Figure 3, *Specification*

3 contains 6 states (S_0-S_5), 31 events and 91 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents LOITER MODE, and the state S_0 integrates other multicopter modes.

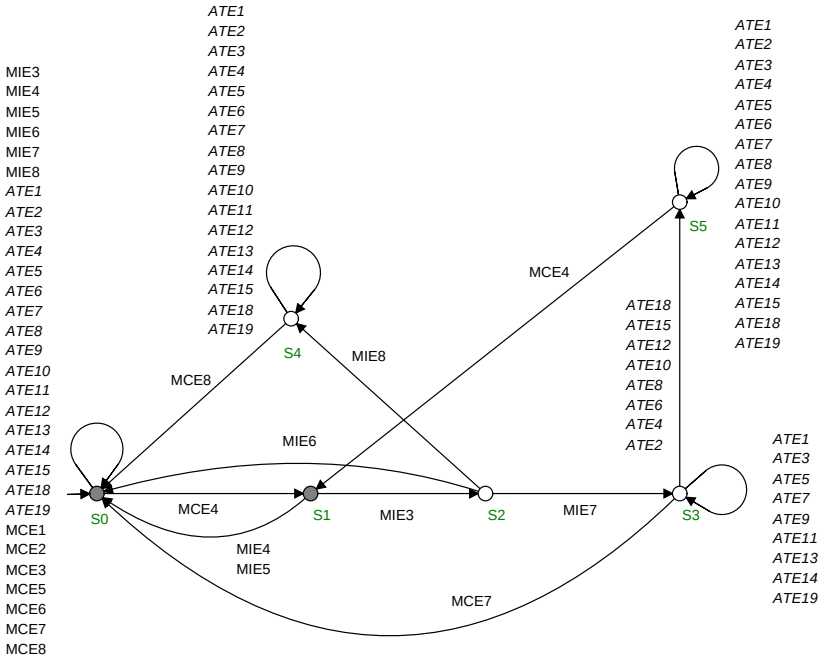

Fig. 3. Automaton model of *Specification 3*. *Specification 3* is triggered under the two successive conditions: i) the multicopter is in LOITER MODE (*MCE4* occurs); and ii) the remote pilot executes an arm action (*MIE3* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to RTL MODE (*MIE7* occurs), if the INS, GPS, barometer, compass, propulsors are all healthy (*ATE1*, *ATE3*, *ATE5*, *ATE7* and *ATE9* occur), the connection to the RC transmitter is normal (*ATE11* occurs), the battery's capacity is able to support the multicopter to return to the base (*ATE13* or *ATE14* occurs), and the multicopter's distance from the base is not less than a given threshold (*ATE19* occurs), then the multicopter enters RTL MODE (*MCE7* occurs); otherwise, the multicopter stays in LOITER MODE (*MCE4* occurs). Furthermore, when the remote pilot uses the flight mode switch to manually switch the multicopter to AL MODE (*MIE8* occurs), the multicopter enters AL MODE (*MCE8* occurs).

3) Specification 4: This control specification is obtained by partially transforming "safety requirement *SR2*" to an automaton model. As shown in Figure 4, *Specification 4* contains 9 states (S_0-S_8), 24 events and 54 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents LOITER MODE, and the state S_0 integrates other multicopter modes.

4) Specification 5: This control specification is obtained by partially transforming "safety requirements *SR7* and *SR8*" to an automaton model. As shown in Figure 5, *Specification 5* contains 6 states (S_0-S_5), 31 events and 91 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents LOITER MODE, and the state S_0 integrates other multicopter

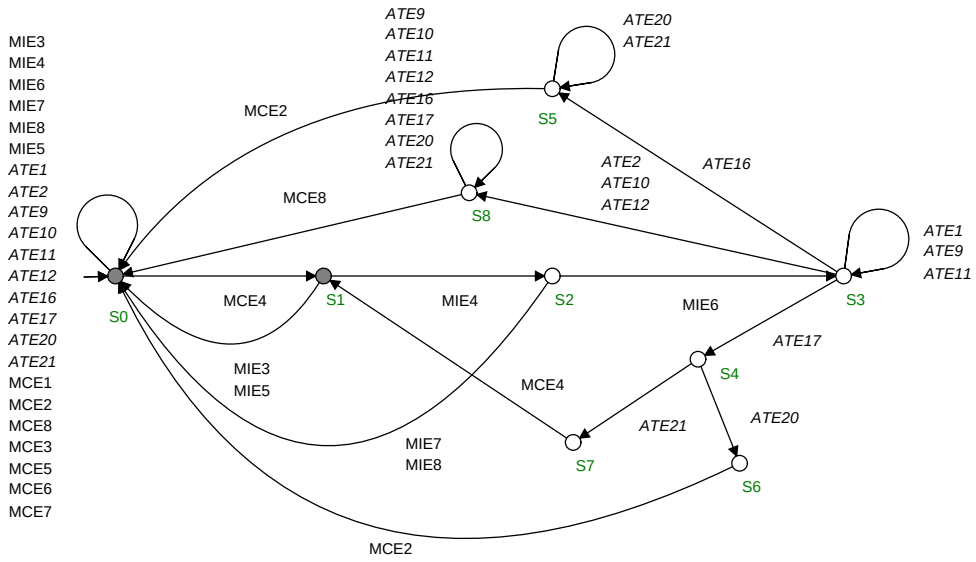

Fig. 4. Automaton model of *Specification 4*. *Specification 4* is triggered under the three successive conditions: i) the multicopter is in LOITER MODE (*MCE4* occurs); ii) the remote pilot executes a disarm action (*MIE4* occurs); and iii) the flight mode switch is on the position of "normal flight" (*MIE6* occurs). In this case, if the INS and propulsors are both healthy (*ATE1* and *ATE9* occur), the connection to RC transmitter is normal (*ATE11* occurs), and the multicopter's altitude is lower than a given threshold (*ATE16* occurs) or the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), then the multicopter is disarmed, and enters STANDBY MODE (*MCE2* occurs). Otherwise, if the multicopter's altitude is not lower than a given threshold (*ATE17* occurs), and the multicopter's throttle is not less than a given threshold over a time horizon (*ATE21* occurs), then the multicopter still stays in LOITER MODE (*MCE4* occurs); if one of the related component is unhealthy (*ATE2*, *ATE10* or *ATE12* occurs), the multicopter enters AL MODE (*MCE8* occurs).

modes.

5) Specification 6: This control specification is obtained by partially transforming "safety requirements *SR2-SR6*" to an automaton model. As shown in Figure 6, *Specification 6* contains 13 states (S_0-S_{12}), 33 events and 129 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents LOITER MODE, and the state S_0 integrates other multicopter modes.

6) Specification 7: This control specification is obtained by partially transforming "safety requirements *SR7* and *SR8*" to an automaton model. As shown in Figure 7, *Specification 7* contains 6 states (S_0-S_5), 31 events and 91 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents LOITER MODE, and the state S_0 integrates other multicopter modes.

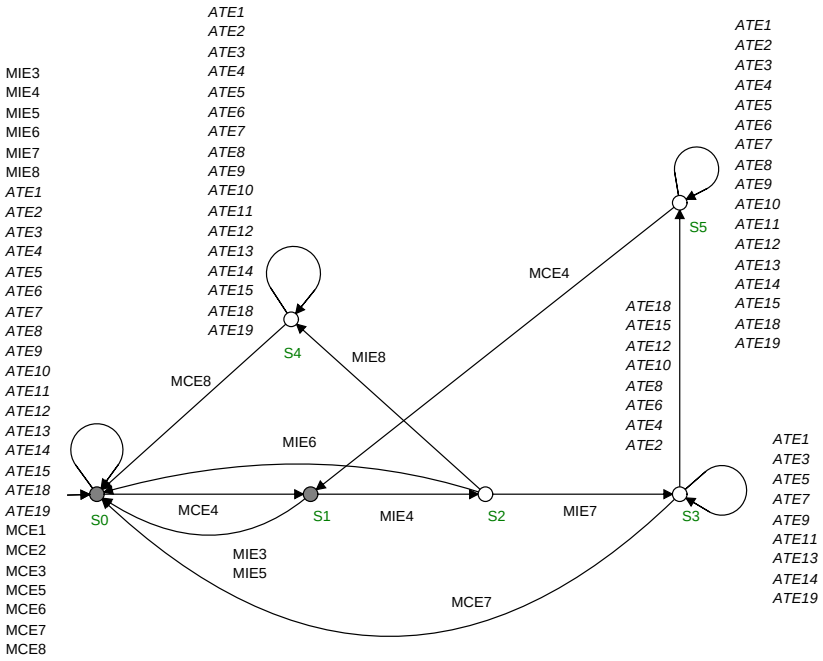

Fig. 5. Automaton model of *Specification 5*. *Specification 5* is triggered under the two successive conditions: i) the multicopter is in LOITER MODE (*MCE4* occurs); and ii) the remote pilot executes a disarm action (*MIE4* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to RTL MODE (*MIE7* occurs), if the INS, GPS, barometer, compass, propulsors are all healthy (*ATE1*, *ATE3*, *ATE5*, *ATE7* and *ATE9* occur), the connection to the RC transmitter is normal (*ATE11* occurs), the battery's capacity is able to support the multicopter to return to the base (*ATE13* or *ATE14* occurs), and the multicopter's distance from the base is not less than a given threshold (*ATE19* occurs), then the multicopter enters RTL MODE (*MCE7* occurs); otherwise, the multicopter stays in LOITER MODE (*MCE4* occurs). Furthermore, when the remote pilot uses the flight mode switch to manually switch the multicopter to AL MODE (*MIE8* occurs), the multicopter enters AL MODE (*MCE8* occurs).

7) Specification 8: This control specification is obtained by partially transforming "safety requirements *SR2-SR6*" to an automaton model. As shown in Figure 8, *Specification 8* contains 11 states (S_0-S_{10}), 33 events and 121 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents ALTITUDE-HOLD MODE, and the state S_0 integrates other multicopter modes.

8) Specification 9: This control specification is obtained by partially transforming "safety requirements *SR7* and *SR8*" to an automaton model. As shown in Figure 9, *Specification 9* contains 5 states (S_0-S_4), 14 events and 22 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents ALTITUDE-HOLD MODE, and the state S_0 integrates other multicopter modes.

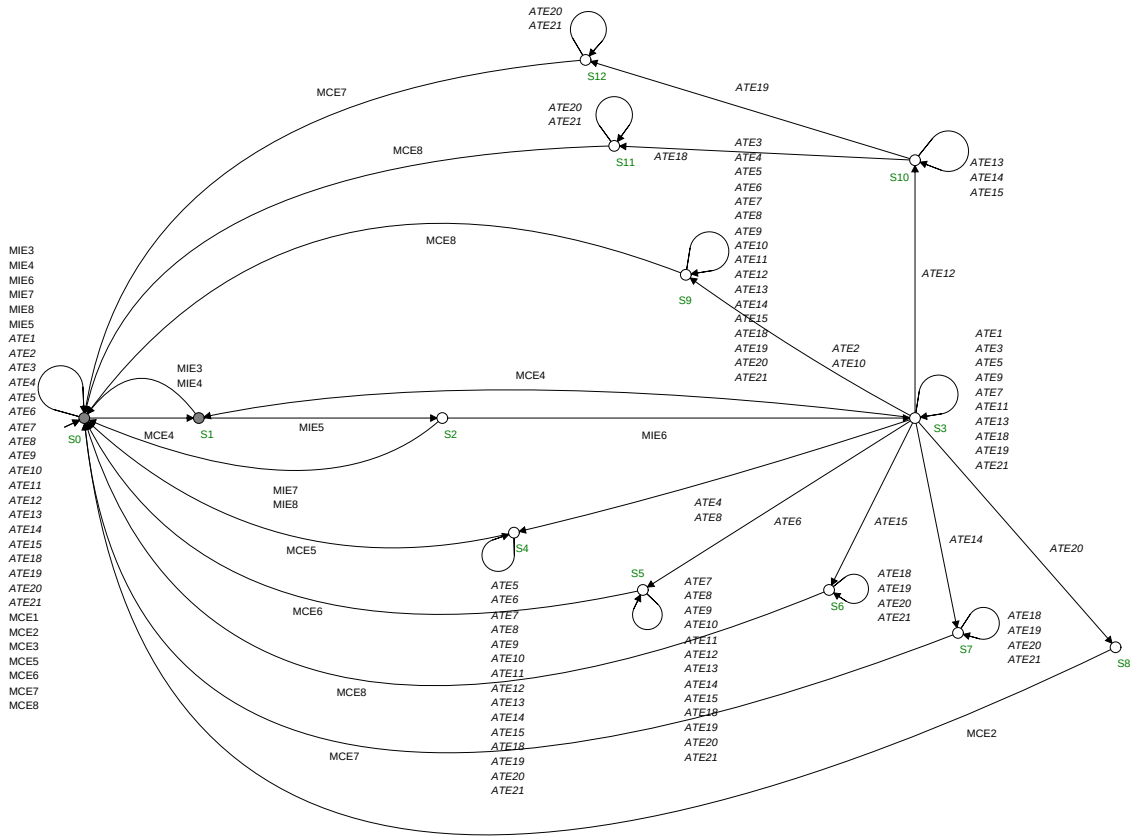

Fig. 6. Automaton model of *Specification 6*. *Specification 6* is triggered under the three successive conditions: i) the multicopter is in LOITER MODE (*MCE4* occurs); ii) the remote pilot normally manipulates the sticks of the RC transmitter (*MIE5* occurs); and iii) the flight mode switch is on the position of "normal flight" (*MIE6* occurs). In this case, if the GPS or compass is unhealthy (*ATE4* or *ATE8* occurs), the multicopter enters ALTITUDE-HOLD MODE (*MCE5* occurs); if the barometer is unhealthy (*ATE6* occurs), the multicopter enters STABILIZE MODE (*MCE6* occurs); if the INS or propulsors are unhealthy (*ATE2* or *ATE10* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the connection to the RC transmitter is abnormal (*ATE12* occurs), and the multicopter's distance from the base is less than a given threshold (*ATE18* occurs), then the multicopter enters AL MODE (*MCE8* occurs); if the connection to the RC transmitter is abnormal (*ATE12* occurs), and the multicopter's distance from the base is not less than a given threshold (*ATE19* occurs), then the multicopter enters RTL MODE (*MCE7* occurs); if the battery's capacity is inadequate but the multicopter is able to perform RTL (*ATE14* occurs), the multicopter enters RTL MODE (*MCE7* occurs); if the battery's capacity is inadequate and the multicopter is unable to perform RTL (*ATE15* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), the multicopter enters STANDBY MODE (*MCE2* occurs); otherwise, the multicopter stays in LOITER MODE (*MCE4* occurs).

9) Specification 10: This control specification is obtained by partially transforming "safety requirement *SR2*" to an automaton model. As shown in Figure 10, *Specification 10* contains 9 states (S_0-S_8), 24 events and 54 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents ALTITUDE-HOLD MODE, and the state S_0 integrates other multicopter

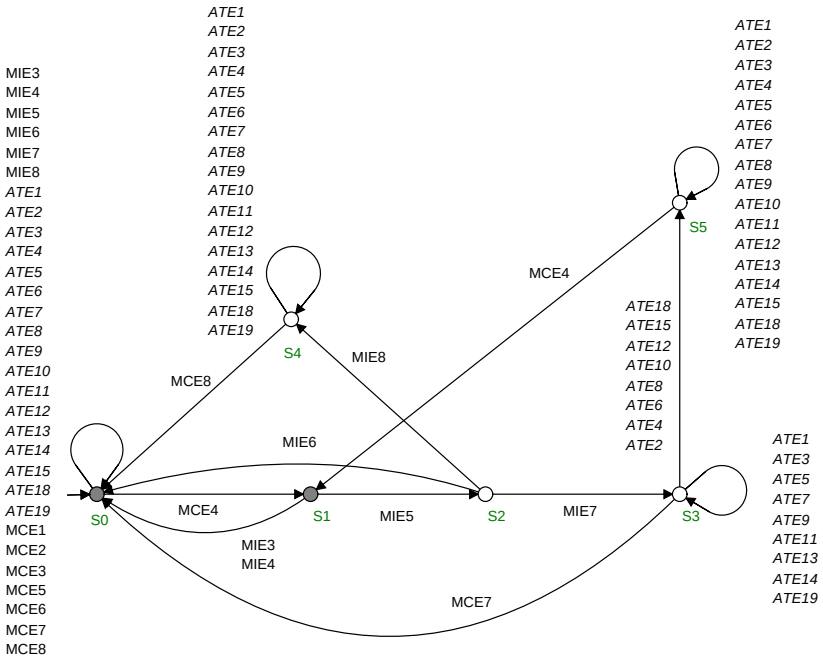

Fig. 7. Automaton model of *Specification 7*. *Specification 7* is triggered under the two successive conditions: i) the multicopter is in LOITER MODE (*MCE4* occurs); and ii) the remote pilot normally manipulates the sticks of the RC transmitter (*MIE5* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to RTL MODE (*MIE7* occurs), if the INS, GPS, barometer, compass, propulsors are all healthy (*ATE1*, *ATE3*, *ATE5*, *ATE7* and *ATE9* occur), the connection to the RC transmitter is normal (*ATE11* occurs), the battery's capacity is able to support the multicopter to return to the base (*ATE13* or *ATE14* occurs), and the multicopter's distance from the base is not less than a given threshold (*ATE19* occurs), then the multicopter enters RTL MODE (*MCE7* occurs); otherwise, the multicopter stays in LOITER MODE (*MCE4* occurs). Furthermore, when the remote pilot uses the flight mode switch to manually switch the multicopter to AL MODE (*MIE8* occurs), the multicopter enters AL MODE (*MCE8* occurs).

modes.

10) Specification 11: This control specification is obtained by partially transforming "safety requirements *SR7* and *SR8*" to an automaton model. As shown in Figure 11, *Specification 11* contains 5 states (S_0-S_4), 14 events and 22 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents ALTITUDE-HOLD MODE, and the state S_0 integrates other multicopter modes.

11) Specification 12: This control specification is obtained by partially transforming "safety requirements *SR2*-*SR6*" to an automaton model. As shown in Figure 12, *Specification 12* contains 11 states (S_0-S_{10}), 33 events and 121 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents ALTITUDE-HOLD MODE, and the state S_0 integrates other multicopter modes.

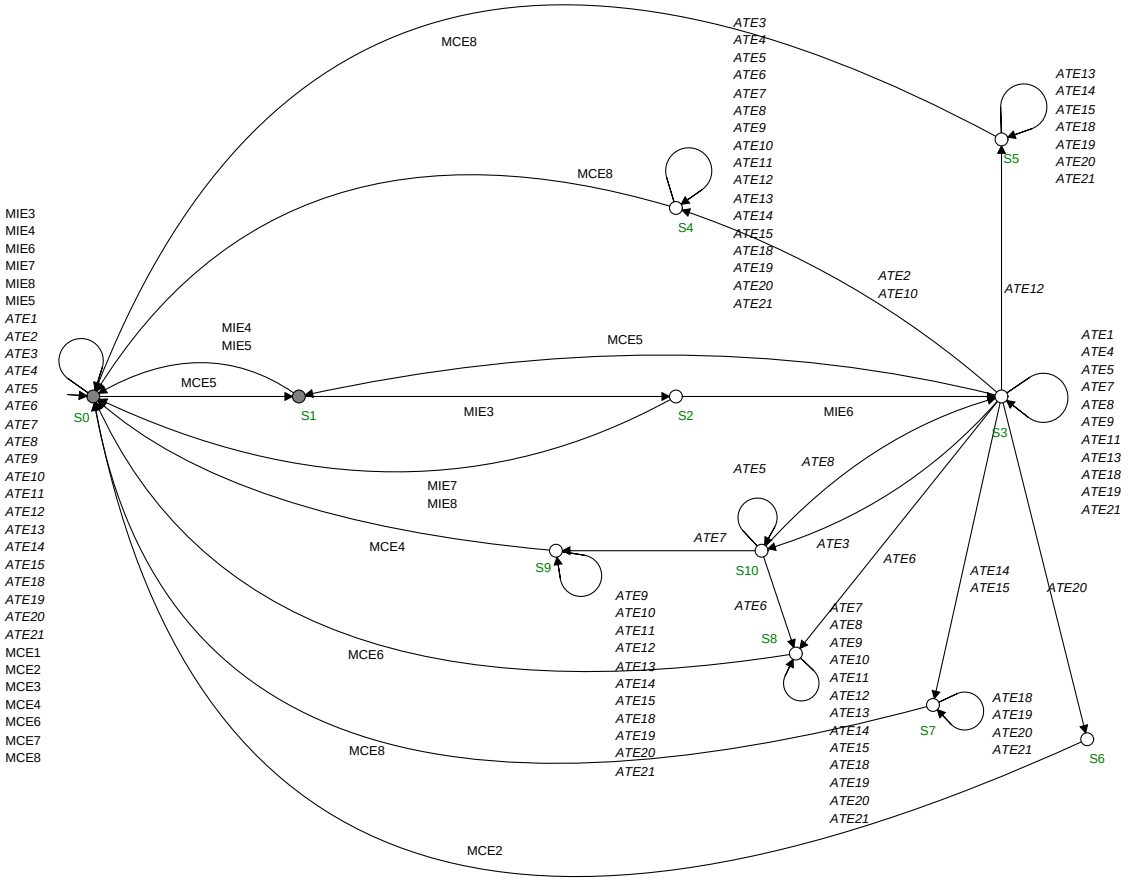

Fig. 8. Automaton model of *Specification 8*. *Specification 8* is triggered under the three successive conditions: i) the multicopter is in ALTITUDE-HOLD MODE (*MCE5* occurs); ii) the remote pilot executes an arm action (*MIE3* occurs); and iii) the flight mode switch is on the position of "normal flight" (*MIE6* occurs). In this case, if the GPS and compass are both healthy (*ATE3* and *ATE7* occur), the multicopter enters LOITER MODE (*MCE4* occurs); if the barometer is unhealthy (*ATE6* occurs), the multicopter enters STABILIZE MODE (*MCE6* occurs); if the INS or propulsors are unhealthy (*ATE2* or *ATE10* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the connection to the RC transmitter is abnormal (*ATE12* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the battery's capacity is inadequate (*ATE14* or *ATE15* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), the multicopter enters STANDBY MODE (*MCE2* occurs); otherwise, the multicopter stays in ALTITUDE-HOLD MODE (*MCE5* occurs).

12) Specification 13: This control specification is obtained by partially transforming "safety requirements *SR7* and *SR8*" to an automaton model. As shown in Figure 13, *Specification 13* contains 5 states (S_0-S_4), 14 events and 22 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents ALTITUDE-HOLD MODE, and the state S_0 integrates other multicopter modes.

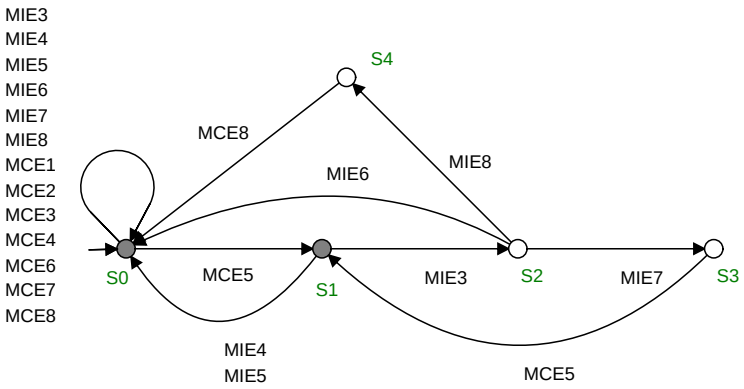

Fig. 9. Automaton model of *Specification 9*. *Specification 9* is triggered under the two successive conditions: i) the multicopter is in ALTITUDE-HOLD MODE (*MCE5* occurs); and ii) the remote pilot executes an arm action (*MIE3* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to RTL MODE (*MIE7* occurs), the multicopter still stays in ALTITUDE-HOLD MODE (*MCE5* occurs); when the remote pilot uses the flight mode switch to manually switch the multicopter to AL MODE (*MIE8* occurs), the multicopter enters AL MODE (*MCE8* occurs).

13) Specification 14: This control specification is obtained by partially transforming "safety requirements *SR2-SR6*" to an automaton model. As shown in Figure 14, *Specification 14* contains 12 states (S_0-S_{11}), 33 events and 123 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents STABILIZE MODE, and the state S_0 integrates other multicopter modes.

14) Specification 15: This control specification is obtained by partially partially transforming "safety requirements *SR7* and *SR8*" to an automaton model. As shown in Figure 15, *Specification 15* contains 5 states (S_0-S_4), 14 events and 22 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents STABILIZE MODE, and the state S_0 integrates other multicopter modes.

15) Specification 16: This control specification is obtained by partially transforming "safety requirement *SR2*" to an automaton model. As shown in Figure 16, *Specification 16* contains 9 states (S_0-S_8), 24 events and 54 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents STABILIZE MODE, and the state S_0 integrates other multicopter modes.

16) Specification 17: This control specification is obtained by partially transforming "safety requirements *SR7* and *SR8*" to an automaton model. As shown in Figure 17, *Specification 17* contains 5 states (S_0-S_4), 14 events and 22 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents STABILIZE MODE, and the state S_0 integrates other multi-

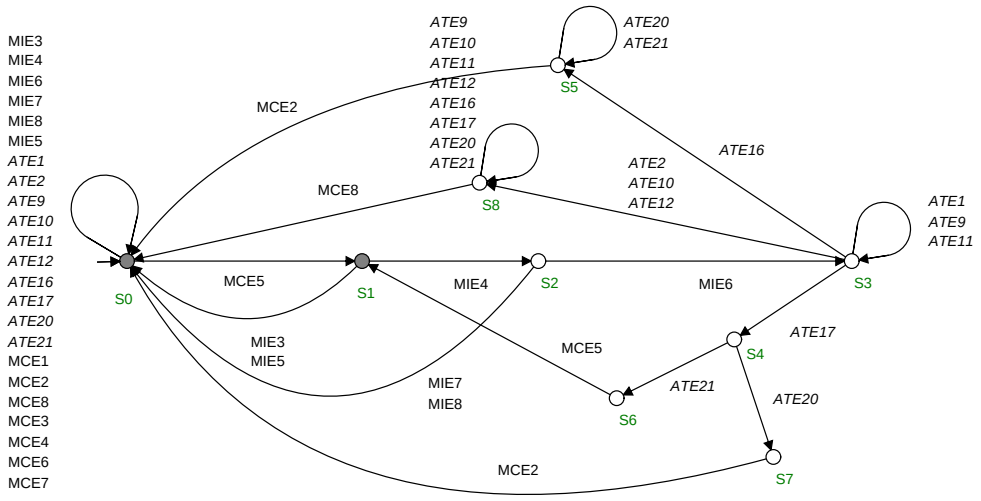

Fig. 10. Automaton model of *Specification 10*. *Specification 10* is triggered under the three successive conditions: i) the multicopter is in ALTITUDE-HOLD MODE (*MCE5* occurs); ii) the remote pilot executes a disarm action (*MIE4* occurs); and iii) the flight mode switch is on the position of "normal flight" (*MIE6* occurs). In this case, if the INS and propulsors are both healthy (*ATE1* and *ATE9* occur), the connection to RC transmitter is normal (*ATE11* occurs), and the multicopter's altitude is lower than a given threshold (*ATE16* occurs) or the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), then the multicopter is disarmed, and enters STANDBY MODE (*MCE2* occurs). Otherwise, if the multicopter's altitude is not lower than a given threshold (*ATE17* occurs), and the multicopter's throttle is not less than a given threshold over a time horizon (*ATE21* occurs), then the multicopter still stays in ALTITUDE-HOLD MODE(*MCE5* occurs); if one of the related equipment is unhealthy (*ATE2*, *ATE10* or *ATE12* occurs), the multicopter enters AL MODE (*MCE8* occurs).

copter modes.

17) Specification 18: This control specification is obtained by partially transforming "safety requirements *SR2-SR6*" to an automaton model. As shown in Figure 18, *Specification 18* contains 12 states (S_0-S_{11}), 33 events and 123 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents STABILIZE MODE, and the state S_0 integrates other multicopter modes.

18) Specification 19: This control specification is obtained by partially transforming "safety requirements *SR7* and *SR8*" to an automaton model. As shown in Figure 19, *Specification 19* contains 5 states (S_0-S_4), 14 events and 22 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents STABILIZE MODE, and the state S_0 integrates other multicopter modes.

19) Specification 20: This control specification is obtained by partially transforming "safety requirement *SR9*" to an automaton model. As shown in Figure 20, *Specification 20* contains

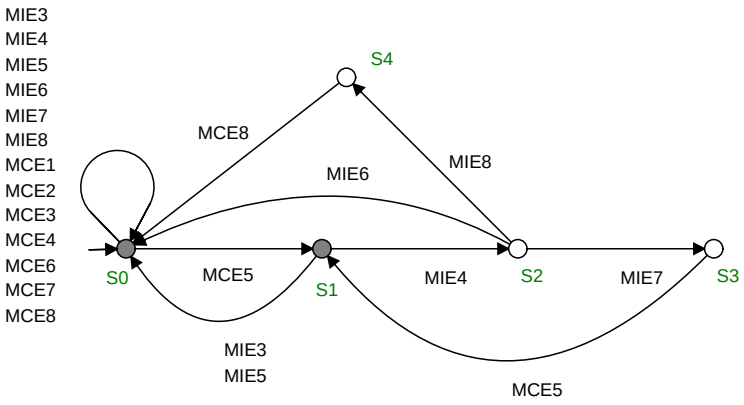

Fig. 11. Automaton model of *Specification 11*. *Specification 11* is triggered under the two successive conditions: i) the multicopter is in ALTITUDE-HOLD MODE (*MCE5* occurs); and ii) the remote pilot executes a disarm action (*MIE4* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to RTL MODE (*MIE7* occurs), the multicopter still stays in ALTITUDE-HOLD MODE (*MCE5* occurs); when the remote pilot uses the flight mode switch to manually switch the multicopter to AL MODE (*MIE8* occurs), the multicopter enters AL MODE (*MCE8* occurs).

4 states (S_0-S_3), 20 events, 41 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents RTL MODE, and the state S_0 integrates other multicopter modes.

20) Specification 21: This control specification is obtained by transforming "safety requirement *SR10*" to an automaton model. As shown in Figure 21, *Specification 21* contains 4 states (S_0-S_3), 26 events and 59 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents RTL MODE, and the state S_0 integrates other multicopter modes.

21) Specification 22: This control specification is obtained by partially transforming "safety requirement *SR9*" to an automaton model. As shown in Figure 22, *Specification 22* contains 3 states (S_0-S_2), 11 events, 15 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents RTL MODE, and the state S_0 integrates other multicopter modes.

22) Specification 23: This control specification is obtained by transforming "safety requirement *SR11*" to an automaton model. As shown in Figure 23, *Specification 23* contains 4 states (S_0-S_3), 28 events and 65 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents AL MODE, and the state S_0 integrates other multicopter modes.

23) Specification 24: This control specification is obtained by transforming "safety requirement *SR12*" to an automaton model. As shown in Figure 24, *Specification 24* contains 4 states (S_0-S_3), 28 events and 65 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents AL MODE, and the state S_0 integrates other multicopter modes.

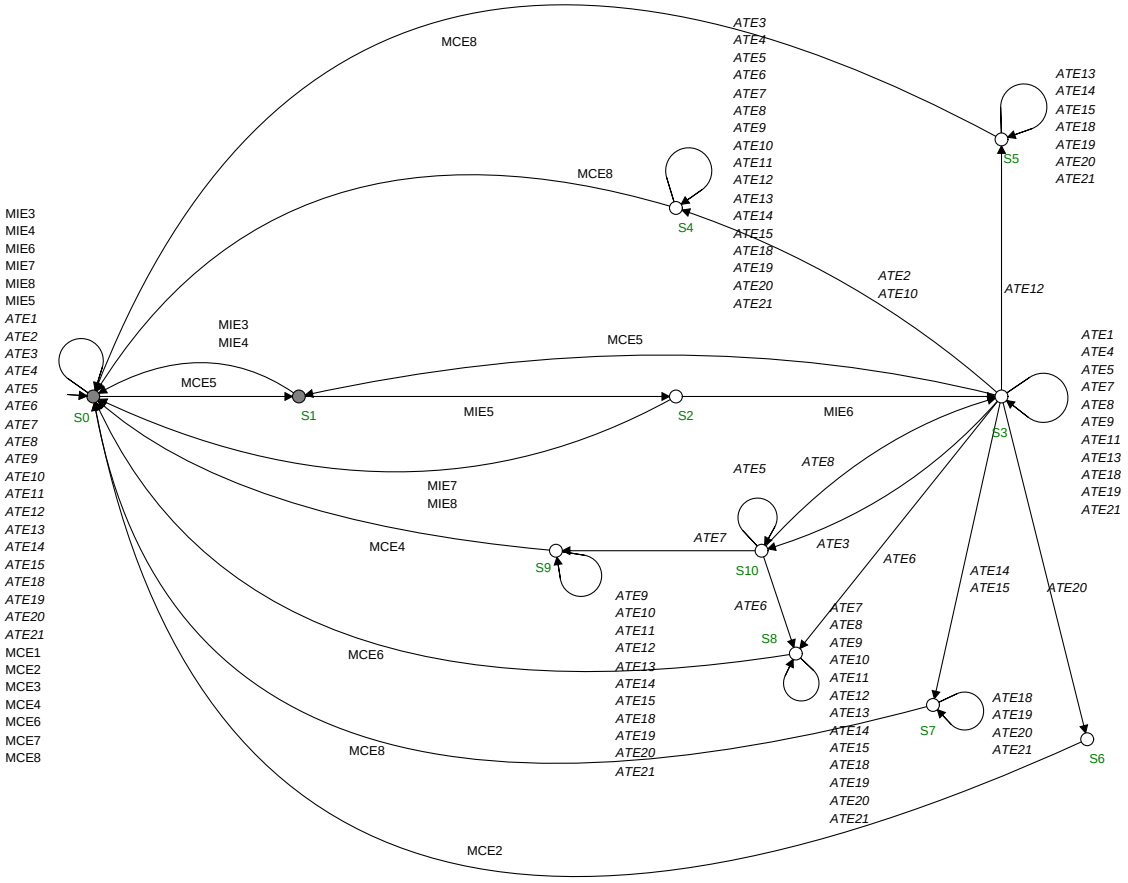

Fig. 12. Automaton model of *Specification 12*. *Specification 12* is triggered under the three successive conditions: i) the multicopter is in ALTITUDE-HOLD MODE (*MCE5* occurs); ii) the remote pilot normally manipulates the sticks of the RC transmitter (*MIE5* occurs); and iii) the flight mode switch is on the position of "normal flight" (*MIE6* occurs). In this case, if the GPS and compass are both healthy (*ATE3* and *ATE7* occur), the multicopter enters LOITER MODE (*MCE4* occurs); if the barometer is unhealthy (*ATE6* occurs), the multicopter enters STABILIZE MODE (*MCE6* occurs); if the INS or propulsors are unhealthy (*ATE2* or *ATE10* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the connection to the RC transmitter is abnormal (*ATE12* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the battery's capacity is inadequate (*ATE14* or *ATE15* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), the multicopter enters STANDBY MODE (*MCE2* occurs); otherwise, the multicopter stays in ALTITUDE-HOLD MODE (*MCE5* occurs).

24) Specification 25: This control specification is obtained by transforming "safety requirement *SR13*" to an automaton model. As shown in Figure 25, *Specification 25* contains 8 states (S_0-S_7), 21 events and 52 transitions. Here, the states S_0,S_1 are marker states. The state S_1 represents AL MODE, and the state S_0 integrates other multicopter modes.

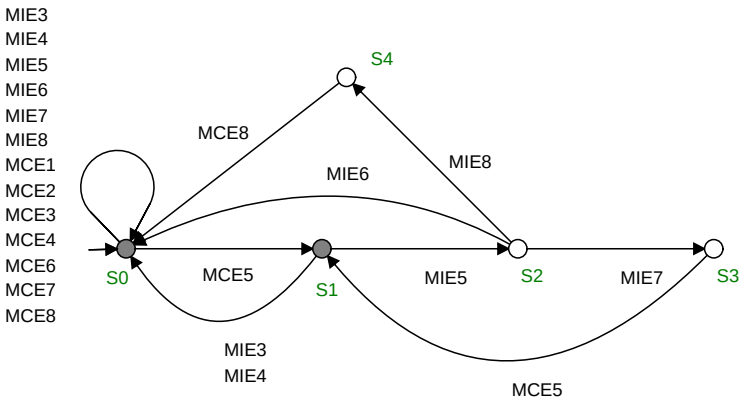

Fig. 13. Automaton model of *Specification 13*. *Specification 13* is triggered under the two successive conditions: i) the multicopter is in ALTITUDE-HOLD MODE (*MCE5* occurs); and ii) the remote pilot normally manipulates the sticks of the RC transmitter (*MIE5* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to RTL MODE (*MIE7* occurs), the multicopter still stays in ALTITUDE-HOLD MODE (*MCE5* occurs); when the remote pilot uses the flight mode switch to manually switch the multicopter to AL MODE (*MIE8* occurs), the multicopter enters AL MODE (*MCE8* occurs).

B. Input of the plant and control specifications to TCT software

An instruction "**create**" is used to input the plant and control specifications into *TCT* software. *TCT* software uses odd numbers to denote the controllable events and even numbers for the uncontrollable events. Thus, all the multicopter events are labeled as shown in Table 2 and Table 3.

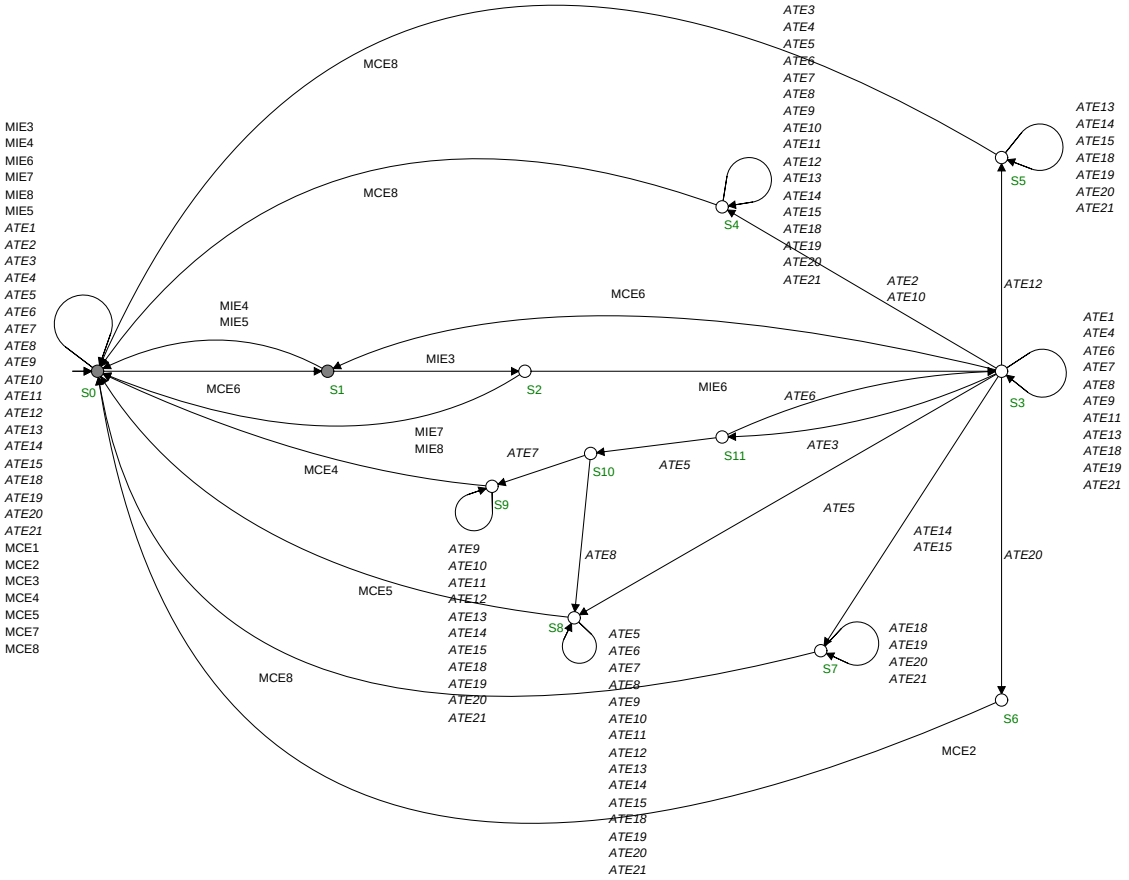

Fig. 14. Automaton model of *Specification 14*. *Specification 14* is triggered under the three successive conditions: i) the multicopter is in STABILIZE MODE (*MCE6* occurs); ii) the remote pilot executes an arm action (*MIE3* occurs); and iii) the flight mode switch is on the position of "normal flight" (*MIE6* occurs). In this case, if the GPS, barometer and compass are all healthy (*ATE3*, *ATE5* and *ATE7* occur), the multicopter enters LOITER MODE (*MCE4* occurs); if the barometer is healthy (*ATE5* occurs), but the GPS or compass is unhealthy (*ATE4* or *ATE8* occurs), then the multicopter enters ALTITUDE-HOLD MODE (*MCE5* occurs); if the INS or propulsors are unhealthy (*ATE2* or *ATE10* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the connection to the RC transmitter is abnormal (*ATE12* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the battery's capacity is inadequate (*ATE14* or *ATE15* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), the multicopter enters STANDBY MODE (*MCE2* occurs); otherwise, the multicopter stays in STABILIZE MODE (*MCE6* occurs).

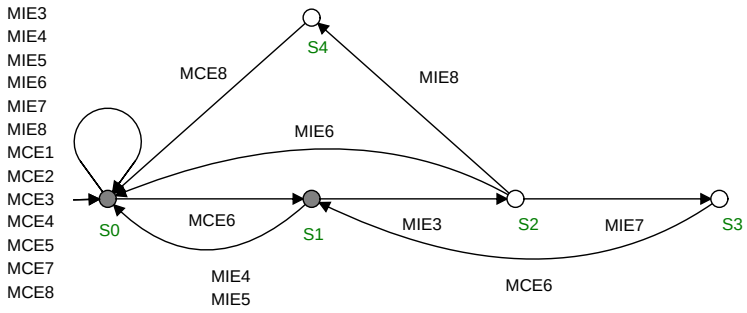

Fig. 15. Automaton model of *Specification 15*. *Specification 15* is triggered under the two successive conditions: i) the multicopter is in STABILIZE MODE (*MCE6* occurs); and ii) the remote pilot executes an arm action (*MIE3* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to RTL MODE (*MIE7* occurs), the multicopter still stays in STABILIZE MODE (*MCE6* occurs); when the remote pilot uses the flight mode switch to manually switch the multicopter to AL MODE (*MIE8* occurs), the multicopter enters AL MODE (*MCE8* occurs).

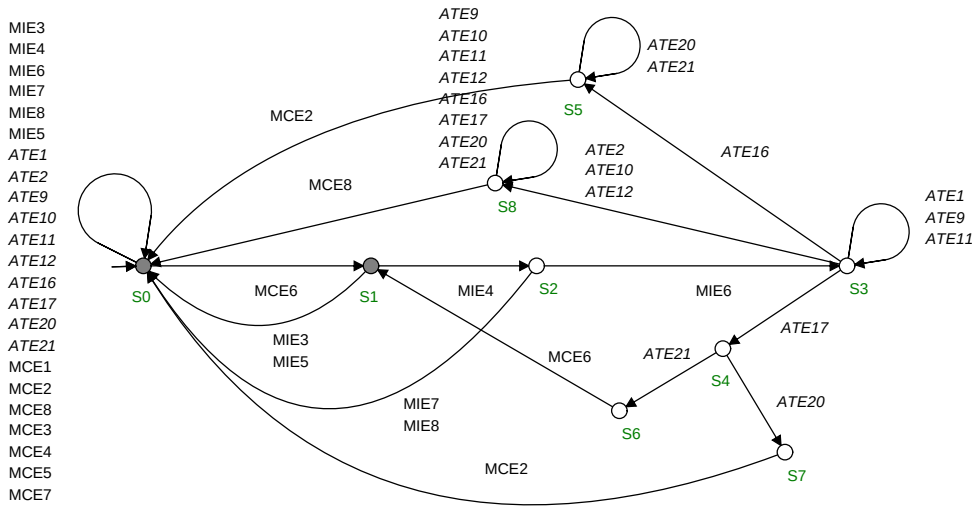

Fig. 16. Automaton model of *Specification 16*. *Specification 16* is triggered under the three successive conditions: i) the multicopter is in STABILIZE MODE (*MCE6* occurs); ii) the remote pilot executes a disarm action (*MIE4* occurs); and iii) the flight mode switch is on the position of "normal flight" (*MIE6* occurs). In this case, if the INS and propulsors are both healthy (*ATE1* and *ATE9* occur), the connection to RC transmitter is normal (*ATE11* occurs), and the multicopter's altitude is lower than a given threshold (*ATE16* occurs) or the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), then the multicopter is disarmed, and enters STANDBY MODE (*MCE2* occurs). Otherwise, if the multicopter's altitude is not lower than a given threshold (*ATE17* occurs), and the multicopter's throttle is not less than a given threshold over a time horizon (*ATE21* occurs), then the multicopter still stays in STABILIZE MODE (*MCE6* occurs); if one of the related equipment is unhealthy (*ATE2*, *ATE10* or *ATE12* occurs), the multicopter enters AL MODE (*MCE8* occurs).

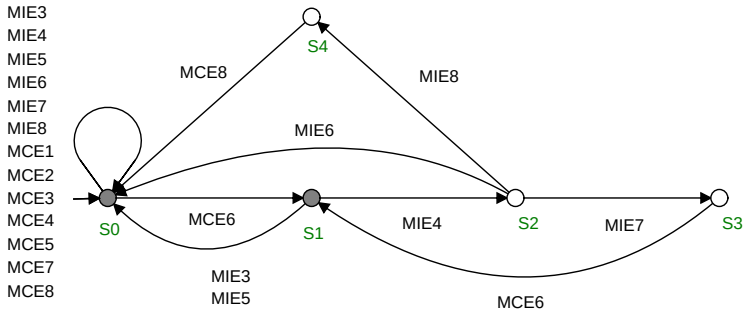

Fig. 17. Automaton model of *Specification 17*. *Specification 17* is triggered under the two successive conditions: i) the multicopter is in STABILIZE MODE (*MCE6* occurs); and ii) the remote pilot executes a disarm action (*MIE4* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to RTL MODE (*MIE7* occurs), the multicopter still stays in STABILIZE MODE (*MCE6* occurs); when the remote pilot uses the flight mode switch to manually switch the multicopter to AL MODE (*MIE8* occurs), the multicopter enters AL MODE (*MCE8* occurs).

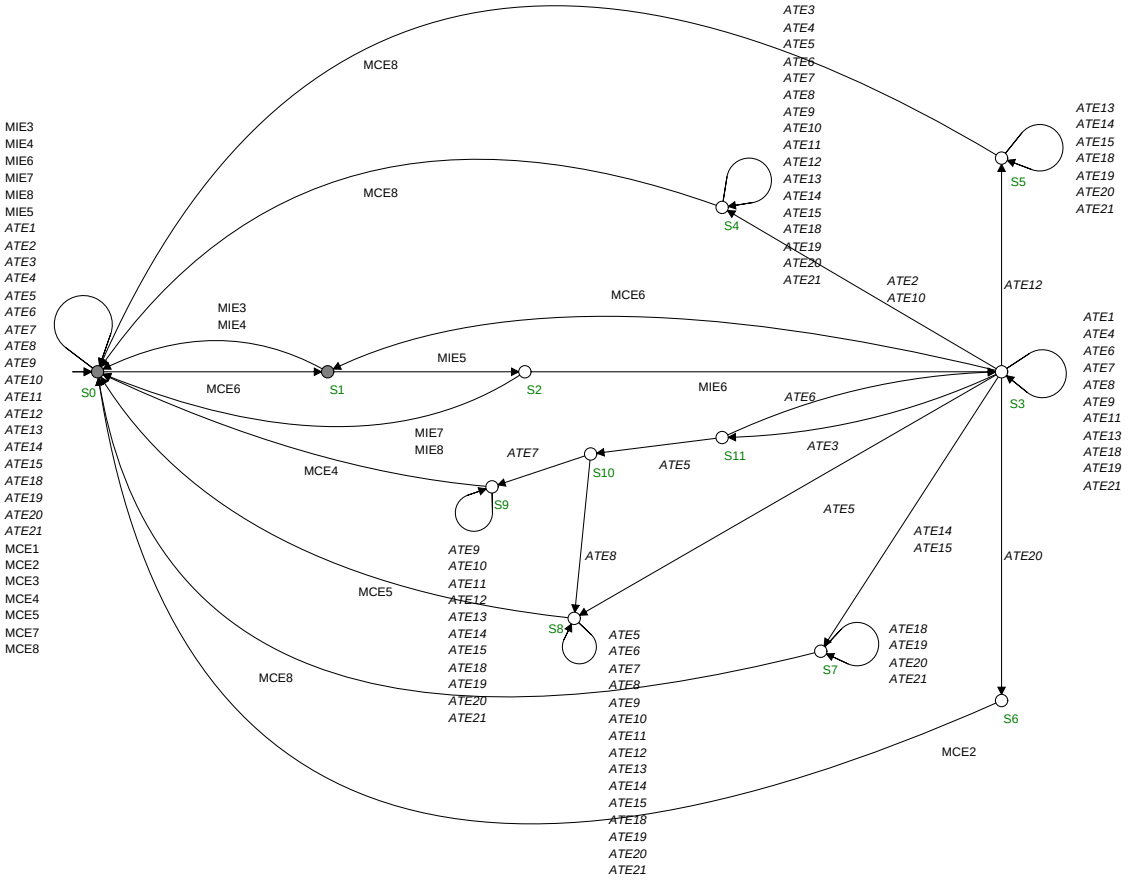

Fig. 18. Automaton model of *Specification 18*. *Specification 18* is triggered under the three successive conditions: i) the multicopter is in STABILIZE MODE (*MCE6* occurs); ii) the remote pilot normally manipulates the sticks of the RC transmitter (*MIE5* occurs); and iii) the flight mode switch is on the position of "normal flight" (*MIE6* occurs). In this case, if the GPS, barometer and compass are all healthy (*ATE3*, *ATE5* and *ATE7* occur), the multicopter enters LOITER MODE (*MCE4* occurs); if the barometer is healthy (*ATE5* occurs), but the GPS or compass is unhealthy (*ATE4* or *ATE8* occurs), then the multicopter enters ALTITUDE-HOLD MODE (*MCE5* occurs); if the INS or propulsors are unhealthy (*ATE2* or *ATE10* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the connection to the RC transmitter is abnormal (*ATE12* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the battery's capacity is inadequate (*ATE14* or *ATE15* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), the multicopter enters STANDBY MODE (*MCE2* occurs); otherwise, the multicopter stays in STABILIZE MODE (*MCE6* occurs).

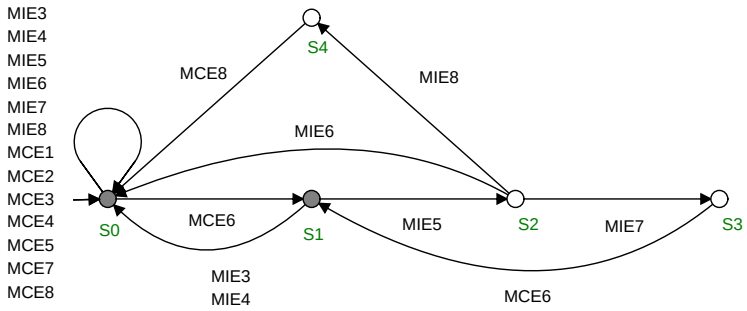

Fig. 19. Automaton model of *Specification 19*. *Specification 19* is triggered under the two successive conditions: i) the multicopter is in STABILIZE MODE (*MCE6* occurs); and ii) the remote pilot normally manipulates the sticks of the RC transmitter (*MIE5* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to RTL MODE (*MIE7* occurs), the multicopter still stays in STABILIZE MODE (*MCE6* occurs); when the remote pilot uses the flight mode switch to manually switch the multicopter to AL MODE (*MIE8* occurs), the multicopter enters AL MODE (*MCE8* occurs).

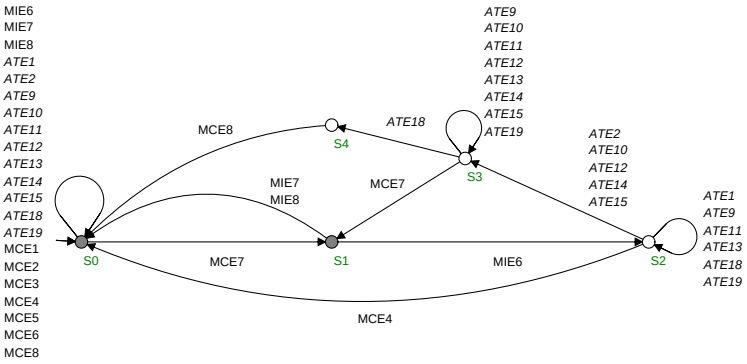

Fig. 20. Automaton model of *Specification 20*. *Specification 20* is triggered when the multicopter is in RTL MODE (*MCE7* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to "normal flight", or the flight mode switch is on the position of "normal flight" (*MIE6* occurs), if the INS and propulsors are both healthy (*ATE1* and *ATE9* occur), the connection to RC transmitter is normal (*ATE11* occurs), and the battery's capacity is adequate (*ATE13* occurs), then the multicopter enters LOITER MODE (*MCE4* occurs). Otherwise, if the multicopter's distance from the base is less than a given threshold (*ATE18* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the multicopter's distance from the base is not less than a given threshold (*ATE19* occurs), then the multicopter stays in RTL MODE (*MCE7* occurs).

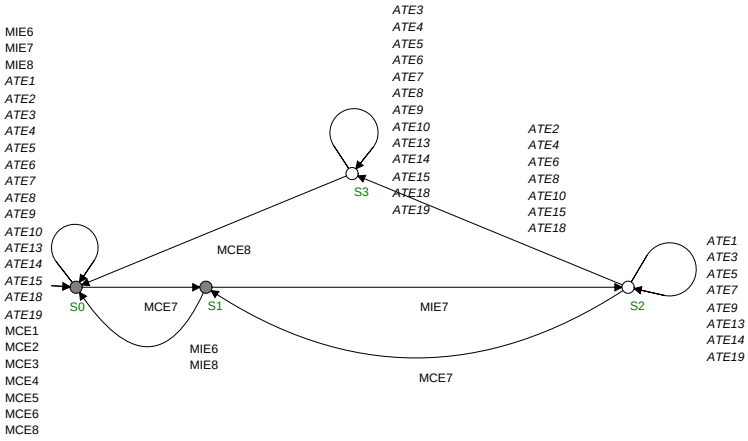

Fig. 21. Automaton model of *Specification 21*. *Specification 21* is triggered under the two successive conditions: i) the multicopter is in RTL MODE (*MCE7* occurs); and ii) the flight mode switch is on the position of "RTL MODE" (*MIE7* occurs). In this case, if the INS, GPS, barometer, compass or propulsors are unhealthy (*ATE2*, *ATE4*, *ATE6*, *ATE8* or *ATE10* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the battery's capacity is inadequate, and the multicopter is unable to perform RTL (*ATE15* occurs), the multicopter enters AL MODE (*MCE8* occurs); if the multicopter's distance from the base is less than a given threshold (*ATE18* occurs), the multicopter enters AL MODE (*MCE8* occurs); otherwise, the multicopter stays in RTL MODE (*MCE7* occurs).

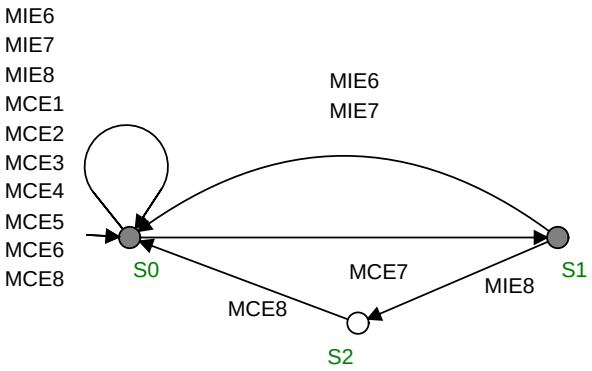

Fig. 22. Automaton model of *Specification 22*. *Specification 22* is triggered when the multicopter is in RTL MODE (*MCE7* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to AL MODE (*MIE8* occurs), the multicopter enters AL MODE (*MCE8* occurs).

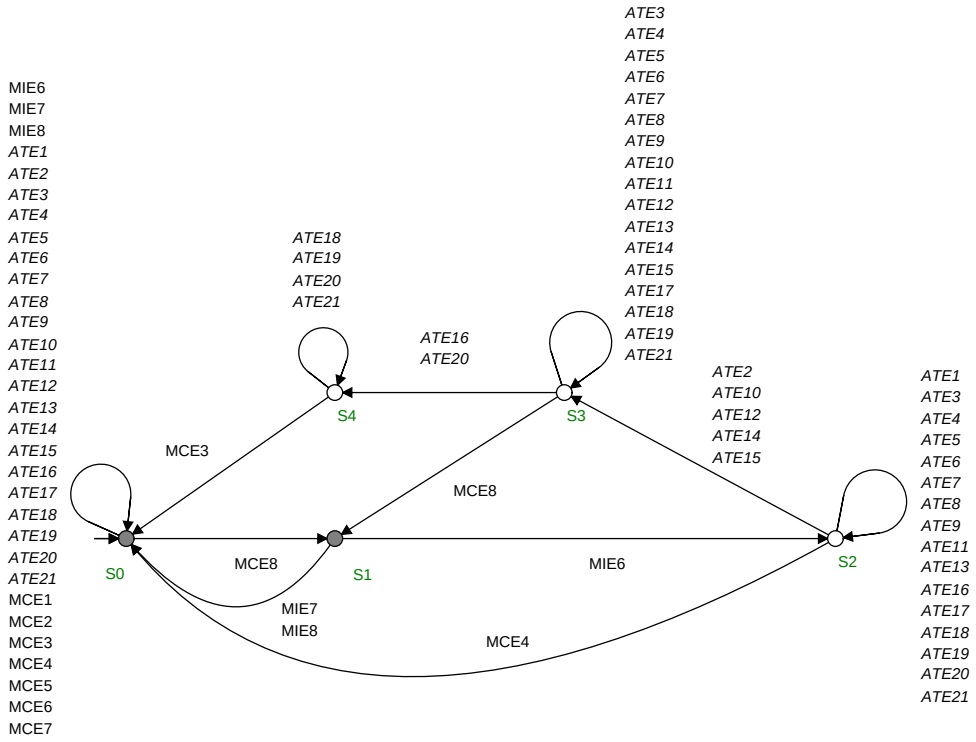

Fig. 23. Automaton model of *Specification 23*. *Specification 23* is triggered when the multicopter is in AL MODE (*MCE8* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to "normal flight", or the flight mode switch is on the position of "normal flight" (*MIE6* occurs), if the INS and propulsors are both healthy (*ATE1* and *ATE9* occur), the connection to RC transmitter is normal (*ATE11* occurs), and the battery's capacity is adequate (*ATE13* occurs), then the multicopter enters LOITER MODE (*MCE4* occurs); Otherwise, if the multicopter's altitude is not lower than a given threshold (*ATE16* occurs), or the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), the multicopter enters GROUND-ERROR MODE (*MCE3* occurs); if the multicopter's altitude is not lower than a given threshold (*ATE17* occurs), and the multicopter's throttle is not less than a given threshold over a time horizon (*ATE21* occurs), the multicopter stays in AL MODE (*MCE8* occurs).

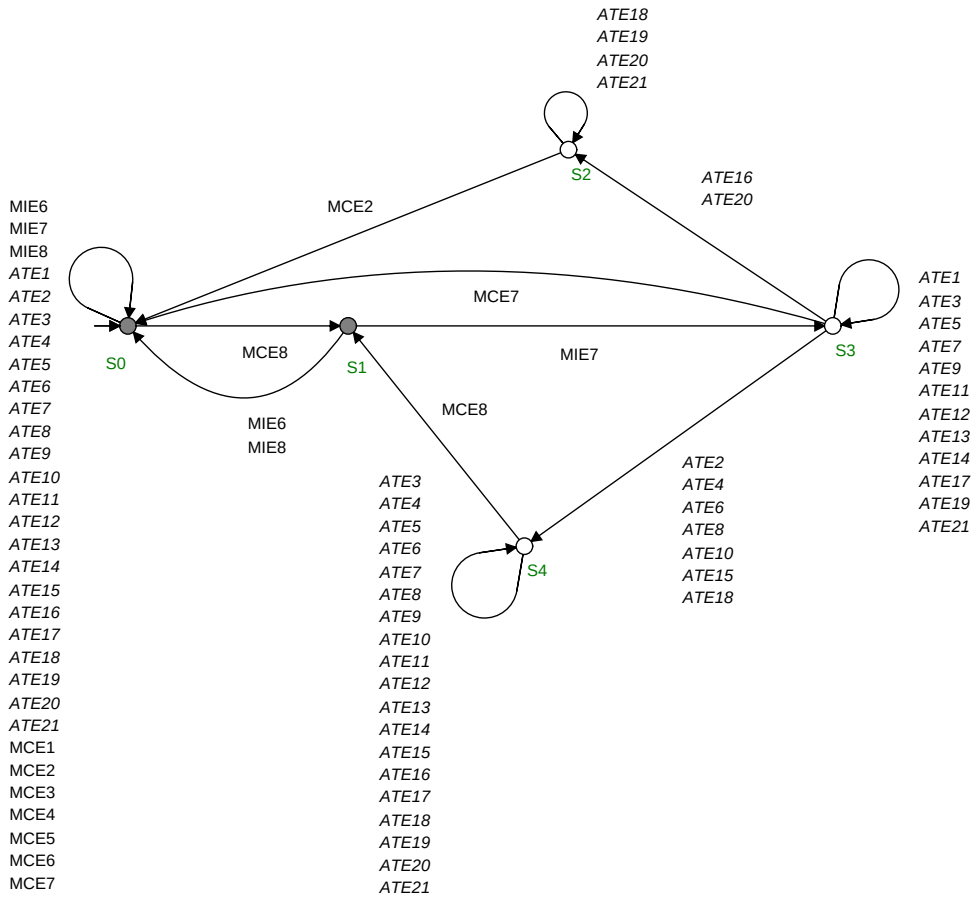

Fig. 24. Automaton model of *Specification 24*. *Specification 24* is triggered when the multicopter is in AL MODE (*MCE8* occurs). In this case, when the remote pilot uses the flight mode switch to manually switch the multicopter to RTL MODE, or the flight mode switch is on the position of "RTL MODE" (*MIE7* occurs), if the INS, GPS, barometer, compass, propulsors are all healthy (*ATE1*, *ATE3*, *ATE5*, *ATE7* and *ATE9* occur), the connection to the RC transmitter is normal (*ATE11* occurs), the battery's capacity is able to support the multicopter to return to the base (*ATE13* or *ATE14* occurs), the multicopter's distance from the base is not less than a given threshold (*ATE19* occurs), the multicopter's altitude is not lower than a given threshold (*ATE17* occurs), and the multicopter's throttle is not less than a given threshold over a time horizon (*ATE21* occurs), then the multicopter enters RTL MODE (*MCE7* occurs). Otherwise, if the multicopter's altitude is not lower than a given threshold (*ATE16* occurs), or the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), the multicopter enters STANDBY MODE (*MCE2* occurs); if if the INS, GPS, barometer, compass or propulsors are unhealthy (*ATE2*, *ATE4*, *ATE6*, *ATE8* or *ATE10* occurs), the battery's capacity is inadequate and the multicopter is unable to perform RTL (*ATE15* occurs), or the multicopter's distance from the base is less than a given threshold (*ATE18* occurs), then the multicopter stays in AL MODE (*MCE8* occurs).

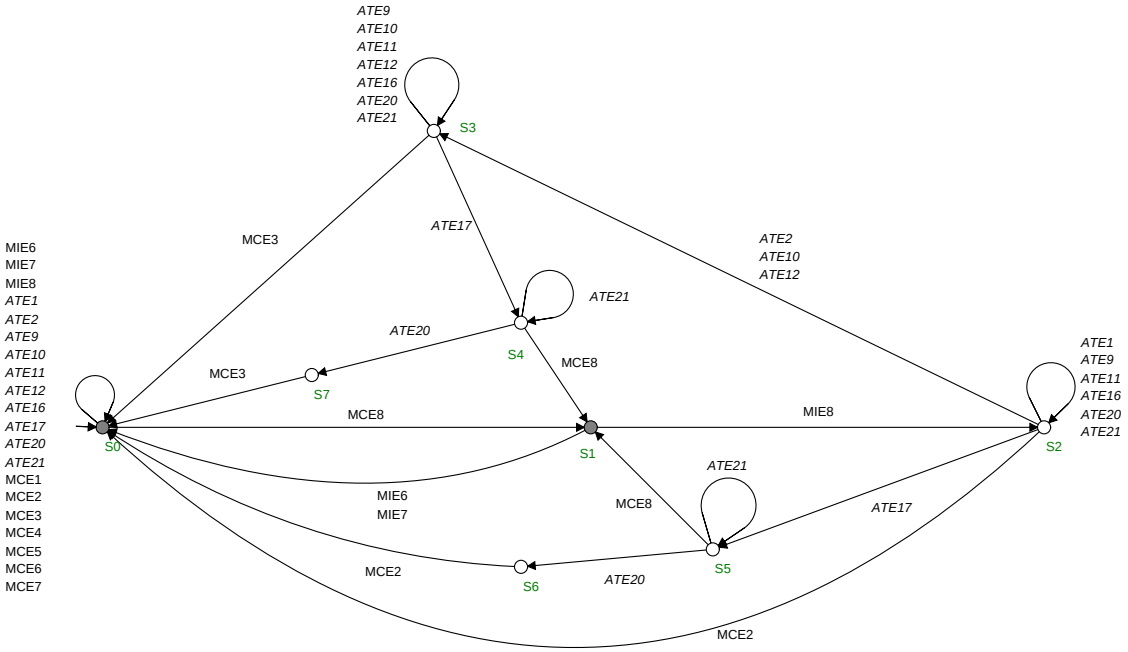

Fig. 25. Automaton model of *Specification 25*. *Specification 25* is triggered under the two successive conditions: i) the multicopter is in AL MODE (*MCE8* occurs); and ii) the flight mode switch is on the position of "AL MODE" (*MIE8* occurs). In this case, if the multicopter's altitude is not lower than a given threshold (*ATE16* occurs), or the multicopter's throttle is less than a given threshold over a time horizon (*ATE20* occurs), the multicopter is automatically disarmed. Otherwise, the multicopter stays in AL MODE (*MCE8* occurs). Here, if the INS and propulsors are both healthy (*ATE1* and *ATE9* occur), the connection to RC transmitter is normal (*ATE11* occurs), the multicopter enters STANDBY MODE (*MCE2* occurs); if one of the related equipment is unhealthy (*ATE2*, *ATE10* or *ATE12* occurs), the multicopter enters GROUND-ERROR MODE (*MCE3* occurs).

Table 2 Controllable event label

Event label	Event name	Event label	Event name
1	*MIE1*	17	*MCE1*
3	*MIE2*	19	*MCE2*
5	*MIE3*	21	*MCE3*
7	*MIE4*	23	*MCE4*
9	*MIE5*	25	*MCE5*
11	*MIE6*	27	*MCE6*
13	*MIE7*	29	*MCE7*
15	*MIE8*	31	*MCE8*

Table 3 Uncontrollable event label

Event label	Event name	Event label	Event name
2	*ATE1*	24	*ATE12*
4	*ATE2*	26	*ATE13*
6	*ATE3*	28	*ATE14*
8	*ATE4*	30	*ATE15*
10	*ATE5*	32	*ATE16*
12	*ATE6*	34	*ATE17*
14	*ATE7*	36	*ATE18*
16	*ATE8*	38	*ATE19*
18	*ATE9*	40	*ATE20*
20	*ATE10*	42	*ATE21*
22	*ATE11*		

In *TCT* software, the multicopter plant is named as "**PLANT**", and the 25 control specifications are named as "$\mathbf{E}_j$", $j = 1, 2, \cdots, 25$.

C. Supervisor synthesis by decentralized supervisory control and supervisor reduction

1) Supervisor synthesis by decentralized supervisory control: Decentralized supervisory control assigns each control specification $\mathbf{E}_j$ a corresponding supervisor. It means that a single supervisor only takes charge of a single subtask. Then, all supervisors work together

to meet the monolithic control specification $\mathbf{E} = \mathbf{E}_1 \| \mathbf{E}_2 \cdots \| \mathbf{E}_{25}$. For **PLANT** and one control specification $\mathbf{E}_j$, the corresponding supervisor is synthesized by

$$\mathbf{S}_j = \mathbf{supcon}\left(\mathbf{PLANT}, \mathbf{E}_j\right),$$

where the sizes of the decentralized supervisors are shown in Table 4. It can be seen that each decentralized supervisor is smaller than the monolithic supervisor $\mathbf{S}$. This means that the decentralized supervisors are 1) easier to be carried out in practical engineering; and 2) convenient to be substituted when any user requirement is changed. Here, the synchronous product of the decentralized supervisors is

$$\mathbf{S}_{\text{DE}} = \mathbf{sync}\left(\mathbf{S}_1, \mathbf{S}_2, \cdots \mathbf{S}_{25}\right).$$

It turns out that $\mathbf{S}_{\text{DE}}$ is nonblocking, meaning that a coordinator is not required. Also, $\mathbf{S}_{\text{DE}}$ is identical to the monolithic supervisor $\mathbf{S}$, testing by

$$\mathbf{isomorph}\left(\mathbf{S}, \mathbf{S}_{\text{DE}}; identity\right) = true.$$

Table 4 Scale of decentralized supervisors

Supervisor name	State number	Transition number	Supervisor name	State number	Transition number
$\mathbf{S}_1$	46	99	$\mathbf{S}_{14}$	77	163
$\mathbf{S}_2$	83	173	$\mathbf{S}_{15}$	51	113
$\mathbf{S}_3$	61	133	$\mathbf{S}_{16}$	54	117
$\mathbf{S}_4$	54	117	$\mathbf{S}_{17}$	51	113
$\mathbf{S}_5$	61	133	$\mathbf{S}_{18}$	77	163
$\mathbf{S}_6$	83	173	$\mathbf{S}_{19}$	51	113
$\mathbf{S}_7$	61	133	$\mathbf{S}_{20}$	52	114
$\mathbf{S}_8$	77	163	$\mathbf{S}_{21}$	50	111
$\mathbf{S}_9$	51	113	$\mathbf{S}_{22}$	40	91
$\mathbf{S}_{10}$	54	117	$\mathbf{S}_{23}$	53	116
$\mathbf{S}_{11}$	51	113	$\mathbf{S}_{24}$	53	116
$\mathbf{S}_{12}$	77	163	$\mathbf{S}_{25}$	58	123
$\mathbf{S}_{13}$	51	113			

2) Supervisor reduction: The 'standard' supervisor $\mathbf{S}_j$ computed by "**supcon**" instruction represents the full optimal controlled behavior, which can be much larger in state size than is actually required for the same control action. This is because the controlled behavior in $\mathbf{S}_j$ incorporates all the transitional constraints embodied in the plant, as well as additional constraints required by control action to enforce the control specifications [1]. Thus, supervisor reduction [1], [2] is performed to find simplified decentralized supervisors, equivalent in control action but of minimum state size.

In *TCT* software, a simplified supervisor $\mathbf{SIMS}_j$ can be obtained by

$$\mathbf{SDAT}_j = \mathbf{condat}\left(\mathbf{PLANT}, \mathbf{S}_j\right)$$

$$\mathbf{SIMS}_j = \mathbf{supreduce}\left(\mathbf{PLANT}, \mathbf{S}_j, \mathbf{SDAT}_j\right).$$

The scale of the simplified decentralized supervisor $\mathbf{SIMS}_j$ is shown in Table 5. It can be seen that the simplified decentralized supervisors $\mathbf{SIMS}_j$ have fewer states than the original decentralized supervisors $\mathbf{S}_j$, meaning an easier realization in practice.

Table 5 Scale of simplified decentralized supervisors

Supervisor name	State number	Transition number	Supervisor name	State number	Transition number
$\mathbf{SIMS}_1$	4	92	$\mathbf{SIMS}_{14}$	6	120
$\mathbf{SIMS}_2$	7	134	$\mathbf{SIMS}_{15}$	3	87
$\mathbf{SIMS}_3$	4	107	$\mathbf{SIMS}_{16}$	4	90
$\mathbf{SIMS}_4$	4	90	$\mathbf{SIMS}_{17}$	3	87
$\mathbf{SIMS}_5$	4	107	$\mathbf{SIMS}_{18}$	6	120
$\mathbf{SIMS}_6$	7	134	$\mathbf{SIMS}_{19}$	3	87
$\mathbf{SIMS}_7$	4	107	$\mathbf{SIMS}_{20}$	4	88
$\mathbf{SIMS}_8$	6	120	$\mathbf{SIMS}_{21}$	3	85
$\mathbf{SIMS}_9$	3	87	$\mathbf{SIMS}_{22}$	2	65
$\mathbf{SIMS}_{10}$	4	90	$\mathbf{SIMS}_{23}$	4	90
$\mathbf{SIMS}_{11}$	3	87	$\mathbf{SIMS}_{24}$	4	90
$\mathbf{SIMS}_{12}$	6	120	$\mathbf{SIMS}_{25}$	5	94
$\mathbf{SIMS}_{13}$	3	87			

For each $\mathbf{SIMS}_j$, a check on correctness can be also performed on *TCT*. Interested readers can refer to [1].

REFERENCES

[1] Wonham W M, Cai K. Supervisory control of discrete-event systems. Lecture notes, Department of electrical and computer engineering, University of Toronto, updated 2016.09.01.

[2] Su R, Wonham W M. Supervisor reduction for discrete-event systems. Discrete Event Dynamic Systems, 2004, 14(1): 31-53.