A Model of Integrated Operator-System Separation Assurance and Collision Avoidance

Steven J. Landry and Amit V. Lagu

School of Industrial Engineering, Purdue University
315 N. Grant St. West Lafayette, IN 47906, USA
slandry@purdue.edu, alagu@purdue.edu

Abstract. A model for the separation assurance and collision avoidance in air traffic has been developed. The objective of the model is to provide qualitative and quantitative predictions of system behavior with respect to separation assurance and collision avoidance. No such model exists, complicating efforts to understand the impact of adding automation to the current system. The model integrates two concepts. First, the system models at the scope of the human-integrated system, instead of the level of the operator. This follows from the work of Duane McRuer, who found that only at the system level was the human as a control system modelable. Secondly, the system considers the separation assurance and collision avoidance problem as a control problem, where agent (automated and human) actions work to control the system from entering undesirable states. This broadly follows the methodology of system safety. Under this methodology, safety is determined by the ability of the agents in the system to impart control to prevent the system from reaching an unsafe state. The model defines system states, the events and conditions that cause transitions between states, and the control that agents in the system can impart to control those transitions.

Keywords: human performance modeling, aviation, safety, air traffic control.

1 Introduction

As identified by Sheridan, one of the great insights of McRuer [9] was that the pilot was so adaptable to different systems that modeling the pilot, as abstract from the system being controlled, was very difficult, but modeling the system, with the pilot embedded within it, was relatively easy [4]. While the McRuer crossover model has had limited application to complex systems, the principle of modeling a system with an embedded human, rather than trying to model the human as abstract from the system, seems still highly relevant.

The safety of future concepts for air traffic control has been difficult to establish, although the current system is known to be remarkably safe from decades of experience. This difficulty in understanding safety is, in part, due to the inapplicability of reliability-based models to a system that is not comprised of subsystems whose failures are independent. In addition, attempts to model the human as abstract from the

V.G. Duffy (Ed.): Digital Human Modeling, HCII 2009, LNCS 5620, pp. 394–402, 2009.

system face significant difficulties in being applied to the very broad tasks assigned to controllers.

A model of the separation assurance and collision avoidance function within the air traffic control system has been developed. The model is of the entire system, with embedded human and automated agents, and is capable of producing qualitative and quantitative assessments of safety. It is particularly useful for quickly examining the impact of changes to the system on safety.

2 Description of the Models

A simple state-based model of the separation assurance and collision avoidance problem was constructed using statechart notation [5]. This model is of the entire human-machine system, rather than of either the system (abstract from the human), or just the human (abstract from the system). The model for a simple system, without separation criteria, air traffic controllers, or automation, is shown in Figure 1. A more complex model, of the current system, is shown in Figure 2.

The models were built to be complete models of the associated systems, where all states were mutually exclusive and exhaustive, except were orthogonal states were identified. Similarly, the conditions were mutually exclusive and exhaustive. The events causing transitions are alleged to be the only events that can cause transitions.

The models were initially analyzed for what they relayed qualitatively about the separation assurance and collision avoidance problem in the National Airspace System (NAS) of the United States. Subsequently, a rough probabilistic assessment was applied to the system to further validate the model's accuracy. Additional information about how the models can be adapted for computational purposes is also provided.

2.1 Model 1 – Simple Collision Avoidance

Model 1 is shown in Figure 1. This model is of a simplified two-aircraft collision avoidance task, similar to visual flight rules (VFR) flight, where controllers are not monitoring the flights and where there are no separation standards enforced. In such a system, collision avoidance is the only concern, and it is established by the actions of the two pilots.

In model 1, the system is in either one of two states. State 1 is that aircraft are separated (have not collided). State 2 is that aircraft have collided. These two states can be seen to be mutually exclusive and exhaustive. The system is in state 1 if condition A is true, and is in state 2 if condition A is not true.

Within state 1 are two substates. The system is in state 1a if a collision will not occur with the current 4D trajectories, and is in state 1b if a collision will occur with the current 4D trajectories (3 spatial dimensions plus time). Again, these states are mutually exclusive and exhaustive under state 1. The system is in state 1a if, in addition to condition A, condition B is true. The system is in state 1b if condition B is false and condition A is true.

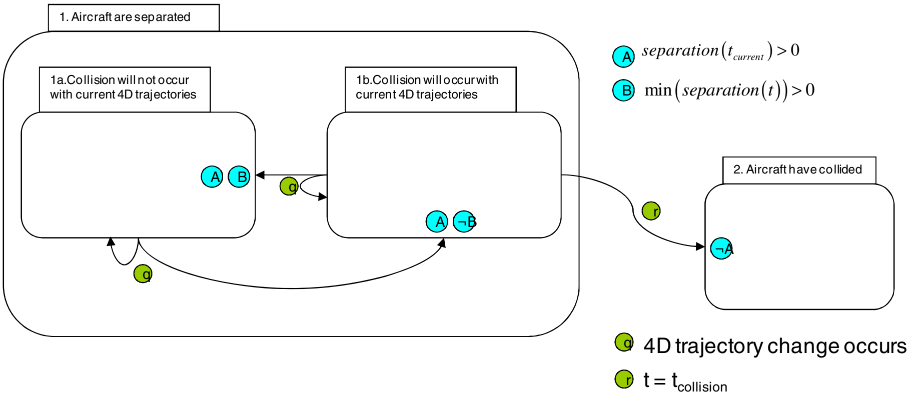
1. Aircraft are separated
1a.Collision will not occur with current 4D trajectories
1b.Collision will occur with current 4D trajectories
2. Aircraft have collided
A
B
¬B
¬A
q
r
A $separation(t_{current}) > 0$
B $\min(separation(t)) > 0$
q 4D trajectory change occurs
r $t = t_{collision}$

Fig. 1. Model 1 - collision avoidance

Transitions between states 1a and 1b can occur only because of a 4D trajectory change (by definition). Transitions between states 1 and 2 can only occur if the system is in state 1b and the current time (t) becomes equal to the time at which a collision will occur ($t_{collision}$). This time can also be defined as the time at which the separation of the two vehicles becomes approximately zero.

If one considers agents within the system (in this case the pilots of the two vehicles), their goal is to prevent the system from reaching state 2. This can be accomplished by detecting that the system is in state 1b and, if so, executing a 4D trajectory change that will result in the system transitioning to state 1a.

These aspects of the model maps well to the actions of pilots with respect to collision avoidance in VFR. Pilots scan for other aircraft, and, if they detect a potential collision, change the 4D trajectory of the aircraft such that a collision will not occur.

The difficulty in this task comes from the uncertainty in detecting system state and in executing a 4D trajectory change that will result in the desired transition. For example, the two aircraft may not be geometrically arranged such that visual contact is possible (e.g. one aircraft above and slightly behind the other). In that case, no detection is possible. Likewise, the execution of a 4D trajectory change is subject to pilot and vehicle delays, and uncertainty in the resulting system state even if the 4D trajectory change is executed properly.

2.2 Model 2 – Separation Assurance and Collision Avoidance

Model 2 adds the problem of separation assurance. In this model, agents must consider the ability of the aircraft to stay safely separated in addition to avoiding a collision. However, separation is a procedural problem and, while being undesirable, is not strictly catastrophic as a collision would be.

In model 2, states 1 and 2 remain unchanged. Within state 1, however, are two orthogonal states. State 1a refers to the current state of the aircraft, and state 1a' refers to the future state of the system. Within state 1a, the system is in state 1a1 if no loss of separation (LOS) has occurred, and is in state 1a2 if a loss of separation has occurred. These states are mutually exclusive and exhaustive with respect to current separation, and are identified by the value of condition C as indicated.

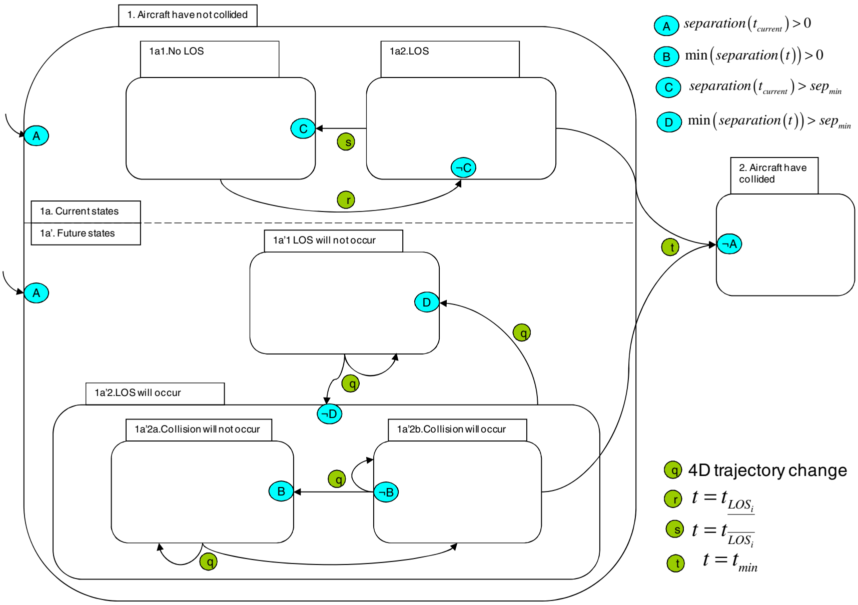
1. Aircraft have not collided
1a1.No LOS
1a2.LOS
A
C
s
¬C
r
1a. Current states
1a'. Future states
1a'1 LOS will not occur
A
D
q
q
¬D
1a'2.LOS will occur
1a'2a.Collision will not occur
1a'2b.Collision will occur
B
q
¬B
q
2. Aircraft have collided
t
¬A
A $separation(t_{current}) > 0$
B $\min(separation(t)) > 0$
C $separation(t_{current}) > sep_{min}$
D $\min(separation(t)) > sep_{min}$
q 4D trajectory change
r $t = t_{LOS_i}$
s $t = t_{\overline{LOS_i}}$
t $t = t_{min}$

Fig. 2. Model 2 - separation assurance and collision avoidance

Within state 1a', the system is in state 1a'1 if a LOS will not occur in the future, and in state 1a'2 if a LOS will occur in the future. The system is in these states if condition D is true or false, respectively.

Within state 1a'2, the system is in state 1a'2a if a collision will not occur, and is in state 1a'2b if a collision will occur. These states map to condition B, as in model 1.

Transitions from state 1a1 and 1a2 can occur due to the start of a LOS event (event r) and the reverse transition occurs due to the end of a LOS event (event s). Transitions between states 1a'1 and 1a'2 occur due to 4D trajectory changes, as do transitions between states 1a'2a and 1a'2b. Transition to state 2 occurs only when the system is simultaneously in states 1a2 and 1a'2b and event t occurs.

In this system, there are several different agents, specifically pilots, air traffic controllers, and automation systems, that work together to keep the system out of state 2. Pilots are not procedurally tasked with separation, so their primary function is collision avoidance. Controllers are primarily tasked with separation assurance. The Traffic Collision Avoidance System on board most commercial aircraft is tasked with collision avoidance. There are also automated systems for detection of impending (conflict alert or CA) and actual LOS (operational error detection program or OEDP) at the air traffic controllers' stations.

These agents each act on different parts of the model. Pilots and TCAS monitor for state 1a'2b and, if detected, apply a 4D trajectory change to move the system to state 1a'2a. Controllers and CA monitor for state 1a'2 and, if detected, controllers apply a 4D trajectory change to move the system to state 1a'1 by passing the 4D trajectory change to the pilot. The OEDP simply detects that the system is in state 1a'2.

There is one additional consideration regarding the model. One might also consider monitoring for the potential for a particular 4D trajectory change to result in a sequence of rapid transitions from safe states to state 2. For example, the system may be in state 1a1 and 1a'1 when a particular 4D trajectory change occurs. (Such changes can occur for reasons other than to control system state; one example is when trajectories are changed to avoid weather or to increase efficiency.) This particular change could result in an immediate transition to state 1a2 and 1a'2, with t_{min} - t being very small. In such a case, a transition to state 2 could happen in a period of time that is shorter than the reaction time of the system.

For example, suppose two aircraft are flying directly at one another, level in opposite directions and separated by the minimum vertical separation of 1,000 feet. A sudden climb by the lower aircraft at an inopportune moment could result in a collision in a matter of seconds. There may be insufficient time for any agent to intervene to prevent the collision. Such a situation is also undesirable.

This capability reflects observed behavior of controllers in that controllers often mitigate conflicts, even when the aircraft do not appear to be in danger of losing separation. Nonetheless, if the minimum separation is such that a plausible mistake or even uncertainty could result in a loss of separation in less time than the controller could respond, the controller would likely intervene by mitigating the potential for LOS. This might be accomplished by applying a 4D trajectory change to increase the minimum t_{min} – t, or by confirming the intentions of the pilot(s) to follow their assigned clearance.

The results of a qualitative analysis of the model are supplied next, followed by application of the best-known probabilities of human performance in this task to try to validate the model.

3 Results

3.1 Qualitative Results

From the model, the critical capabilities for agents, including humans, is the ability to detect system state, to determine the minimum t_{min} - t for any plausible 4D trajectory changes, and to identify a 4D trajectory that can control the value of conditions B (for collision avoidance) and D (for separation assurance). Changes to the system or conditions that diminish these capabilities can be said to negatively impact the safety of the system.

Consider the introduction of TCAS. The ability of pilots to detect and prevent a collision at high speed is rather low, and is very low in instrument conditions. TCAS enhances this ability by detecting closure rates without relying on visual cues. Such an ability significantly increases the ability to detect state 1a'2b, and controls the trajectories of one (or both) aircraft to move the system to state 1a'2a.

Next, consider proposals to replace the air traffic controller with an automated separation assurance system [3]. The ability of such systems to detect system state is not yet clearly defined. In practice, it is difficult to estimate the open-loop behavior of the system accurately, which is a requirement to be able to accurately estimate the effectiveness of a conflict detection capability. As yet, there is no indication that the system is less capable at detecting conflicts than controllers.

Moreover, such systems hold promise because this ability is not affected by the number of aircraft, as would a controller. That is, controllers are currently limited to about 12 aircraft in a sector at a given time, depending on the complexity of the sector. Automation is limited only by the number of comparisons that can be made in the time available (a few seconds). This number is very large, and will grow as computing power increases.

However, such systems do not mitigate potential LOS as do controllers. The system merely detects a predicted LOS and attempts to resolve it. It is possible that aircraft are allowed to achieve a position from which a LOS, and possibly a collision, can occur in less time than is required to intervene. Therefore, there is no protection against a sudden LOS occurring due to detection uncertainty or sudden 4D trajectory change.

This finding corresponds well to the cases that elude detection and resolution by the current version of the automated system. Unexpected changes result in instant or near-instant LOS, making detection irrelevant or useless in such cases. An alternative is to develop a system for detecting pairs of aircraft that will achieve a position from which a LOS or collision can occur in a very short period of time, and resolve those pairs as if a LOS were predicted.

In general, given some new set of procedures or capabilities, the model states that, if there is no impact on the key capabilities – detection and control of state, those new procedures or capabilities will have no impact on safety. Conversely, if the procedures or capabilities do have an impact on those key capabilities, then safety will be reduced. In such cases, the specific impact, and possible mitigation strategies, should be investigated.

3.2 Quantitative Results

The model is a held to be a complete model of the separation assurance and collision avoidance problem. This is supported by the nature of the underlying states, which are mutually exclusive and exhaustive. Furthermore, the events are held to be a complete list of the events necessary and capable of causing a transition. As such, it should be possible to formalize the model mathematically, although this would not necessarily provide information about the behavior of the operators. Moreover, such a formalization may not provide any useful insight when the behavior of the agents themselves are not formalizable.

However, additional evidence was sought to see if the model would comport well with actual system data. In model 1, the probability that the system would end up in state 2 is given by the following equation:

$$P(2) = P(\mathrm{1b})\Big[P(\neg\mathrm{detect\ 1b}) + P(\mathrm{detect\ 1b})\,P(\neg\mathrm{1a}\,|\,\mathrm{detect1b})\Big] \qquad [1]$$

Equation 1 states that the probability the system ends up in state 2 (collision) over some set of repeated trials is the probability the system gets into state 1b (collision will occur with current 4D trajectories) multiplied by the sum of the probability that state was not detected and the probability it was detected but not resolved. Since these figures have been estimated, we can approximate the prediction of the model.

All probability estimates were taken from a report to NASA by LMI consulting [6], except where indicated.

P(1b) is the probability that the system is in state 1b (collision will occur if no control is applied) and has been estimated to be 0.000066. The two terms in the brackets are the probability that the state was not detected and the probability it was detected but not resolved (respectively). Those probabilities, for VFR flight, are estimated at 0.074 and 0.00001. If we make several conservative assumptions, this results in an estimate of P(2) ≈ $5 \cdot 10^{-6}$. The assumptions made to get this result are that there are no procedural methods in use to reduce the probability of collision, and that only one pilot is in a position to detect and resolve the conflict.

While rates of collision per flight are not reported, a somewhat recent figure regarding VFR collisions places the rate at 0.035 per 100,000 flying hours [10]. Considering a high majority of VFR flights are between 1 and 10 hours, this places the rate per flight at approximately $1 \cdot 10^{-6}$. The discrepancy between the model and the (rough) real-world estimate is a factor of 5.

The case for model 2 is more complex. In that system, there are hierarchical relationships that must be considered. Since state 1a2 is a prerequisite to being in state 1a'2b, it can be ignored. The equation then looks similar to equation 1 above:

$$P(2) = P(\text{1a'2b})\left[P(\neg\text{detect 1a'2b}) + P(\text{detect 1a'2b})\,P(\neg\text{1a'2a}|\text{detect1a'2b})\right] \quad [2]$$

Unlike in the above analysis, however, we must consider the actions of multiple agents. For the purposes of this approximation, we make several conservative assumptions:

- the detection and resolution of each agent is independent;
- the influence of controller detection tools is insignificant;
- although agents are detecting and resolving different states, those actions can be approximated as acting on state 1a'2b; and
- the failures of one agent within a type are not independent from failures of the other agents of the same type (i.e. a second TCAS would likely fail in the same cases as a first TCAS), so only one agent of each type is modeled.

Given these assumptions, the following are used as approximations for equation 2:

$$P(\neg\text{detect 1a'2b}) = \prod_{i=1}^{n} P_i(\neg\text{detect 1a'2b}) \quad [3]$$

$$P(\text{detect 1a'2b})\,P(\neg\text{1a'2a}|\text{detect1a'2b}) = \prod_{i=1}^{n} P_i(\text{detect 1a'2b})\,P_i(\neg\text{1a'2a}|\text{detect1a'2b}) \quad [4]$$

The probability that the system is in state 1a'2b is estimated at 0.000066. Other probabilities are given in Table 1.

Table 1. Probabilities estimated for model 2 validation

Agent	**P(¬detect)**	**P(¬resolve|detect)**
Controller	0.0000027	0.0001
Pilot	0.0001	0.0001
TCAS	0.00001	0.00001

Based on these estimates, the probability of arriving in state 2 is approximately $1 \cdot 10^{-8}$. A few estimates from literature are $9.8 \cdot 10^{-8}$ in U.S. airspace in the 1980s [1] and a target level of service from the International Civil Aviation Organization of $1.5 \cdot 10^{-8}$ [2]. The model number compares well to these estimates.

4 Discussion

The qualitative results identify a key deficiency of proposed automation to replace air traffic controller responsibility for separation assurance. Specifically, air traffic controllers mitigate potential conflicts in addition to detecting and resolving predicted conflicts. Proposed automation does not do this, and because of this, cannot ensure that an unexpected event will not result in a LOS or collision.

While algorithms for identifying aircraft that should be mitigated are being investigated, it is possible that such a set is large, and that mitigating those possibilities could decrease capacity. In such a case, it may be important to further subdivide the mitigation set into those with higher and lower probabilities of having the unexpected event occur. If a rule-based method for accomplishing this subdivision can be found, it can be incorporated into the automation.

However, it is possible that such a subdivision is not reliably rule-based. In such a case, the automation may identify the mitigation set to the controller, who would select those that should be mitigated and those that can simply be monitored. The controller may choose additional measures, such as confirming clearances with the pilots of the mitigation aircraft, or identifying specific maneuvers that the pilot must avoid in order to be sure that a LOS or collision will not occur.

The quantitative results, while preliminary, show that the model at least grossly reflects actual system behavior. The quantitative analysis shown, however, does not reflect the dynamic nature of the system.

For example, pilots, controllers, and automation take continuous or dynamically sampled information and predict future separation. This detection must take place in sufficient time to identify and execute a resolution maneuver. A simple static analysis is most likely inaccurate since it does not reflect this very fundamental aspect of the system.

There are a few ways in which this can be addressed. First, a dynamic model can be developed. This can be done algebraically, by integrating the probabilities of detection and resolution, or can be done in Monte Carlo simulations. The challenge for these methods is to accurately capture the dynamic behavior as probabilities, which may not be possible. Second, the model can be transformed into formal models such as State Event Fault Trees [7] or Stochastic Petri Nets [8]. The primary challenge to these latter methods is whether such models can be created where the underlying behavior of agents embedded within the system is not deterministic and, moreover, is difficult to model accurately.

Acknowledgments

This work was supported by NASA Ames Research Center under cooperative agreement number NNA06CN25A. Russ Paielli is the technical monitor.

References

1. Barnett, A., Higgins, M.K.: Airline safety: The last decade. Management Science, 1–21 (1989)
2. Brooker, P.: The risk of mid-air collision to commercial air transport aircraft receiving a radar advisory service in class F/G airspace. The Journal of Navigation 56(2), 277–289 (2003)
3. Erzberger, H.: Transforming the NAS: The next generation air traffic control system. In: The 24th International Congress of the Aeronautical Sciences, Yokohama, Japan (2004)
4. Gerovitch, S.: Interview with Tom Sheridan [Electronic Version] (2003), `http://web.mit.edu/slava/space/interview/interview-sheridan.htm` (retrieved from, 1 March 2009)
5. Harel, D.: Statecharts: A visual formalism for complex systems. Science of Computer Programming 8(3), 231–274 (2002)
6. Hemm, B., Busick, A.: NAS separation assurance benchmark analysis. In: The NASA Research Announcement Review (2009)
7. Kaiser, B., Gramlich, C., Förster, M.: State/event fault trees—A safety analysis model for software-controlled systems. Reliability Engineering and System Safety 92(11), 1521–1537 (2007)
8. López-Grao, J.P., Merseguer, J., Campos, J.: From UML activity diagrams to stochastic petri nets: application to software performance engineering. ACM SIGSOFT software engineering notes 29(1), 25–36 (2004)
9. McRuer, D., Graham, D.: Human pilot dynamics in compensatory systems (No. AAFFDL-TR-65-15). USAF (1965)
10. Taneja, N., Wiegmann, D.A., Savoy, I.: Analysis of midair collisions in civil aviation. In: The 45th Annual Meeting of the Human Factors and Ergonomics Society, Santa Monica, CA (2001)