Analytical Risk Model for Automated Collision Avoidance Systems

Vitali Volovoi[*], Alexandra Balueva[†], and Rene Valenzuela Vega[‡]

Georgia Institute of Technology, Atlanta, GA, 30332, USA

As increasingly sophisticated collision avoidance systems are developed, assessing their effectiveness becomes both more important and challenging. In this paper, an application of a new analytical procedure is presented. While Monte Carlo simulations can capture the underlying stochastic processes, they require a very large number of simulations to estimate rare events with sufficient accuracy. The advantage of the analytical methods is not only computational efficiency and higher precision, but also increased transparency of the contributing risk factors, which is particularly beneficial given the uncertainty about the input parameters and the associated need of sensitivity studies. The proposed method relies on discrete (non-homogeneous) Markov chains that are solved in closed form to evaluate system-level risk. This method provides an efficient means for modeling dependent subsystems without explicit state-space representation of individual components. Instead, Markov chains for non-repairable portions of the model are semi-inverted and the resulting transition rates are used in the full Markov model. The developed procedure is first illustrated with an example that exhibits the salient features of the underlying process, and is then applied to Advanced Airspace Concept (AAC) in order to demonstrate the method's capabilities and to compare the results with those of published Monte Carlo simulations.

I. Introduction

Collision avoidance systems are critical for the safety of airspace, especially given the expectations of a significant increase in operation density in the future. Another related but distinct factor that increases the importance of collision avoidance systems is the issue of integration of Unmanned Air Vehicles (UAVs) into the national airspace. The targeted levels of safety as a function of air traffic density have been used to provide a baseline characterization (*i.e.,* without taking into account any mitigation action) of the collision risk,[1] thus providing clear motivation for mitigation strategies in UAV operations. Quantification of the overall (system-level) safety impact of collision-avoidance systems requires an understanding of the relevant interactions among the various layers of protection against collisions, as well as of the frequencies and patterns of encounters that can lead to collisions. The latter (collision encounter problem) has been extensively investigated,[2,3] but the challenges of the former problem are also significant, and this paper is devoted to addressing those challenges. One can divide the overall problem of estimating the risk of collision into three steps:

1. Determining the conflict frequency;
2. Given the conflict, determining the chances of resolving it by a deployed collision avoidance system (the focus of this paper);

[*] Assistant Professor, School of Aerospace Engineering, 270 Ferst Dr.; Senior AIAA Member.

[†] Graduate Research Assistant, School of Aerospace Engineering, 270 Ferst Dr.

[‡] Graduate Research Assistant, School of Aerospace Engineering, 270 Ferst Dr.; Student AIAA Member.

Journal of Guidance, Control, and Dynamics (Accepted for publication, 2012)

3. Determining collision chances, given Near Mid-Air Collision (NMAC), which is the failure of the collision avoidance system to resolve a conflict.

It is a common and generally a reasonable assumption that the calculations involved in these three steps are mutually independent (at least in the first approximation).

From the system reliability and safety modeling standpoint, a collision-avoidance system relies on time redundancy, as there are several consecutive attempts to detect and resolve a conflict. This time redundancy is supplemented by functional redundancy, as the time before the conflict is separated into distinct phases (layers) with the conflict resolution task assigned to distinct subsystems. This functional separation is motivated by the increased urgency of the task combined with less uncertainty about the conflict. So, as a general rule, as time progresses, conflict resolution should be simpler (less complex) in order to facilitate reliability, and can be simpler, as it deals with less uncertainty. In addition, increasing the diversity of the protective layers provides some protection against common-cause failures that can defeat the intended redundancy. Combining structural and time redundancy is not unique to collision avoidance, and is well recognized as providing a more efficient means of protection than each type of redundancy alone in other applications, such as in designing fault-tolerant computer systems to negate the effects of transient faults.[4] While detection becomes more efficient as time progresses (as the uncertainty about the trajectories decreases), there is the potential for accumulation of failures that hinder both successful detection and resolution of those conflicts.

There are several methods for modeling the system reliability of time-redundant systems, including the use of semi-Markov processes[5] or universal generating function technique.[6] Therein, the variability of the duration of individual tasks necessitates the use of continuous-time Markov processes, commonly used in reliability modeling of renewable systems.[7] Those methods are not directly applicable to the modeling of automated collision avoidance systems, as they don't allow the presence of accumulated permanent faults. Indeed, permanent faults violate the assumption of semi-Markov processes requiring for a transition from a state to be fully determined by the current state and the holding (sojourn) time in that state. In contrast, for the problem of conflict resolution, the duration of each attempt is of secondary importance, but the number of those attempts is not known *a priori*, so discrete Markov chains suffice. On the other hand, fault-tree analysis (i.e., analysis based on static Boolean algebra)[8] can deal with permanent failures, and provide important initial insights,[9, 10] but have some known limitations for modeling dynamic scenarios that involve dependent events.[11] Combined use of Markov analysis and Fault Trees has been previously suggested in the literature, *e.g.,* dynamic fault trees,[12, 13] where traditional fault trees are augmented with special gates representing specific dynamic scenarios, *e.g.,* functional dependency. Effectively, dynamic fault trees serve as pre-processors for Markov models, which are constructed internally and automatically. In contrast, the proposed method does not require full representation of state space of non-repairable portions of the system; instead only relevant conditional probabilities of dependent subsystems are calculated.

If dynamic interactions are confined to a single layer of protection, then a decoupled (hierarchical) analysis is possible, as advocated in the context of sense-and-avoid systems:[14] an inner loop that includes a collision encounter model and relies on Monte Carlo simulation combined with an "outer loop" analysis based on fault trees. However, if different layers share common failure modes, neglecting this coupling in the fault-tree analysis can lead to nonconservative risk estimates. In order to account for this coupling, the scope of Monte Carlo simulation can be extended to encompass several layers of conflict avoidance. However, increases both the complexity of the simulation models and the number of the simulation runs needed to capture rare events. While importance sampling can provide an increase in the convergence rate,[15] this improvement is problem-dependent.

In what follows, the developed procedure is first described on a conceptual example and then applied to a specific application, Advanced Airspace Concept (AAC),[16] with the issues regarding the generality of the procedure addressed as appropriate. The selection of the application is motivated by the availability of the detailed description of an automated avoidance system safety model conducted using Monte Carlo simulation.[17, 18] The goal of this paper *is not* to evaluate the assumptions made for AAC,[17, 18] but to demonstrate an analytical method that can capture the dynamic interactions without the need of lengthy Monte Carlo simulations for systems with the mixture of non-repairable or Markov (when state transitions only depend on the current state and time) components.

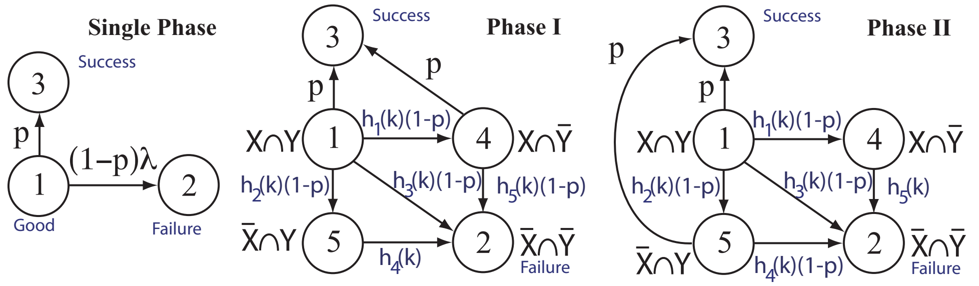

Figure 1. State space for single phase (left) and two-phase (center and right) scenarios

II. Conceptual example

Let us assume that at moment $t_1 = 0$ the system is fully operational, and consecutive attempts to detect and resolve the conflict are made at times $t_k = \delta(k-1)$, $k = 1 \dots n = 20$. At each time step $1 \leq k \leq n$, probability of successful detection and resolution is the same, $p = 0.4$. If failures of the system are neglected, the probability of failure is $p_f = (1-p)^{20} = 3.656 \times 10^{-5}$: there are 20 independent attempts to resolve the conflict, and each time the chances of failure to resolve the conflict is $1 - p$.

Next we introduce the possibility of permanent system failures that preclude conflict resolution. The system is operational at the beginning of the conflict resolution, but failures occur with the constant failure rate $\lambda = 0.001/\delta$, so that the chance of system being operational at step k is $R(k) = R(tk) = \exp\left[-\lambda(k-1)\right]$. As a result, the number of attempts for conflict resolution is not known *a priori*. Fig. 1 (left) depicts a discrete time Markov chain for this process with three possible states: (1) the conflict has not been resolved and the system is operational; (2) the conflict has not been resolved and the system has failed (no future resolutions are possible); and (3) the conflict has been resolved. Transitions described in the figure allow the assembling of transition matrix with elements Q_{ij} corresponding to the conditional probability of transitioning to state i at the next step, given the current position j (each column adds up to one).

$$Q = \begin{pmatrix} (1-p)(1-\lambda) & 0 & 0 \\ (1-p)\lambda & 1 & 0 \\ p & 0 & 1 \end{pmatrix} \tag{1}$$

An initial state of the system $\pi(0) = \{1, 0, 0\}$ allows the calculation of the probabilities of the final state after n time steps $\pi(n) = Q^n \pi(0)$. Specifically, $1 - \pi_3(n)$ will correspond to the chances of failure to resolve the conflict.

Since conflict resolutions occur at discrete times, instead of following the process step-by-step, it is possible to evaluate system failure by exploring disjoint events that lead to failure based on the number of resolution attempts k made ($k = 1 \dots n$). Indeed, $k < n$ attempts implies that *i)* all attempts made were unsuccessful (with the probability $(1-p)^k$), and *ii)* the system was operational up to step k, but failed before the next step, $k+1$, was possible (the chances of that are $R(k) - R(k+1)$). At the last step n, the failure to detect only occurs if all n attempts fail, which is expressed as $R(n)(1-p)^n$. Therefore, the total probability of failure is given by

$$p_f = R(n)(1-p)^n + \sum_{k=1}^{n-1} \left[R(k) - R(k+1)\right](1-p)^k \tag{2}$$

Both methods yield identical results, which in the considered numerical example renders $p_f = 1.53 \times 10^{-3}$. Both procedures apply to any system with non-repairable components, if the system's reliability $R(k)$ is properly calculated (e.g., by means of Boolean algebra), and, for Markov states, the transition rate is a standard hazard rate $\lambda(k) = f(k)/R(k)$, $f(t) = -\frac{dR(t)}{dt}$. If this rate or the detection probability p varies with step k, then the procedure remains the same, but the final state is calculated as $\pi(n) = \prod_{i=1}^{n} Q^i \pi(0)$.

Next, let us consider a scenario with functional redundancy where two phases with different systems are utilized with an overlap between the two systems X and Y: in the first phase, the functionality is provided by either of the two subsystems U and V, and in the second phase, subsystem W replaces subsystem U. Now, the Markov model has two additional states (see Fig. 1, center and right): state 4 for system X is down and Y up $(\bar{X} \bigcap Y)$, while state 5 corresponds to the opposite situation $(X \bigcap \bar{Y})$. If subsystem X failed early, subsystem Y gets only engaged at time step m. No assumptions about the types of failure distributons are made for each subsystem. Considering the non-repairable part in isolation, the probabilities for each step can be determined using Boolean algebra: $\hat{P}_1(k) = R_V(k) + (1 - R_V(k))R_U(k)R_W(k)$, $\hat{P}_4(k) = (1 - R_V(k))R_U(k)(1 - R_W(k))$, and $\hat{P}_4(k) = (1 - R_V(k))(1 - R_U(k))R_W(k)$. Here hats over the probabilities are used to emphasize that no renewable portion of the system is considered, corresponding to setting $p = 0$ in Fig. 1 (center and right). Three balance equations can be written (the fourth one is redundant):

$$\hat{P}_1(k+1) = \hat{P}_1(k)(1 - h_1(k) - h_2(k) - h_3(k)) \tag{3}$$

$$\hat{P}_4(k+1) = h_1(k)\hat{P}_1(k) + (1 - h_5(k))\,\hat{P}_4(t_k) \tag{4}$$

$$\hat{P}_5(k+1) = h_2(k)\hat{P}_1(k) + (1 - h_4(k))\,\hat{P}_5(t_k) \tag{5}$$

These equations could be used to calculate the discrete transition rates, but there are five unknowns, $h_1(k) \ldots h_5(k)$, and only three equations. However, $h_4(k) = \lambda_W(k)$ and $h_5(k) = \lambda_U(k)$ (since in both cases subsystem V has failed), so $h_i(k)$ can be determined $(i = 1 \ldots 5)$ using Eq. 3-5, and the result can be used to assemble matrices $Q(k)$ in accordance with transitions depicted in Fig. 1 (center and right). In general, there might be more than one possible configuration for the degraded state, and in this case the total transition rates have to be weighted in accordance with the probability of each degraded configuration. Traditionally Markov processes are used to evaluate states' probabilities as functions of time given known transition rates; in contrast, the current procedure relies on Boolean algebra to calculate the probabilities of states for subsystems subject to permanent failures, and the result is used to calculate transition rates.

Fig. 2 compares the numerical results for system failure probability as a function of probability p of single-conflict resolution for two different set of assumptions. First, components are considered to be independent for each phase, and second, the common-cause failures are taken into account. Here $\lambda_U = \lambda_W = 0.1/\delta$ and $\lambda_V = 0.001/\delta$. For verification purposes, the results of 10 million Monte Carlo runs using Stochastic Petri Nets[19, 20] are also provided. If the two phases are independent, both the Boolean method for the final states evaluated for each phase separately (Eq. 2) and the Markov procedure yield identical results. However, evaluating the final states for dependent components is impossible without knowing the terms of type $P(Y(k)|X(m))$ (the conditional probability that system Y is operational at time step k given that system X was operational at time step m), effectively requiring the tracking of all the intermediate steps (as done by Markov modeling). Furthermore, while numerical values are provided for illustrative purposes only, the challenges of estimating common-cause effects can be observed: if for low values of the probability of single-conflict resolution p those effects are negligible; for high p the predictions vary by two orders of magnitude. The relative error of Monte Carlo simulation degrades from a fraction of a percent for low p to up to 15% for higher values of p, as expected when dealing with rare events. However, this level of accuracy might be acceptable, and for this small problem 10 million Monte Carlo runs takes less than a minute on a modern laptop. Nevertheless, realistic models will require more computational effort, and a 15% error rate might be important if two configurations are compared where simple variance reduction techniques, such as common random numbers, are not directly applicable. The presented analytical models not only provide computational efficiency and transparency, but they can also serve as alternative and relatively independent means for verifying modeling accuracy.

III. Application to AAC

Successful conflict resolution requires the appropriate equipment to be operational, and successful trajectory generation and conflict detection are also necessary. There are several layers of conflict avoidance, each invoked in sequence as time progresses. There is an overlap in terms of the equipment used by each layer, so that the permanent failures of layers are not independent. Furthermore, within each layer, several attempts are made to resolve the conflict. In the case of AAC, there are three such layers: Autoresolver (AR), Tactical Separation-Assured Flight Environment (TSAFE), and Traffic-alert Collision Avoidance System (TCAS): first AR is engaged (from 8-20 minutes until 3 minutes before the conflict), followed by TSAFE (from 3 minutes until 1 minute), and TCAS (at 1 minute before the conflict). There is an additional (final) level of safety (visual avoidance by pilots) that is applied last, and its efficiency is provided by the fraction of conflicts that were unresolved by the first three layers but resolved by the fourth layer (so its evaluation

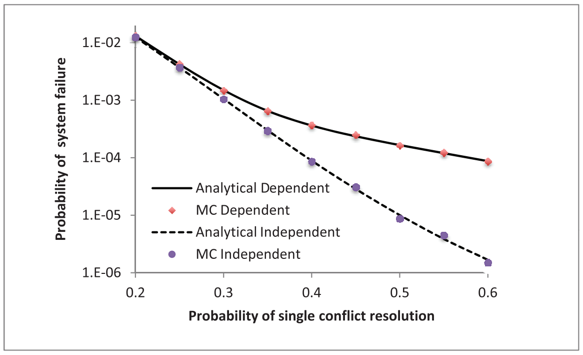

Figure 2. System failure as a function of probability of single conflict resolution p

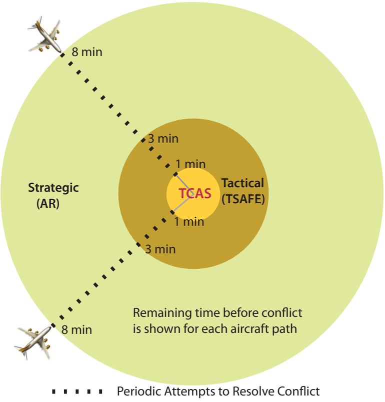
8 min
3 min
1 min
TCAS
Tactical
(TSAFE)
Strategic
(AR)
1 min
3 min
8 min
Remaining time before conflict
is shown for each aircraft path
Periodic Attempts to Resolve Conflict

Figure 3. Three layers of conflict resolution in AAC (the fourth layer, visual avoidance, is not depicted).

is decoupled from the evaluation of the first three layers).

At $t_1 = 0$ all subsystems are failure-free[17,18] and there is the first possibility of identifying the conflict (this is the initial state A_1, which is $T = 8$ min away from the conflict). At every time step t_k, $k = 1 \ldots n$, an attempt is made to resolve the conflict; n is the total number of those attempts for all layers (phases). For ACC we have $n = 15$ and $t_{k+1} - t_k = 0.5$ min for $k = 1 \ldots n - 1$. The following sets of intermediate states are considered: $A_1 \ldots A_{10}$ for AR, $B_{11} \ldots B_{15}, E_{11} \ldots E_{15}$ for TSAFE, and C for TCAS. In addition, there are two "final" states, F and S, corresponding to system failure and success, respectively.

To minimize the complexity of the risk analysis, it is important to identify subsystems (modules) that are as large as possible without obscuring the coupling among the subsystems. Specifically, the common components that make the performance of layers dependent require a separate treatment. In the case of AAC,[17] the following coupling mechanisms are identified:

1. Mode S transponder on each aircraft. Its functionality is critical to all three conflict-avoidance systems, so T denotes the transponder subsystem (corresponding to the transponders of both aircraft). Based on the assumptions made in Ref. 17, such a failure causes the entire collision avoidance system to fail.

2. Resolution Delivery (RD). There are shared components between AR and TSAFE contributing to RD functionality; however, the chances of the loss of RD functionality during the AR phase are negligible. Indeed, the chances of RD functionality in AR configuration for the whole flight can be calculated[21] as $\approx 5.76 \times 10^{-15}$. Noting that the overall risk of system failure is on the order of $\sim 1 \times 10^{-6}$ — 1×10^{-9}, this failure mode can be neglected. This is explained by quadruple redundancy at the component level for the AR phase. As a result, the failure of RD needs to be considered only for TSAFE, and therefore this source of coupling between different phases can be neglected. Such prescreening of the contributing risk factors (at the subsystem rather than component level) is important to simplify the analysis.

3. The speaker that announces the resolution to the pilot in both the TSAFE and TCAS systems. We will denote this subsystem as K, so that its failure occurs when a speaker system on either of the two aircraft fails The purpose of separating the functionality of this subsystem stems from the fact that while TSAFE can operate with one of the speakers down, TCAS cannot (here we follow the assumptions made in Ref. 17 for consistency, although an argument can be made that TCAS can facilitate collision avoidance even if only one of the aircraft reacts). In order to make this distinction, we introduce separate states during TSAFE operation (B_k if both speakers are operating, and E_k otherwise).

   This use of compressed state-space representation of conditional states for two subsystems (as described in the conceptual example) can be contrasted with a brute-force approach that would rely on explicit consideration of the possible states of all components of these two subsystems. In the considered model there are five components and $2^5 = 32$ states.[21] When both systems are down, the occurrences of further failures are irrelevant, so there are actually fewer distinct states, and symmetry considerations can be used to further reduce the state space. Still, this approach is prone to state-space explosion, and has poor scalability for problems with a larger number of components.

4. Location functionality for both aircraft is common to AR and TSAFE (subsystem L). The mode S transponder participates in location as well, but it is treated separately, so subsystem L excludes the mode S transponder. Finally, subsystems of AR and TSAFE that related to neither location nor transponder, are denoted as R and Z, respectively.

As a result, the distinct subsystems R, Z, K, L, T provide the required level of granularity to capture all the coupling from the equipment perspective. At the last step of TSAFE, E_{15} implies failure (and so the corresponding probability needs to be added to the failed state), while B_{15} is the same as C. State C implies that TCAS is required (and both speakers and both transponders are operational). A full description of the corresponding transition matrices is provided in Ref.[21]

A. Discussion

The system safety structure and parameters of the AAC model[17] were used as an illustration and a reference point for constructing the corresponding analytical model, so this work should not be considered as an endorsement of that model (and as a result, the endorsement of the corresponding risk estimation). However, this can be considered a starting point for constructing meaningful models, which can be used for developing safety cases for particular collision-avoidance implementation, along with the requirements for the performance characteristics of the individual components. To this end, several initial observations can be made:

1. The probability of detection is based on squaring the probability of not deviating by half of the distance.[17] Based on purely geometric considerations, the probability of detection is significantly higher. In the extreme case of a head-on collision, one can derive an analytical formula using normal cross-track error distribution and the Euclidean difference. It can be ascertained that the currently used formulae provide conservative estimates. However, there is a possibility of a correlation between the errors (common bias) both in time and between the two aircraft in conflict. The former would lead to the increased chances of system failure.

2. Commission error: for example, a "false positive" situation where the system mistakenly identifies a conflict; this is potentially an important consideration due to the reduction of the time available for correcting the error. Similarly, resolution of an existing conflict can be executed incorrectly. The issue is related to the "Byzantine fault tolerance."[22] A more detailed modeling of conflict resolution is needed to estimate the associated probabilities.

3. At time $t_1 = 0$, all systems are assumed to function properly; this needs to be revisited, as the risks during the recovery process are not trivial (requiring a separate model).

4. The failure rate of the ADS-B Mode S transponder is obtained from Ref. 10, with the source citing a value one order of magnitude higher, and based on an exposure of 20 minutes (and not two hours). Apparently, this reduction of the failure rate is due to a credit for redundancy. Due to the importance of this parameter on the overall failure of the system, this issue should be further investigated and the redundancy of the transponders must be modeled explicitly.

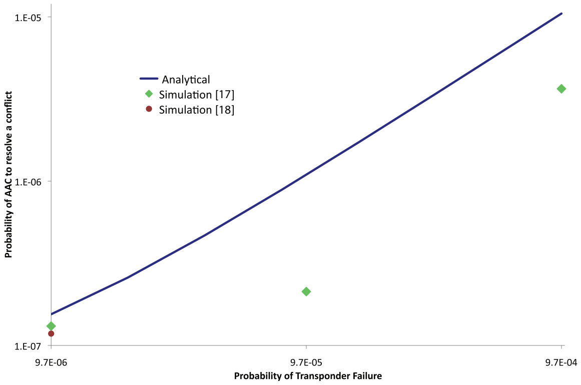

Figure 4. Sensitivity of the probability of ACC failure to the failure of AC Mode S transponder; log-log scale is used.

In accordance with Monte Carlo simulation,[17] out of 10 billion runs there were 1180 cases where the three layers of AAC failed (829 of those cases were resolved using the last fourth layer). This translates into the chances of failure of all three systems to be 1.180×10^{-7}. Those results can be compared with the numerical results obtained analytically using the developed procedure. If only the transponder is allowed to fail (all the other subsystems cannot fail), then the total probability of failure is 1.117×10^{-7}, which is very close to the result reported in Ref.[17] As expected, transponders dominate the overall failure rate (due to the lack of redundancy). Upon the completion of the first phase (9 steps of AR), the AAC system will fail with the probability 1.04315×10^{-7}, while the chances that the system will transition to TSAFE is 7.0173×10^{-4}. After all three phases are completed and TCAS has been engaged, the chance of failure of AAC is 1.548×10^{-7}. Figure 4 depicts the sensitivity of the probability of ACC failure with respect to the probability of AC Mode S transponder failure, which is the main driver of system failure. The latter is varied over the two orders of magnitude, and depicted using the log-log scale with the results from Ref.[17,18] shown for comparison as well.

IV. Conclusions

An analytical procedure has been presented for evaluating the reliability of several layers of collision avoidance. A distinct feature of the developed procedure is its ability to model dependent subsystems by employing a novel semi-inversion of the Markov model. Specifically, a submodel that corresponds to the nonrenewable part of the system is evaluated using Boolean algebra, and the expressions obtained for subsystem state probabilities are used to infer the transition rates among those states. Finally, those transition rates are supplemented by the inclusion of recurrent events, resulting in a complete state-space representation.

Acknowledgments

This research was supported by the National Aeronautics and Space Administration (NASA Research Announcement No. NRA #NNA08BA64C). In particular, thanks go to Parimal H. Kopardekar, Heinz Erzberger, and David Thipphavong for their valuable assistance and encouragement.

References

[1] Weibel, R. E. and Hansman Jr., R. J., "Safety considerations for operation of different classes of UAVs in the NAS," Vol. 1, Chicago, IL, United states, 2004, pp. 341 – 351.

[2] Kochenderfer, M., Espindle, L., Kuchar, J., and Griffith, J., "A comprehensive aircraft encounter model of the national airspace system," *Linc. Lab. J. (USA)*, Vol. 17, No. 2, 2008, pp. 41 – 53.

[3] Kochenderfer, M., Edwards, M., Espindle, L., Kuchar, J., and Griffith, J., "Airspace Encounter Models for Estimating Collision Risk," *J. Guid. Control Dyn. (USA)*, Vol. 33, No. 2, 2010, pp. 487 – 99.

[4] Krishna, C. and Singh, A., "Reliability of checkpointed real-time systems using time redundancy," *Reliability, IEEE*

Transactions on, Vol. 42, No. 3, Sept. 1993, pp. 427 –435.

[5] Lisnianski, A. and Jeager, A., "Time-redundant system reliability under randomly constrained time resources," *Reliability Engineering and System Safety*, Vol. 70, No. 2, 2000, pp. 157 – 166.

[6] Lisnianski, A., Levitin, G., and Ben-Haim, H., "Structure optimization of multi-state system with time redundancy," *Reliability Engineering and System Safety*, Vol. 67, No. 2, 2000, pp. 103 – 112.

[7] Birolini, A., *Reliability Engineering: Theory and Practice*, Springer, sixth ed., 2010.

[8] M. Rausand, M. and Høyland, *System Reliability Theory. Models, Statistical Methods, and Applications*, John Wiley and Sons, New York, 2nd ed., 2004.

[9] Andrews, J., Erzberger, H., and Welch, J., "Safety Analysis for Advanced Separation Concepts," *Air Traffic Control Quarterly*, Vol. 14, No. 1, 2006, pp. 5–24.

[10] Hemm, R. and Busick, A., "Safety Analysis of the Separation Assurance Function In Today's National Airspace System," *9th AIAA Aviation Technology, Integration, and Operations Conference*, Hilton Head, South Carolina, Sep. 21-23 2009.

[11] Labeau, P., Smidts, C., and Swaminathan, S., "Dynamic reliability: Towards an integrated platform for probabilistic risk assessment," *Reliability Engineering and System Safety*, Vol. 68, No. 3, 2000, pp. 219 – 254.

[12] Dugan, J., Bavuso, S., and Boyd, M., "Dynamic fault-tree models for fault-tolerant computer systems," *IEEE Transactions on Reliability*, Vol. 41, No. 3, 1992, pp. 363–377.

[13] Čepin, M. and Mavko, B., "A dynamic fault tree," *Reliability Engineering and System Safety*, Vol. 75, No. 1, 2002, pp. 83 – 91.

[14] "Sense and avoid for Unmanned Aircraft Systems. Final Report of FAA Sponsored Sense and avoid Workshop," Tech. rep., Federal Aviation Administration, 9 October 2009.

[15] Blom, H. A. P., Obbink, B. K., and Bakker, G. J., "Simulated Safety Risk of an Uncoordinated Airborne Self Separation Concept of Operation," *Air Traffic Control Quarterly*, Vol. 17, No. 1, 2009, pp. 63–93.

[16] Erzberger, H. and Paielli, R., "Concept for Next Generation Air Traffic Control System," *Air Traffic Control Quarterly*, Vol. 10, No. 4, 2002, pp. 355–378.

[17] Blum, D. M., Thipphavong, D., Rentas, T. L., He, Y., Wang, X., and Pate-Cornell, M. E., "Safety Analysis of the Advanced Airspace Concept using Monte Carlo Simulation," *AIAA Guidance, Navigation, and Control Conference*, Toronto, Ontario, Canada, Aug. 2-5 2010.

[18] Thipphavong, D., "Accelerated Monte Carlo Simulation for Safety Analysis of the Advanced Airspace Concept," *10th AIAA Aviation Technology, Integration, and Operations Conference*, Fort Worth, Texas, Sep. 13-15 2010.

[19] Volovoi, V. V., "Modeling of System Reliability Using Petri Nets with Aging Tokens," *Reliability Engineering and System Safety*, Vol. 84, No. 2, 2004, pp. 149–161.

[20] Volovoi, V., "Stochastic Petri Nets Modeling using SPN," *Proceedings of Annual Reliability and Maintainability Symposium*, IEEE, Newport Beach, CA, January 2006, pp. 75–81.

[21] Volovoi, V., Balueva, A., and Valenzuela, R., "Analytical Risk Model for Automated Collision Avoidance Systems," *11th AIAA Aviation Technology, Integration, and Operations Conference (ATIO)*, Virginia Beach, VA, 20 - 22 Sep 2011.

[22] Lamport, L., Shostak, R., and Pease, M., "The Byzantine Generals Problem," *ACM Trans. Program. Lang. Syst.*, Vol. 4, July 1982, pp. 382–401.