Fault Tolerance of Relative Navigation Sensing in Docking Approach of Spacecraft

Dimitry Gorinevsky
Mitek Analytics LLC, Palo Alto, CA 94306
and EE Department, Stanford University
dimitry@mitekan.com, gorin@stanford.edu

Gabriel M. Hoffmann, Mitek Analytics LLC and AA Department, Stanford University
Marina Shmakova, Mitek Analytics LLC and Physics Department, Stanford University
Robert W. Mah, NASA Ames Research Center
Scott Cryan, NASA Johnson Space Center
Jennifer D. Mitchell, NASA Johnson Space Center

Abstract—This paper analyzes fault tolerance of spacecraft relative navigation in Automated Rendezvous and Docking (AR&D). The relatively low technology readiness of existing relative navigation sensors for AR&D has been carried as one of the NASA Crew Exploration Vehicle Project's top tasks. Fault tolerance could be enhanced with the help of FDIR (Fault Detection, Identification and Recovery) logic and use of redundant sensors. Because of mass and power constraints, it is important to choose a fault tolerant design that provides the required reliability without adding excessive hardware. An important design trade is determining whether a redundant sensor can be normally unpowered and activated only when necessary. This paper analyzes reliability trades for such fault tolerant system. A Markov Chain model of the system is composed of sub-models for sensor faults and for sensor avionics states. The sensor fault sub-model parameters are based on sensor testing data. The avionics sub-model includes FDIR states; the parameters are determined by Monte Carlo simulations of the near field docking approach. The integrated Markov Chain model allows the probabilities of mission abort and a mishap to be computed. The results of the trade study include dependence of the probabilities on the backup sensor activation delay.

TABLE OF CONTENTS

1 INTRODUCTION 1
2 MARKOV CHAIN MODEL 2
3 SENSOR MODEL 3
4 AVIONICS/FDIR MODEL 5
5 ANALYSIS RESULTS 6
6 CONCLUSIONS 7
REFERENCES 8
BIOGRAPHY 9

This work was supported by NASA Exploration Systems Mission Directorate ETD Program, AR&D Sensors project, through Mitek Analytics LLC research subaward #8318-MAL-001, perotsystems-QSS prime contract #NNA04AA18B.
U.S. Government work not protected by U.S. copyright.
IEEEAC Paper #1251, Version 6 Updated 12/02/2007.

1. INTRODUCTION

NASA's Exploration System architecture has a requirement for automated rendezvous and docking (AR&D) of the spacecraft. The relatively low technology readiness of existing relative navigation sensors for AR&D has been carried as one of the NASA Crew Exploration Vehicle (CEV) Project's top tasks, e.g., see [6], [14].

Operating a chaser spacecraft in proximity of the target during a docking approach is safety critical because of the collision risk. The relative navigation system needs to be fault-tolerant; a fault could lead to a mishap. From many points of view AR&D is similar to aircraft Autoland systems, which navigate and guide aircraft relative to a landing strip. Much work on fault tolerant design of Autoland was done in the 1980s when these systems were first developed and introduced, e.g., see [7]. By contrast, there is little prior work on fault tolerance of AR&D navigation.

Because of spacecraft mass and power constraints, it is important to choose a fault tolerant design providing required reliability with minimum hardware. One challenge is determining how many redundant relative navigation sensors are needed. Another is determining whether the redundant sensors can be kept unpowered and activated only when necessary.

We consider spacecraft relative navigation during close-range approach. The system fault tolerance and redundancy management (FT/RM) configuration is as outlined in [23]. There are two relative navigation sensors. Normally, the main sensor is used. The backup sensor is activated if the main sensor fails. An alternative is having both sensors operational all the time. We assume that the inertial navigation system of the spacecraft is fault tolerant. This paper studies (FT/RM) of relative spacecraft navigation for the described system configuration. The analysis approach could be used for other FT/RM architectures and configurations.

Looking at the relative navigation system design from the FT/RM perspective, the first question is:

Question 1: Is the two fault tolerance requirement (Fail Operational/Fail Safe) achieved?

A short answer to this question is 'yes'. This answer is based on our earlier study [10]. Achieving the fault tolerance requires (i) being able to detect a fault of the relative navigation sensor and (ii) having a redundancy management and fault recovery capability. The relative sensor fault detection approach based on analytical redundancy is discussed in detail in [10]. It relies on fault-tolerant inertial navigation. The basic idea is that an observed relative pose change must be accompanied by commensurate acceleration and rotation measured by the IMUs. A mismatch indicates a fault.

If a persistent fault of the relative navigation sensor is detected, a backup sensor could be activated to continue operation (Fail Operational). A fault of the backup relative navigation sensor could be detected the same way. The second failure would require aborting the AR&D approach (Fail Safe). A brief discussion of the Guidance and Control (G&C) for the abort is contained in [10]. The analysis in this paper assumes that a safe abort of the docking approach is always possible. This simplifying assumption is introduced to reduce complexity and to focus on the navigation system analysis. Once the CEV G&C logic for the docking abort is established, the analysis can be extended to include the interaction between the navigation and G&C.

The answer to Question 1 and the above discussion of the fault tolerance do not depend on the sensor reliability. The main focus of this study is

Question 2: Is the AR&D mission failure probability sufficiently small to be acceptable?

The answer depends on the reliability of the relative sensors. It also depends on reliability improvements provided by the FT/RM architecture. Establishing probabilities of mission failures (mission abort or a mishap) requires probabilistic risk analysis (PRA), which is the main focus of this study.

The PRA must address (i) the presence of a redundant spare (backup sensor) (ii) the intermittent nature of sensor faults and possibile recovery (with a delay) in sensor fault detection logic. These problem features cause logical loops and are difficult to model with standard fault trees. A possible approach is to use a dynamical fault tree (DFT) model. The discussion in [21] indicates that there are several alternative interpretations and formulations of DFT models. This could make the approach not completely rigorous. An alternative formulation, which we use, is a continuous-time Markov chain model. Such models are used for PRA of fault tolerant computer systems with stand-by spares and component repair (reboot), e.g., see [19], [25] among many papers in this area. More examples of modeling PRA problems with logical loops using Markov chains can be found in [2], [4], [5], [17].

The main drawback of using Markov chains mentioned in [21] is exponential explosion of state dimension for complex models. This is not an issue herein. We develop simple Markov chain models for system parts. One such part is a relative navigation sensor that can experience an intermittent failure. Another such part is the sensor avionics, which host fault detection identification and recovery (FDIR) logic. The partial models are integrated taking into account interactions between the main and backup sensor and respective avionics systems.

The integrated model has just 24 states and can be built manually. It is however preferable to automate model development and integration. We integrate the models using off-the shelf software. There are several software packages, a few of them freely available, that facilitate building Markov chain models for PRA. Some of them are surveyed in [3].

The main contribution of this paper is the trade study for fault tolerant design of relative navigation system for AR&D. The trade study results are useful for design of NASA CEV spacecraft. The results are detailed in Section 5 of the paper.

The PRA approach in this paper integrates the Markov chain model of the mission from interacting, simpler sub-models. The approach and the modeling methodology detailed in the next sections could be considered as a separate contribution. The model is overviewed in Section 2 of the paper. Section 3 describes the sensor fault submodel. It presents sensor test data analysis contributing to model parameter understanding. Section 4 describes the sensor avionics submodel, including the FDIR logic. The section discusses a Monte Carlo simulation study of relative navigation used to evaluate the parameters of the avionics model.

2. MARKOV CHAIN MODEL

In this work, the system level performance of the FT/RM architecture is modeled using a continuous time Markov chain model. Since use of continuous Markov chain models in engineering analysis is not standard, below is brief background. A detailed mathematical formulation of continuous-time Markov chain models can be found in [20] among other textbooks. In a general form, the model is described by n discrete states. At time t, it can be at state k with a probability $x_k(t)$, where $\sum_k x_k(t) = 1$. The probability of transition from state j into state $k \neq j$ over an infinitesimal interval of time $[t,\ t+dt]$ is assumed to be $q_{kj}x_j(t)dt$, where $q_{kj} \geq 0$ is a constant transition rate. The probability rate of staying in the same state j is

$$q_{jj} = -\sum_{k=1,k\neq j}^{n} q_{kj}.$$

The evolution of the state vector $x(t) = [x_1(t),\ \ldots,\ x_n(t)]^T$ is given by

$$\dot{x}(t) = Qx(t) \tag{1}$$

where Q is a $n \times n$ transition matrix with entries q_{kj}. An advantage of the model (1) is that the solution can be found semi-analytically in the form

$$x(t) = \exp\left(Q(t - t_0)\right) x_0, \tag{2}$$

where $x_0 = x(t_0)$ is the initial probability distribution vector. This allows models of large size to be solved. A disadvantage is that only exponential transition probabilities are modeled.

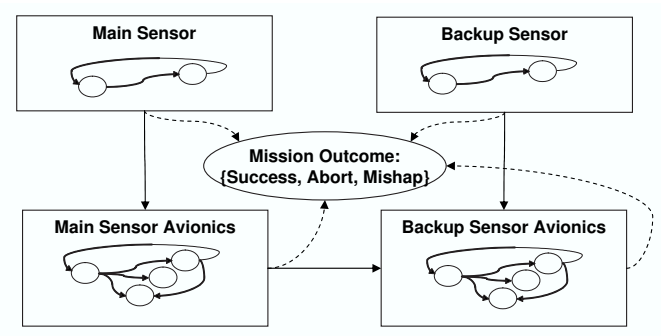


Figure 1. Overview of the PRA model

A continuous time Markov chain model for relative navigation FT/RM is build by integrating partial models, see Figure 1. The four partial models shown in Figure 1 are described in detail in the subsequent sections of the paper. The two models describe the fault condition of the main and the backup relative navigation sensor. The models describe the condition of the sensor heads and its relation with the environment condition (such as glint and lighting) that can influence the sensor performance. These two Markov chains are identical and independent.

Two more models describe the state of the avionics hardware and software for the main and the backup sensor. The FDIR algorithms are a part of the avionics software. The avionics models for the two sensors are independent and identical, with the exception of the initial state.

The arrows connecting the partial models in Figure 1 describe the dependencies between the partial models. In particular, the main sensor avionics state is influenced by the state of the sensor head for the main sensor. (The FDIR algorithms in the sensor avionics detect, or not, a fault of the sensor head). Similarly, the backup sensor avionics state is influenced by the backup sensor head state. In addition, the backup sensor avionics state is influenced by the main sensor avionics state. (The backup sensor is activated if the main sensor fails).

Figure 1 also shows schematically the mission outcome (the oval in the middle). We consider three possible mission outcomes: mission success, mission abort, and a mishap. The solution (2) of the Markov chain is calculated on a given time interval (over the duration of the docking approach). The probabilities of these outcomes are evaluated in the end of the interval. If at least one sensor head is healthy and the respective sensor avionics perform nominally, then the mission is considered a success. If both sensor heads are faulty and these faults have been detected by the avionics, then the mission is aborted. Finally, if the sensor head is faulty but the sensor avionics erroneously considers the sensor healthy (an uncovered failure), then a mishap outcome is assumed.

The partial models and their assumed parameters are discussed in detail in Sections 3 and 4 of the paper. Section 5 presents the assumed set of the model parameters and considers sensitivity of the analysis results to the parameter variations.

We used an evaluation version of Mobius package from UIUC [15] to build the model. The model is simple and could be also integrated manually (this would be more laborious, though) or by using one of several other software packages available, e.g., see the survey in [3].

3. SENSOR MODEL

Consider a model for the fault condition of a relative navigation sensor. The model is illustrated in Figure 2 and includes two states: Sensor Healthy (state #1) and Sensor Faulty (state #2). As mentioned above, these states describe environmental conditions that cause deterioration of the sensor performance, such as glint and lighting.

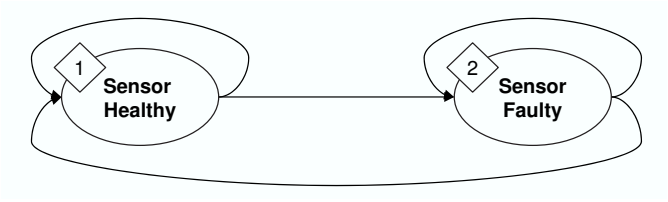


Figure 2. Markov chain model for sensor fault

The model in Figure 2 is fully described by two transition rates: the sensor failure rate q_{12} and sensor fault recovery rate q_{21}. These rates were assumed as shown in Table 1 (The Mean Time is an inverse of the Rate).

Transition (from $\rightarrow$ to state)	Rate (sec^{-1})	Mean Time
Sensor failure ($1 \rightarrow 2$)	$3 \cdot 10^{-7}$	100 h
Sensor fault recovery ($2 \rightarrow 1$)	$1 \cdot 10^{-2}$	100 s

Table 1. Sensor fault model parameters

Table 1 can be justified as follows. The sensor failure rate is based on the experience with AVGS units described in [11], [14]. No sensor failures were registered in about 1000 hours of lab and flight tests. A conservative assumption that one failure happens every 1000 hours on average yields the rate shown in the table. The assumed failure rate has a similar order of magnitude to the sensor failure rates assumed in the NASA ESAS reliability study [8] based on the relative navigation sensor failures observed in Shuttle flights.

The sensor fault recovery rate characterizes mean time the sensor is off-line because of a fault. The main sources of intermittent faults for optics-based sensors are environmental factors such as glint or lighting. The lighting conditions depend on the sun angle. For low Earth orbit with a 120 min orbital period, a 100 second time interval corresponds to a 5 degree change in the sun angle. This should provide a sufficient lighting environment change for the glint to go away. The 100 second average persistency of the fault corresponds to the sensor fault recovery rate in Table 1.

Sensor model discussion

Let us discuss the sensor failure model in more detail. An extensive program of testing several types of relative navigation sensors was carried at NASA. The tests are described in [14]. In this work we used the sensor test data to build a more detailed characterization of the faults. In the test, the target is moved with respect to the sensor, which measures the relative pose. The sensor output data are recorded along with the ground truth data obtained with an independent high-accuracy measurement system. The differences between the two measurements (residuals) can be then analyzed. At each point in time, the residual vector consists of three linear coordinate residuals and three attitude angle residuals.

The low sensor failure rate in Table 1 is ascertained by having sufficiently relaxed sensor error specifications. Tightening these specifications would lead to a higher rate of intermittent sensor faults. Having an FDIR logic and FT/RM architecture in place allows trading a higher sensors fault rate against the improvement in sensor accuracy specs. This paper analyses the tradeoffs with respect to mission risks.

The residual data for the sensor could be characterized using the empirical covariance matrix.

$$Q = \frac{1}{N-1}\sum_{j=1}^{N} r_j r_j^T \tag{3}$$

where $r_j \in \Re^6$ is the j-th residual vector and N is the number of the data points in the test set. We assume that the sensor is not biased and the residuals have zero mean. In practice, when tuning a navigation filter using the relative sensor data, the residuals (observation noise) are assumed zero-mean normally distributed. One can then characterize the residual vectors through the squared Mahalanobis distances

$$d_j^2 = r_j^T Q^{-1} r_j \tag{4}$$

For the normally distributed residuals, d_j^2 should follow χ_6^2 distribution, where 6 is the number of degrees of freedom.

We processed a set of $N = 256,412$ residual data vectors obtained in the tests. The Mahalanobis distances (4) are shown in Figure 3. By introducing a threshold (dashed line) and counting a fraction of the data points above the threshold

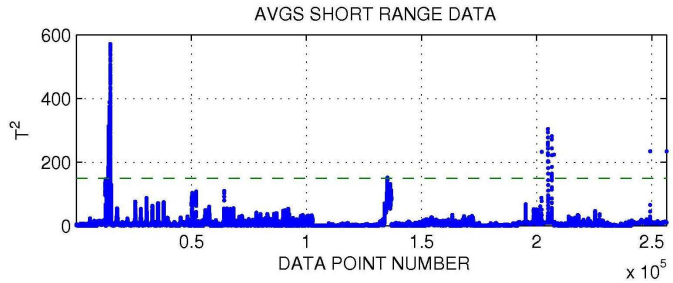


Figure 3. Sensor test data for determining outliers

we can estimate an empirical probability of the outlier. Figure 4 shows the results obtained for different thresholds (solid line) together with the cumulative probability density for χ_6^2 (dashed line).

The empirical cumulative probability distribution (solid line) in Figure 4 has heavy tail. It decays slower than the cumulative probability distribution for normally distributed residuals (dashed line). At the same time, engineering approaches to FDIR algorithm design assume a normal distribution model for outlier detection. There are two possible approaches to handling this discrepancy

1. Assume that the covariance is larger than the empirical such that all the data points are bounded by the χ_6^2 distribution envelope. Current design follows this approach. There are no outliers, but the sensor accuracy specifications are relaxed.
2. Assume the empirical covariance obtained from the data. This covariance is by a factor of 20 smaller compared to the first approach. The smaller covariance improves the accuracy of the navigation filter. At the same time, more outliers (faults) in the sensors data must be detected and removed. The drawback of the approach is that it has more reliance on the FDIR logic to handle the outliers.

The trades between the two described approaches can be evaluated by using the developed PRA framework. One model parameter that is impacted is sensor failure rate in Table 1. Another model parameter is the sensor noise covariance, which influences the FDIR-related performance probabilities discussed in the next section.

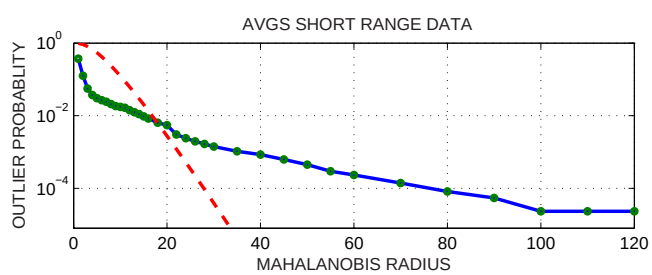


Figure 4. Sensor outlier rate vs. the accuracy threshold (solid line) and cumulative χ_6^2 distribution (dashed line)

4. AVIONICS/FDIR MODEL

Consider now a Markov chain model of the avionics states for a relative navigation sensor. Figure 5 illustrates the model for the backup sensor. The model has four states: No Fault (state #1) describes nominal operation of the sensor avionics hardware and software, Fault Detected (state #2) is a state where FDIR software suspends sensor output, Permanent Failure of the Sensor (state #3) means the avionics are permanently disabled (e.g., a CPU or power supply failure), Backup Sensor Cold (state #4) describes a power-conserving stand-by state from which the sensor could be activated.

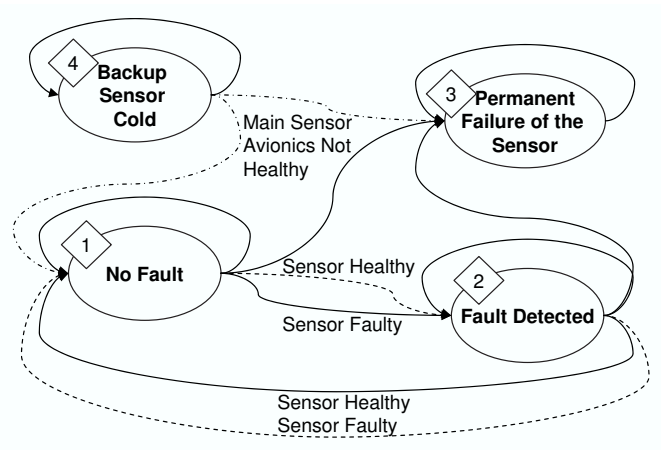


Figure 5. Markov chain model for sensor avionics

Initially the backup sensor is at state #4. From this state it can transition into two states: nominal operation state #1 (nominal activation) or permanent failure state #3 (activation attempt failed). These transitions are shown by dash-dotted lines. They are conditional on the main sensor being not healthy. If the main sensor avionics are operating nominally, then the backup sensor is kept inactive (state #4).

The model for the main sensor avionics is the same as in Figure 5, it is just assumed that the sensor is initially in No Fault state #1. Hence, the probability of being in state #4 is zero, initially and subsequently.

Table 2 shows the transition rates q_{ij} assumed for the model in Figure 5. The transitions probabilities related to hardware (first three lines in Table 2) were defined based on literature and expert evaluations. The rate of permanent avionics failure (transition between states #1 and #3) is assumed similar to what is considered in [12] for navigation system avionics. Several causes of a system failure have probabilities of a few points per a million hours each. We assumed the failure rate of 10 per million hours. The backup activation failure rate was assumed to be about three orders of magnitudes higher. This reflects the activation time being a few seconds out of the 1000 second mission, but yielding a number of failures per mission comparable with other causes. The assumed backup activation rate is an inverse of the backup activation time of 5 sec. This activation time assumes that the temperature of the backup sensor is controlled and stabilized and is mainly time needed to boot up the sensor avionics. The backup activation delay is a parameter of the trade study described in the next section and 5 sec is just one of the values considered (the nominal value).

Transition (from state $\rightarrow$ to state)	Rate (sec^{-1})	Mean Time
Avionics failure ($1 \rightarrow 3$)	$2.8 \cdot 10^{-9}$	100,000 h
Backup activation failure ($4 \rightarrow 3$)	$1 \cdot 10^{-4}$	10,000 s
Backup activation ($4 \rightarrow 1$)	0.2	5 s
Recovery for healthy sensor ($2 \rightarrow 1$)	0.1	10 s
Fault detection for faulty sensor ($1 \rightarrow 2$)	10	0.1 s
Type II error: sensor healthy, but fault detected ($1 \rightarrow 2$)	$1 \cdot 10^{-5}$	28 h
Type I error: recovery for faulty sensor ($2 \rightarrow 1$)	$2.5 \cdot 10^{-4}$	4,000 s

Table 2. Avionics fault model parameters

Transitions probabilities related to FDIR (last four lines in Table 2) were determined as a result of a Monte Carlo simulation analysis of the FDIR algorithm performance in low Earth orbit docking approach. The FDIR algorithms and the simulation scenario are described in our earlier paper [10]

FDIR model and Monte Carlo simulation

The Monte Carlo simulation was set up as follows. The chaser and target spacecraft were simulated with 6 degrees of freedom each, in low earth orbit. A visualization of the approach scenario is shown in Figure 6, and described in detail in [10]. The spacecraft pictures and error ellipses are magnified in the picture. The spacecraft dynamics were simulated as two bodies in low Earth orbit with 6 degrees of freedom each. Motion noise, sensor noise, and a proportional-integral-derivative (PID) control are simulated, with the control system using linear programming (LP) to schedule sensor firing. The simulation generated relative navigation sensor measurements. The simulation included essential components for autonomous rendezvous.

The simulated relative navigation sensor had a nominal operating rate of 5 Hz, with time jitter added to simulate potential variation in the sensor's output. It provided relative position measurements throughout the flight, and relative attitude measurements 70% of the time. The nominal noise of the relative navigation sensor and the inertial navigation system was modeled as Gaussian, with covariances equal to those expected for a typical human-rated spacecraft sensor suite. The chosen values were for a Honeywell SIGI, found in [13], [16]. Inertial navigation measurements were simulated at 100 Hz.

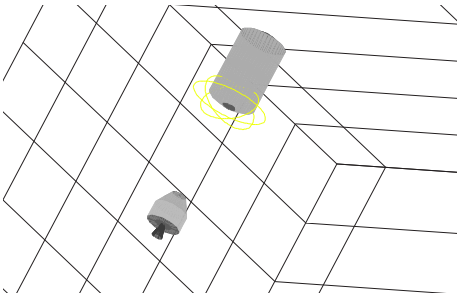


Figure 6. Visualization of R-bar approach used for Monte Carlo simulations.

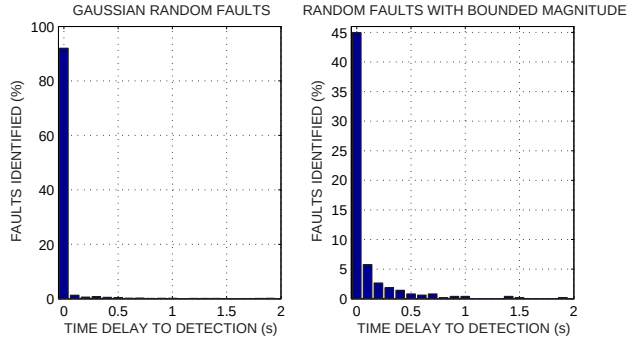


Figure 7. Time delay from fault onset to fault detection in Monte Carlo simulations of a spacecraft approach.

The simulated docking procedure mimics the R-bar approach of a chaser vehicle to the International Space Station [9]. Alternative approaches, such as those currently proposed for the Orion vehicle [6], are similar in terms of sensing requirements. The simulated approach begins at a 100 m range. The control system uses a PID controller to track the approach path, and a linear program solver to optimally fire the thrusters. The navigation system fuses inertial and relative navigation data using a multi-rate Extended Kalman Filter (EKF) as described in [24].

For the Monte Carlo analysis, 5000 random trajectories were generated, with variation in the initial cross track position, along track position, and orientation. Faults were injected at a random range with random magnitude.

Several trends were observed. The smaller the random fault magnitude, the more delay before it is detected. Regardless of fault magnitude, the expected time to detection decays monotonically after the fault onset. For smaller fault magnitudes, on the scale of the spacing of retro-reflectors on the target spacecraft, the distribution of time delays was close to exponential. The time to detection histograms for random faults with standard deviation of 0.7 m in each axis, and for faults bounded to be less than 0.6 in magnitude, are shown in Figure 7 The range at which the fault occurs is randomly generated, as are the fault magnitudes. The data shown is for faults under 0.6 m in magnitude. Although the numerical results are specific to the parameters chosen for this simulation, they provide one representative set of values for use in the avionics fault model, validate the choice of time delay models, and provide reasonable Type I and Type II error probabilities for the FDIR algorithm.

5. Analysis Results

The PRA study was carried out by running the integrated Markov chain model for a fixed interval of time and evaluating the probabilities of the three mission outcomes (success, abort, mishap) in the end. The used simulation duration of 1000 seconds is representative.

For the nominal case parameters in Table 1 and Table 2, the mission abort probability is $8.3 \cdot 10^{-3}$ and the mishap probability is $3.4 \cdot 10^{-7}$. The abort probability below 0.01 can be considered acceptable. The mission mishap probability below 10^{-4} is acceptable, cite [8]. Figure 8 shows how the system performance characterization (the two probabilities) varies when the backup sensor activation delay varies from zero (hot stand-by) to infinity (no backup sensor). The unreliability numbers (abort and mishap probabilities) stay acceptable through the range of activation delays. In particular, for the assumed model parameters the system with no backup sensor (infinite activation delay) has acceptable performance.

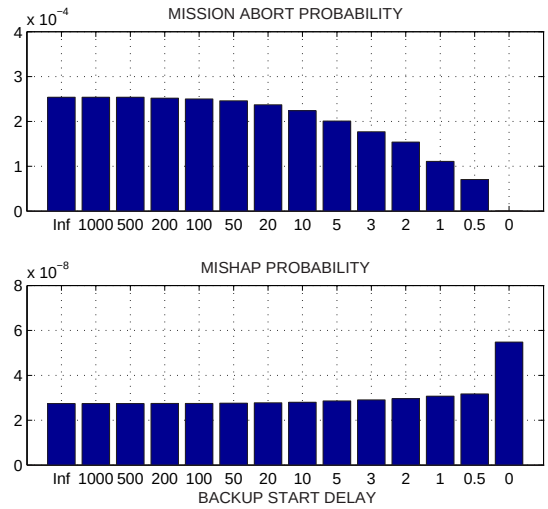


Figure 8. Nominal case results depending on the backup activation time

A sensitivity analysis was performed by varying each of the parameters in Table 2 an order of magnitude and observing the change in the system performance characterization. A strong dependence on FDIR performance parameters (which were obtained as a result of Monte Carlo study) was observed. The sensitivity to other problem parameters is relatively small. Of all FDIR parameters, the highest sensitivity is to the Type I error rate (false positive probability). The mission abort probability increases two orders of magnitude per order of magnitude increase of the Type I error rate. Changes in other parameters influence the results to a lesser extent.

The sensitivity to the FDIR parameters is high; at the same time, accuracy of computing these parameters is not very high. The FDIR parameters obtained in the Monte Carlo simulation study are sensitive to many simulation parameters which, in turn, are known only roughly. Therefore we felt compelled to consider FDIR parameters that are shifted into the unfavorable direction. Such Markov chain transition parameters for FDIR model are shown in Table 3. We will call these worst-case parameters.

Transition (from state → to state)	Rate (sec^{-1})	Mean Time
Fault detection for faulty sensor ($1 \rightarrow 2$)	0.1	10 s
Type II error: sensor healthy, but fault detected ($1 \rightarrow 2$)	$5 \cdot 10^{-4}$	2,000 s
Type I error: recovery for faulty sensor ($2 \rightarrow 1$)	0.001	1,000 s

Table 3. Worst case avionics fault model parameters

In addition to the above described results, we considered a 'worst-case' FDIR performance for parameters in Table 3. (The remaining model parameters are in Tables 1 and 2). The worst-case parameters yield mission abort probability of $2 \cdot 10^{-4}$ and the mishap probability of $2.9 \cdot 10^{-8}$. The results for different backup sensor activation delays in the worst-case parameter set are shown in Figure 9. One can observe that the mission abort probability has a knee point for backup activation delay of 20-30 s. Decreasing the activation delay below this number does not visibly improve the mishap probability.

The mishap probability decreases for large activation delay. This is somewhat counterintuitive and is because the abort probability increases much more. The mishap is caused by uncovered failures of the backup sensor. In cases when the mission is aborted because of the main sensor failure, the backup sensor is not activated and there is no chance for a mishap. Thus, the mishap probablity decreases if more faults of the main sensor are detected.

The sensitivity analysis for the worst-case data set shows little sensitivity to fault detection rate and Type II FDIR error rate (false positives). The performance could become critically bad for (i) slow FDIR recovery, and (ii) a large rate of Type I FDIR errors (false negatives). This finding provides important requirements to the FDIR algorithm design and tuning.

The overall finding is that the considered FT/RM architecture provides acceptable performance even for the worst-case parameters as long as the backup activation delay does not exceed 20-30 sec. In that case mission abort probability is less than 0.01 and mishap probability is less than 10^{-6}.

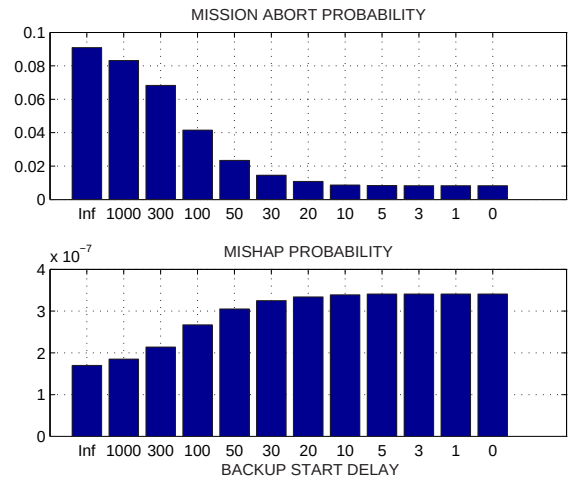


Figure 9. Worst case results depending on the backup activation time

Study limitations

The most important limitation of the above analysis results is that the abort guidance and control (G&C) logic is not considered. This is because the study focus was on the relative navigation system and the G&C logic design for CEV AR&D was not yet available at the time of this study. In fact the abort G&C logic needs to be considered in interaction with relative navigation. Our PRA model assumed that abort is always possible if a sensor is lost. In fact, this might be untrue in the immediate vicinity of the target, depending on the approach speed. The PRA model also implicitly assumed that once the backup sensor is activated it will come up on-line in time for the docking. This might be untrue in the end of the approach and depends on the G&C logic.

The reported study was necessarily limited in scope. The mentioned limitations provide possible directions of enhancing the developed PRA model and improving the analysis.

6. CONCLUSIONS

This paper presented a probabilistic risk assessment study for redundant relative navigation sensors in automated rendezvous and docking of CEV spacecraft. An architecture with a single off-line backup sensor was considered. The backup activation delay is one of the study parameters. The summary of the findings is as follows

1. The considered configuration with one active relative navigation sensor and one cold backup sensor appears to ensure an acceptable risk of mission abort or mishap for backup activation delay of 20 sec or less.
2. For the worst-case model parameters, the mission abort probability does not exceed 0.01 in the 1000 seconds of the final approach. In all studied cases the mishap probability is less than $3.5 \cdot 10^{-7}$. This is true for backup sensor activation

delay less that 20 sec. This finding does not consider abort guidance and control.

3. The results (specific probability numbers) strongly depend on the Markov chain model of the FDIR performance. (The previous conclusions assume the worst-case model.) The Monte Carlo simulation study undertaken to quantify FDIR performance parameters in the model was quite sensitive to configuration and tuning of the FDIR algorithms. This emphasizes the importance of FDIR in the overall system design.

REFERENCES

[1] D. J. Allerton and H. Jia, "A review of multisensor fusion methodologies for aircraft navigation systems," *The Journal of Navigation*, Vol. 58, 2005, pp. 405-417.

[2] P. S. Babcock, G. Rosh, and J. J. Zinchuk, "An automated environment for optimizing fault-tolerant systems design," *IEEE Annual Maintainability and Reliability Symposium*, 1991, Orlano, FL

[3] P. Buchholz, "Structured analysis techniques for large Markov Chains," *ACM Workshop on Tools for Solving Structured Markov Chains*, October 2006, Pisa, Italy

[4] R. W. Butler and S. C. Johnson, *Techniques for Modeling the Reliability of Fault-Tolerant Systems With the Markov State-Space Approach*, NASA Reference Publication 1348, September 1995.

[5] *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments*, The Ohio State University, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC 20555-0001

[6] C. D'Souza, C. Hanak, P. Spehar, F. D. Clark, and M. Jackson, "Orion Rendezvous, Proximity Operations, and Docking Design and Analysis," *AIAA GN&C Conference*, Hilton Head, SC, August 2007.

[7] S. Everett, K. Markin, P. Wroblewski, and M. Zeltser, "Design considerations for achieving MLS Category III requirements," *Proceedings of IEEE*, Vol. 77, No. 11, 1989, pp. 1752–1761.

[8] *Exploration Systems Architecture Study – Final Report*, Chapter 8. Risk and Reliability, NASA 2005, available: http://www.nasa.gov/pdf/140639main_ESAS_08.pdf

[9] W. Fehse, *Automated Rendezvous and Docking of Spacecraft*, Cambridge University Press, New York, NY, 2003.

[10] G. Hoffmann, D. Gorinevsky, R. Mah, C. Tomlin, and J. Mitchell, "Fault tolerant relative navigation using inertial and relative sensors," *AIAA GN&C Conference*, August 2007, Hilton Head, SC

[11] R.T. Howard, A.S. Johnston, T.C. Bryan, and M. L. Book, "Advanced video guidance sensor (AVGS) development testing," NASA Marshall Space Flight Center, 2004, NTRS: 2004-11-03, Document ID: 20040071003

[12] M. K. Jeerage, "Reliability analysis of fault-tolerant IMU architectures with redundant inertial sensors", *IEEE AES Magazine*, July 1990.

[13] R. Majure, "Demonstration of a ring laser gyro system for pointing and stabilization applications," *IEEE PLANS '90 – Position Location and Navigation Symposium*, Las Vegas, NV, March 1990.

[14] J. D. Mitchell, S. P. Cryan, D. Strack, L. L. Brewster, M. L. Williamson, R. T. Howard, A. S. Johnston, "Automated rendezvous and docking sensor testing at the flight robotics laboratory," *IEEE Aerospace Conference*, 3-10 March 2007

[15] *Mobius: Model based environment for validation of system reliability, availablity, security, and performance*, available: http://www.mobius.uiuc.edu/

[16] *Navigation Accelerometers: QA2000-020 Performance Specifications*, available: http://www.honeywell.com/, July 2007.

[17] M. E. Pate-Cornell and L. M. Lakats, "Organizational warning systems: a probabilistic approach to optimal design," *IEEE Trans. on Engineering Management*, Vol. 51, No. 2, 2004, pp. 183–196.

[18] M. E. Polites, "Technology of automated rendezvous and capture in space, *Journal of Spacecraft and Rockets*," Vol. 36, No. 2, 1999.

[19] V. S. Sharm and K. S. Trivedi, "Reliability and performance of component based software systems with restarts, retries, reboots and repairs," *17th Internat. Symp. on Software Reliability Engineering*, Nov. 2006

[20] L. C. G. Rogers and D. Williams, *Diffusions, Markov Processes, and Martingales. Volume 1, Foundations*, Series: Cambridge Mathematical Library, 2nd Edition, Cambridge University Press, 2000

[21] W. E. Vesely, M. Stamatelatos, J. B. Dugan, J. Fragola, J. Minarick, and J. Railsback, *Fault Tree Handbook with Aerospace Applications.*, Version 1.1. NASA Office of Safety and Mission Assurance, Washington, DC 20546 August 2002.

[22] B. K. Walker, "Performance evaluation of systems that include fault diagnostics," *Joint Automatic Control Conference*, June 1981, Charlottesville, VA

[23] S. Tamblyn, H. Hinkel, and D. Saley, "NASA CEV reference GN&C architecture," *30th Annual AAS Guidance and Control Conference*, February 3-7, 2007, Breckenridge, CO, AAS 07-071, NASA/JSC/EG: FltDyn-CEV-06-151, NASA DAA: 11564

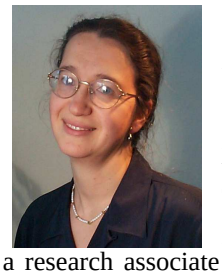
[24] S. Thrun, W. Burgard, and D. Fox, *Probabilistic Robotics*, MIT Press, Cambridge, MA, 2005.

[25] O. Yong and J.B. Dugan, "Approximate sensitivity analysis for acyclic Markov reliability models," *IEEE Transactions on Reliability*, Vol. 52, No. 2, 2003, pp. 220–230.

BIOGRAPHY

Dimitry Gorinevsky is a Consulting Professor of Electrical Engineering in Information Systems Laboratory at Stanford University and a Principal of Mitek Analytics LLC. He received a Ph.D. from Moscow (Lomonosov) University and a M.Sc. from the Moscow Institute of Physics and Technology. He held research, engineering, and academic positions in Moscow, Russia; Munich, Germany; Toronto and Vancouver, Canada. He spent 10 years with Honeywell. His interests are in decision and control systems applications across many industries. He has authored a book, more than 140 reviewed technical papers and a dozen patents. Dr. Gorinevsky is an Associate Editor of IEEE Transactions on Control Systems Technology. He is a recipient of Control Systems Technology Award, 2002, and Transactions on Control Systems Technology Outstanding Paper Award, 2004, of the IEEE Control Systems Society. He is a Fellow of IEEE.

Gabriel Hoffmann is a PhD candidate at Stanford. He is also with Mitek Analytics LLC working on NASA AR&D project. At Stanford, Gabriel develops hardware, flight software, and control laws for a fleet of quadrotor helicopter unmanned aerial vehicles (UAVs). He has been the team lead for controls systems for the Stanford Racing Team since 2004. He designed the control system that ran the autonomous unmanned vehicle Stanley, though a 132 mile race across off-road desert terrain to win DARPA Grand Challenge in 2005. He also designed the control system that ran the autonomous unmanned vehicle Junior through 56 miles of urban terrain to place second in the DARPA Urban Challenge. Gabriel interned at Boeing Space Systems, Houston, working on the International Space Station. He interned at the NASA Ames Academy in 2001.



Marina Shmakova is working on modeling and analysis of fault tolerant systems with Mitek Analytics LLC. She is also a Staff Scientist at Physics Department of Stanford University. She worked on analysis of Hubble Space Telescope data including the attitude and pointing data and observational data. As a research associate at Stanford Linear Accelerator Center, Dr. Shmakova worked on different aspects of astrophysics and high energy physics. She has Ph.D. and in MS in Physics from University of Tennessee.

Robert Mah is a Senior Scientist in Intelligent Systems Division at NASA Ames Research Center (ARC). He received a Ph.D. in Applied Mechanics and M.S. in Mechanical Engineering from Stanford University in 1988 and 1976. He has led and managed NASA projects and groups for more than 30 years. He is a recipient of many NASA awards including NASA Exceptional Achievement Medal, three Space Act awards, several awards for Technology Transfer and Commercialization, Spacecraft Docking Simulation Award, and several others. He published a few dozen papers and has several patents received and pending. He was a keynote or invited speaker at many international and NASA conferences; his work was featured in the media. Dr. Mah is NASA ARC Representative on ORION Flight Performance SIG. He currently is a Project Scientist for Integrated Vehicle Health Management project in NASA Aviation Safety Program.

Scott Cryan received BS Aerospace Engineering from University of Buffalo in 1988. Since then, he has been working Space Shuttle and International Space Station GPS receivers. In addition to the GPS receiver role on Space Shuttle and ISS, he had been working on GPS receivers for several projects at NASA JSC. Recently, Mr. Cryan has been investigating relative navigation sensor performance via testing and analyses with open loop simulations. Currently, Mr. Cryan is the relative navigation subsystem manager for the CEV Project at NASA-JSC.

Jennifer Mitchell is the Crew Exploration Vehicle Flight Dynamics Deputy Functional Area Manager at NASAs Johnson Space Center and also serves as the Project Manager for the Exploration Systems Technology Development Automated Rendezvous and Docking Sensor Technology Project. She has supported guidance, navigation and control system development and testing for the Autonomous Extravehicular Robotic Camera (AERCam), the International Space Station, and the X-38 Crew Return Vehicles Space Integrated Global Positioning System / Inertial Navigation System. She has a BS in Aerospace Engineering from Texas A&M University.