Mission Failure Probability Calculations for Critical Function Mechanizations in the Automated Highway System

Eushiuan Tran
Philip Koopman
Carnegie Mellon University
Pittsburgh, Pennsylvania

Robotics Institute Technical Report
CMU-RI-TR-97-44
December 16, 1997

Abstract

Reliability analysis is an important part of the Automated Highway System (AHS) research and development. In 1994, Honeywell released the “Malfunction Management Activity Area Report for AHS Health Management Precursor System Analysis” which showed a reliability analysis of the AHS vehicle system. However, the Honeywell report does not describe in detail how they arrived at their answers. In this paper, we will be providing a more detailed analysis of how Honeywell arrived at the probability of failure vs. time plots for both the different subsystems in an AHS vehicle and the overall system. Matlab programs were written to calculate system reliabilities for series and parallel systems. In performing the analysis, there were several places as stated in the paper where our answers differed from Honeywell’s answers. Because of these differences, our results and conclusions are different from Honeywell’s results and conclusions. Based on a 95% test coverage and a system failure rate limit of 1 x 10^{-6} failures per mission, Honeywell determined that triplex redundancy for all subsystems is necessary to meet these requirements. However, for the purposes of our study, and assuming 100% test coverage and also a system failure rate limit of 1 x 10^{-6} failures per mission, we determined that duplex redundancy will result in a mission time of 3.5 hours, which is still satisfactory.

Introduction

In November of 1994, Honeywell released the “Malfunction Management Activity Area Report for AHS Health Management Precursor System Analysis.” (FHWA-RD-95-047 Nov 95 US Department of Transportation, Federal Highway Administration) A major part of this report includes mission failure calculations for different critical function mechanizations. The critical functions in an AHS vehicle have been sub-divided into subsystems to simplify the task of deriving mechanizations: steering, braking, sensors, engine, processing, communication, and displays and controls. Safety diagrams and probability of failure vs. time(hrs) are shown for each mechanization.

The Honeywell report does not describe in detail how they arrived at their answers. The plots are also too small to make accurate readings. In this report, we will illustrate how the data was calculated and show more detailed plots. Several of our plots are different from the ones in the Honeywell report. These are Figures 15, 28, 34, 40, and 44. (as numbered in the Honeywell report.)

We created a small tool kit to compute the reliability of the automotive subsystems using parallel/serial diagrams. The coding is done in Matlab. We have used these tools to generate and compare our automated computations against the results of the report.

In this paper, we will first outline the basic reliability theory that we used for our calculations. Next, we will present the probability of failure vs. time plots for each of the subsystems in an AHS vehicle. After that, we have proposed four possible systems for an AHS vehicle. Finally, we will conclude with interpretations of what the numbers mean. The appendix shows a sample of the programs written.

Basic Reliability Theory

Reliability is the probability of a component, or system, functioning correctly over a given period of time under a given set of operating conditions. Related to the reliability of a component is the rate at which such devices fail. The failure rate λ of a device is the number of failures in a given period of time. From experience, it has been shown that the failure rate of electronic components follow the characteristics of a bathtub curve. Initially, components exhibit high “infant mortality” due to the presence of manufacturing faults that were not detected during the testing stage of the manufacture. As time passes, the number of components containing defects diminishes and the failure rate drops to a fairly constant level. At a later time, the failure rate increases as the component “wears out.” Manufacturers usually aim to use the components only during the useful life period during which the failure rate is constant. It can be shown that during this useful life stage, the failure rate is related to the reliability of the device through the following expression:

$$R(t) = e^{-\lambda \cdot t}$$

This exponential relationship between reliability and time is known as the exponential failure law. For a constant failure rate, the reliability falls exponentially with time.

During the design stage, it is important to be able to compute the reliability of a system containing different components. Combinational reliability models allow the reliability of a system to be calculated from the reliability of its component parts. This model distinguishes between two situations: first, where the failure of any one of a number of components will cause system failure, and second, where only the failure of several components simultaneously will cause a malfunction. These two situations can be modeled by series and parallel models respectively.

In a series system, if $R_i(t)$ is the reliability of the ith component in the system, then the overall system reliability is given by the following expression:

$$R(t) = \prod_{i=1}^{n} R_i(t)$$

In a parallel system, if $R_i(t)$ is the reliability of the ith component in the system, then the overall system reliability is given by the following expression:

$$R(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t))$$

Probability of Failure vs. Time Plots

Honeywell assumed that the overall AHS probability of failure must be less than 1 x 10^{-6} in their probability of failure plots. Based on this, they have calculated probabilities for both duplex and triplex modular redundancy in most of the subsystems. In the following plots, all assumptions are as specified in the Honeywell report. All subsystem and system reliabilities are calculated using the series and parallel reliability equations.

Steering

Three mechanizations are demonstrated for the steering subsystem. The safety diagram for the first subsystem is shown in Figure 1. Figure 2 shows the Matlab plot and Table 1 shows the data used to generate the Matlab plots.

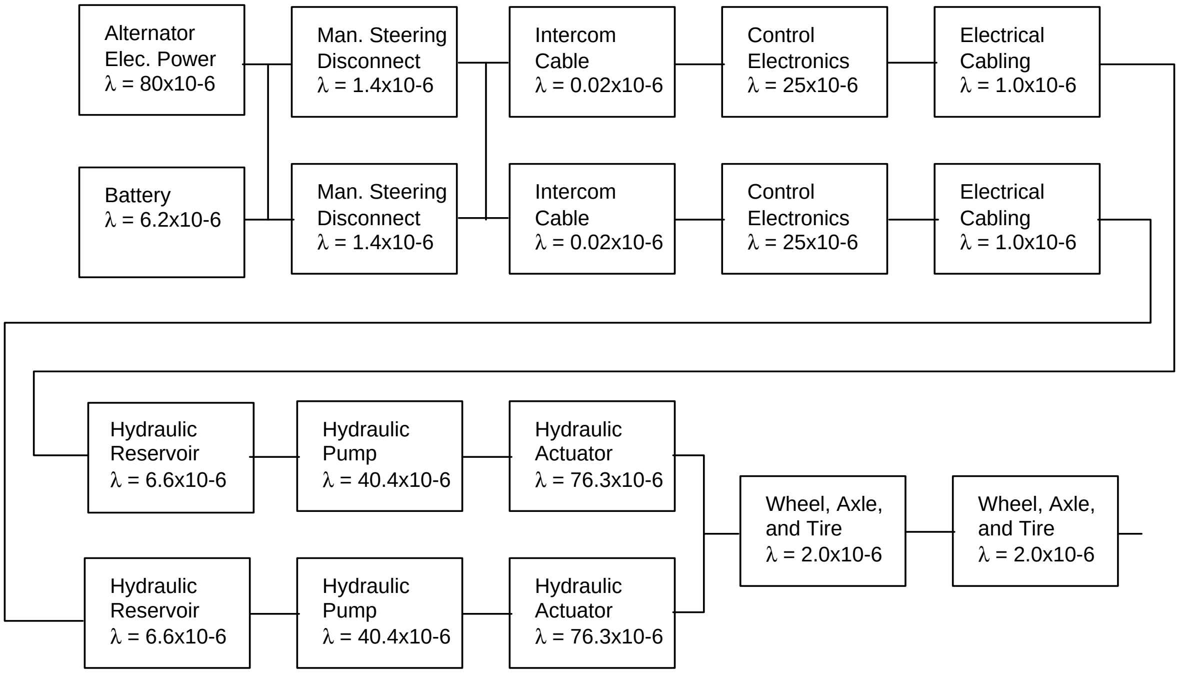
Alternator Elec. Power λ = 80x10-6
Man. Steering Disconnect λ = 1.4x10-6
Intercom Cable λ = 0.02x10-6
Control Electronics λ = 25x10-6
Electrical Cabling λ = 1.0x10-6
Battery λ = 6.2x10-6
Man. Steering Disconnect λ = 1.4x10-6
Intercom Cable λ = 0.02x10-6
Control Electronics λ = 25x10-6
Electrical Cabling λ = 1.0x10-6
Hydraulic Reservoir λ = 6.6x10-6
Hydraulic Pump λ = 40.4x10-6
Hydraulic Actuator λ = 76.3x10-6
Wheel, Axle, and Tire λ = 2.0x10-6
Wheel, Axle, and Tire λ = 2.0x10-6
Hydraulic Reservoir λ = 6.6x10-6
Hydraulic Pump λ = 40.4x10-6
Hydraulic Actuator λ = 76.3x10-6

Figure 1: Dual Redundant Steering Safety Diagram Compared to Honeywell Figure 14

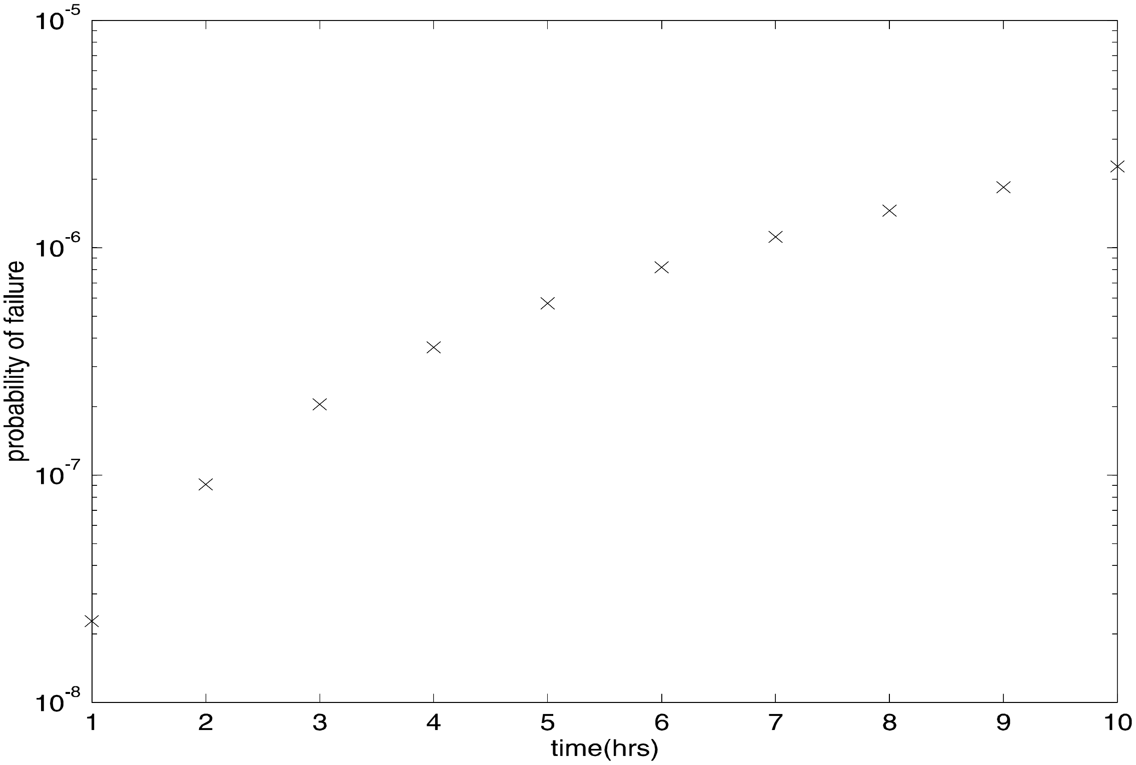

Figure 2: Probability of Failure vs. Time for Dual Redundant Steering Subsystem Compared to Honeywell Figure 15 (Different)

Table 1: Dual Redundant Steering Subsystem

Time(hrs)	Probability
1	2.2791e-08
2	9.1151e-08
3	2.0506e-07
4	3.6450e-07
5	5.6944e-07
6	8.1988e-07
7	1.1158e-06
8	1.4571e-06
9	1.8439e-06
10	2.2761e-06

To be consistent with assumptions from the Honeywell report, the wheel, axle, and tire failure rate is not included. This is because if it were, the probability of failure for a single wheel, axle, and tire combination would exceed the entire AHS budget.

Figure 3 shows the safety diagram for the second steering mechanization. It shows a partially triply redundant system with the power supply and steering wheel clutch remaining dual redundant. The Matlab plot is shown in Figure 4 and Table 2 contains the data.

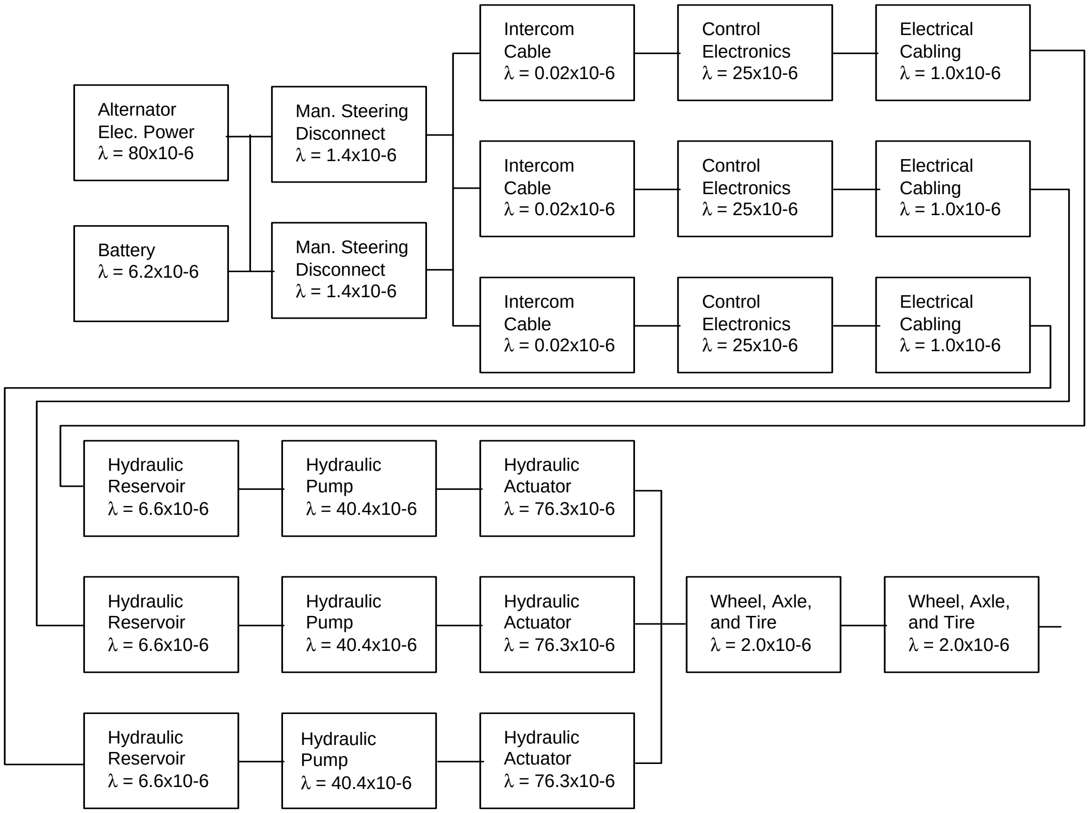
Alternator Elec. Power λ = 80x10-6
Battery λ = 6.2x10-6
Man. Steering Disconnect λ = 1.4x10-6
Man. Steering Disconnect λ = 1.4x10-6
Intercom Cable λ = 0.02x10-6
Control Electronics λ = 25x10-6
Electrical Cabling λ = 1.0x10-6
Intercom Cable λ = 0.02x10-6
Control Electronics λ = 25x10-6
Electrical Cabling λ = 1.0x10-6
Intercom Cable λ = 0.02x10-6
Control Electronics λ = 25x10-6
Electrical Cabling λ = 1.0x10-6
Hydraulic Reservoir λ = 6.6x10-6
Hydraulic Pump λ = 40.4x10-6
Hydraulic Actuator λ = 76.3x10-6
Hydraulic Reservoir λ = 6.6x10-6
Hydraulic Pump λ = 40.4x10-6
Hydraulic Actuator λ = 76.3x10-6
Wheel, Axle, and Tire λ = 2.0x10-6
Wheel, Axle, and Tire λ = 2.0x10-6
Hydraulic Reservoir λ = 6.6x10-6
Hydraulic Pump λ = 40.4x10-6
Hydraulic Actuator λ = 76.3x10-6

Figure 3: Partial Triple Redundant Steering Safety Diagram Compared to Honeywell Figure 17

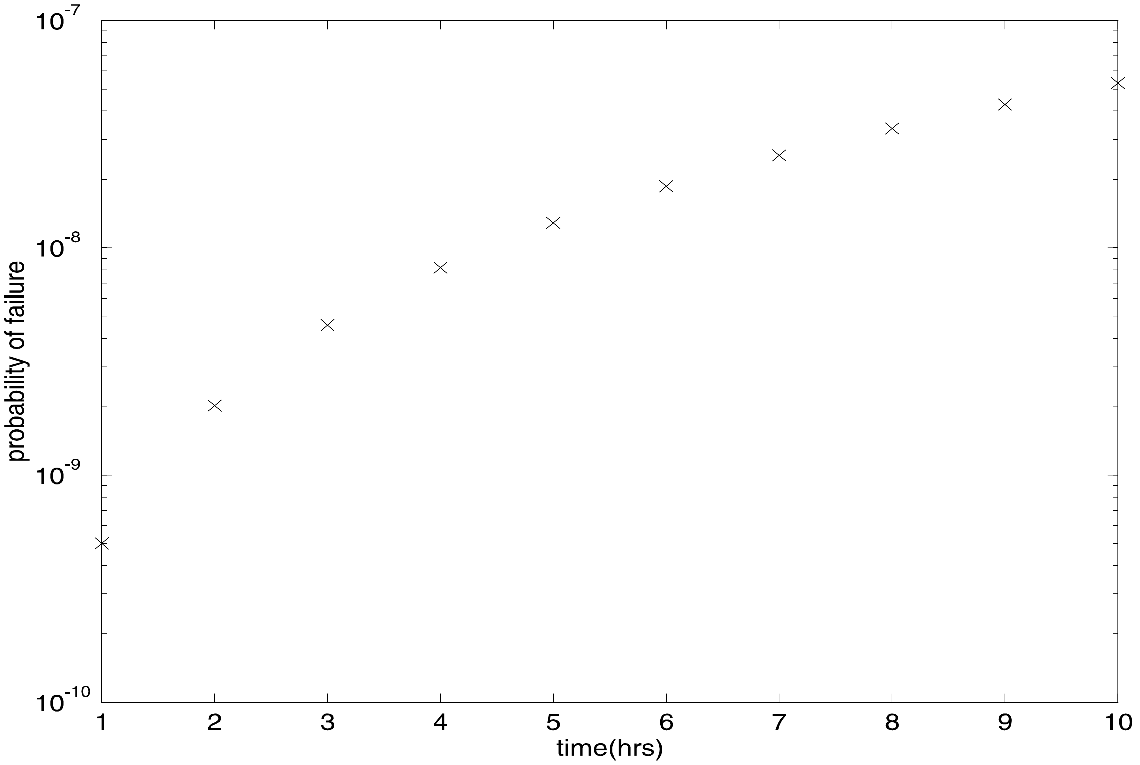

Figure 4: Probability of Failure vs. Time for Partial Redundant Steering Subsystem Compared to Honeywell Figure 18

Table 2: Partial Triple Redundant Steering Subsystem

Time(hrs)	Probability
1	5.0127e-10
2	2.0183e-09
3	4.5709e-09
4	8.1789e-09
5	1.2862e-08
6	1.8640e-08
7	2.5533e-08
8	3.3560e-08
9	4.2741e-08
10	5.3096e-08

In order to improve reliability, full triplex redundancy is illustrated in Figures 5 and 6 and Table 3.

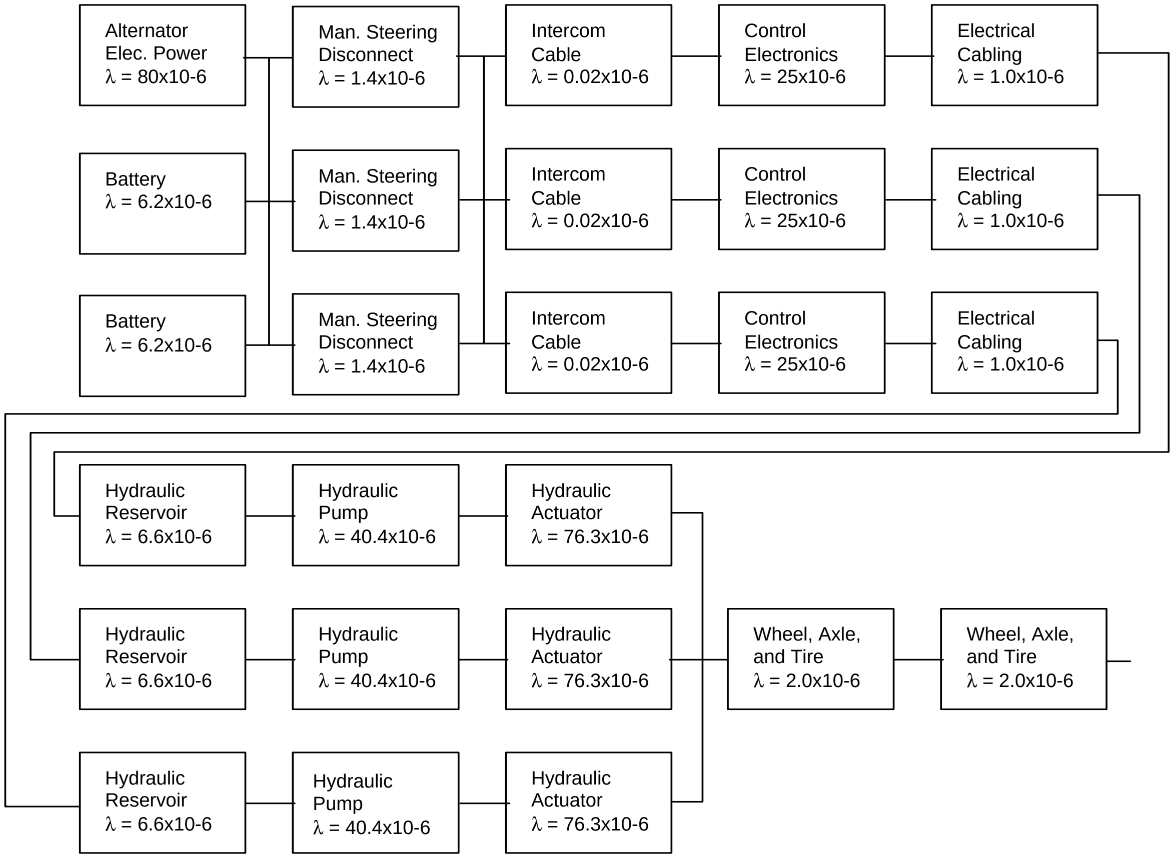

Figure 5: Full Triple Redundant Steering Safety Diagram Compared to Honeywell Figure 20

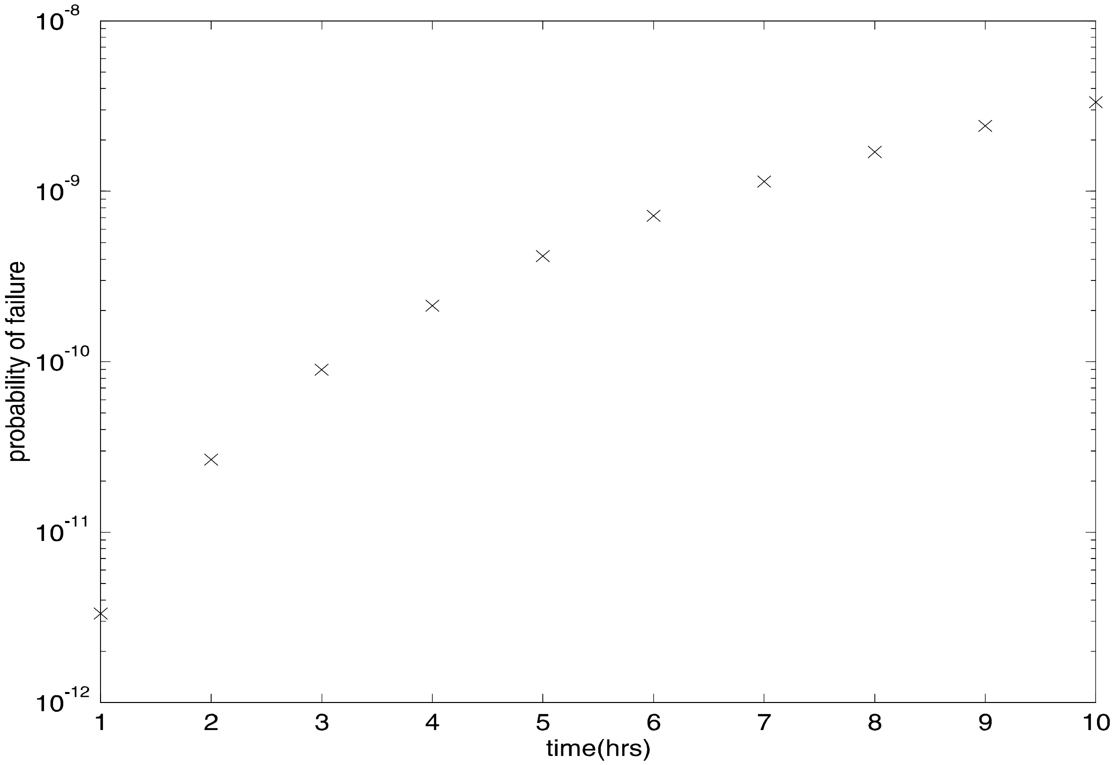

Figure 6: Probability of Failure vs. Time for Full Triple Redundant Steering Subsystem Compared to Honeywell Figure 21

Table 3: Full Triple Redundant Steering Subsystem

Time(hrs)	Probability
1	3.3317e-12
2	2.6647e-11
3	8.9914e-11
4	2.1308e-10
5	4.1608e-10
6	7.1883e-10
7	1.1412e-09
8	1.7031e-09
9	2.4244e-09
10	3.3249e-09

Braking

There are two mechanizations for the braking subsystem. Figures 7 and 8 and Table 4 illustrate dual redundancy.

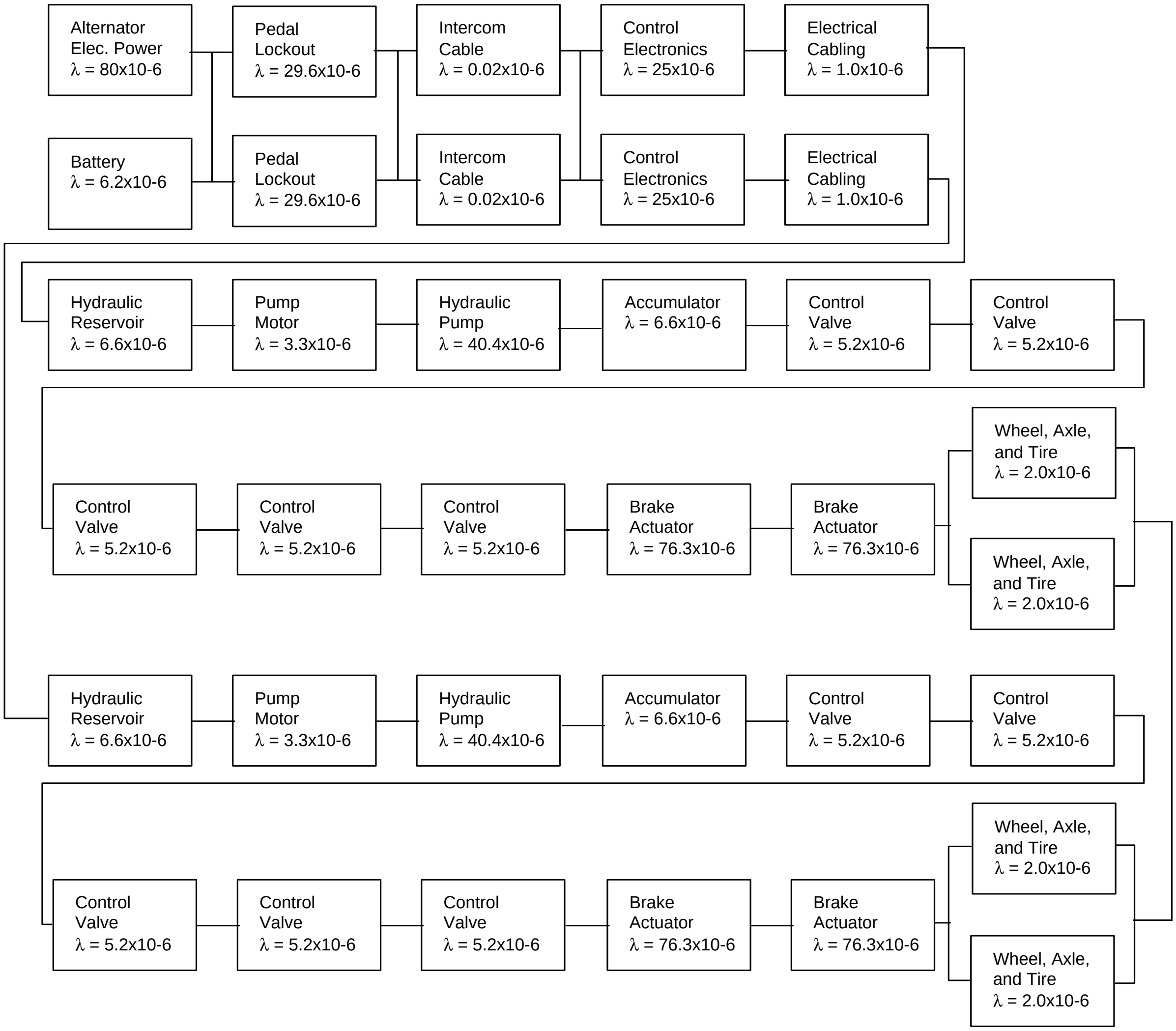
Alternator Elec. Power λ = 80x10-6
Pedal Lockout λ = 29.6x10-6
Intercom Cable λ = 0.02x10-6
Control Electronics λ = 25x10-6
Electrical Cabling λ = 1.0x10-6
Battery λ = 6.2x10-6
Pedal Lockout λ = 29.6x10-6
Intercom Cable λ = 0.02x10-6
Control Electronics λ = 25x10-6
Electrical Cabling λ = 1.0x10-6
Hydraulic Reservoir λ = 6.6x10-6
Pump Motor λ = 3.3x10-6
Hydraulic Pump λ = 40.4x10-6
Accumulator λ = 6.6x10-6
Control Valve λ = 5.2x10-6
Control Valve λ = 5.2x10-6
Wheel, Axle, and Tire λ = 2.0x10-6
Control Valve λ = 5.2x10-6
Control Valve λ = 5.2x10-6
Control Valve λ = 5.2x10-6
Brake Actuator λ = 76.3x10-6
Brake Actuator λ = 76.3x10-6
Wheel, Axle, and Tire λ = 2.0x10-6
Hydraulic Reservoir λ = 6.6x10-6
Pump Motor λ = 3.3x10-6
Hydraulic Pump λ = 40.4x10-6
Accumulator λ = 6.6x10-6
Control Valve λ = 5.2x10-6
Control Valve λ = 5.2x10-6
Wheel, Axle, and Tire λ = 2.0x10-6
Control Valve λ = 5.2x10-6
Control Valve λ = 5.2x10-6
Control Valve λ = 5.2x10-6
Brake Actuator λ = 76.3x10-6
Brake Actuator λ = 76.3x10-6
Wheel, Axle, and Tire λ = 2.0x10-6

Figure 7: Dual Redundant Brake Safety Diagram Compared to Honeywell Figure 24

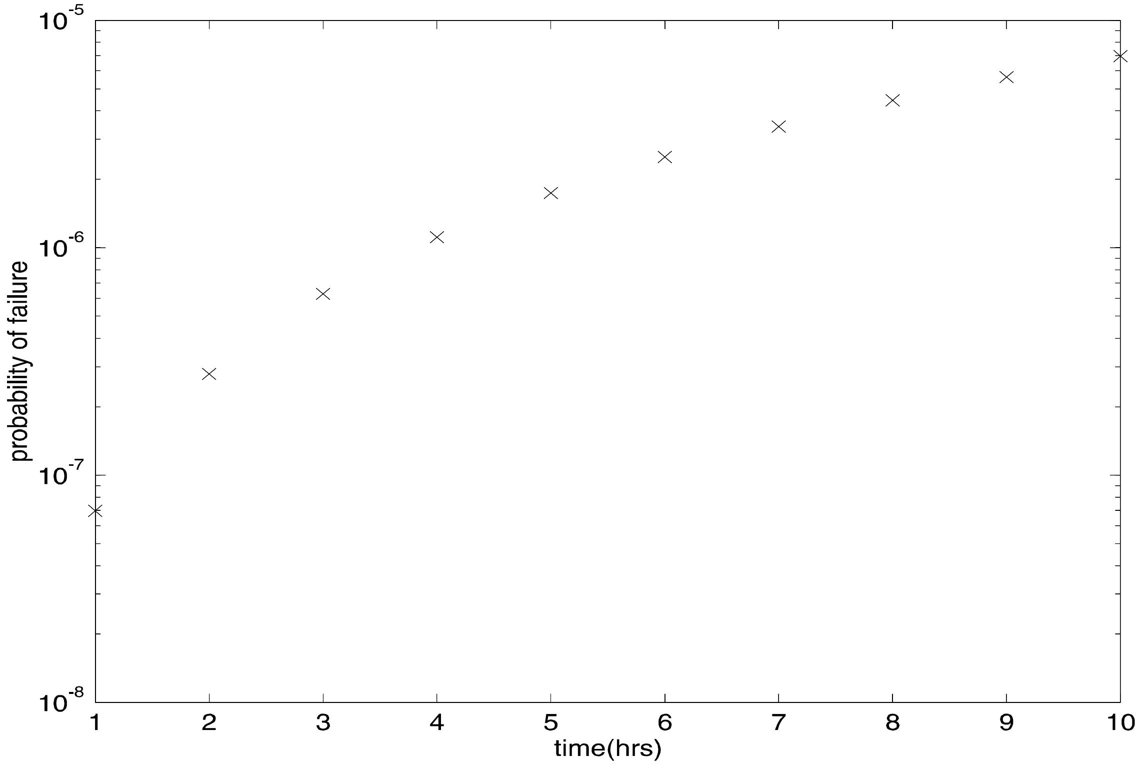

Figure 8: Probability of Failure vs. Time for Dual Redundant Brake Subsystem Compared to Honeywell Figure 25

Table 4: Dual Redundant Brake Subsystem

Time(hrs)	Probability
1	6.9736e-08
2	2.7887e-07
3	6.2731e-07
4	1.1149e-06
5	1.7416e-06
6	2.5073e-06
7	3.4118e-06
8	4.4551e-06
9	5.6371e-06
10	6.9575e-06

Figure 9 and 10 and Table 5 show a triple redundant braking system, with individual actuators for each wheel.

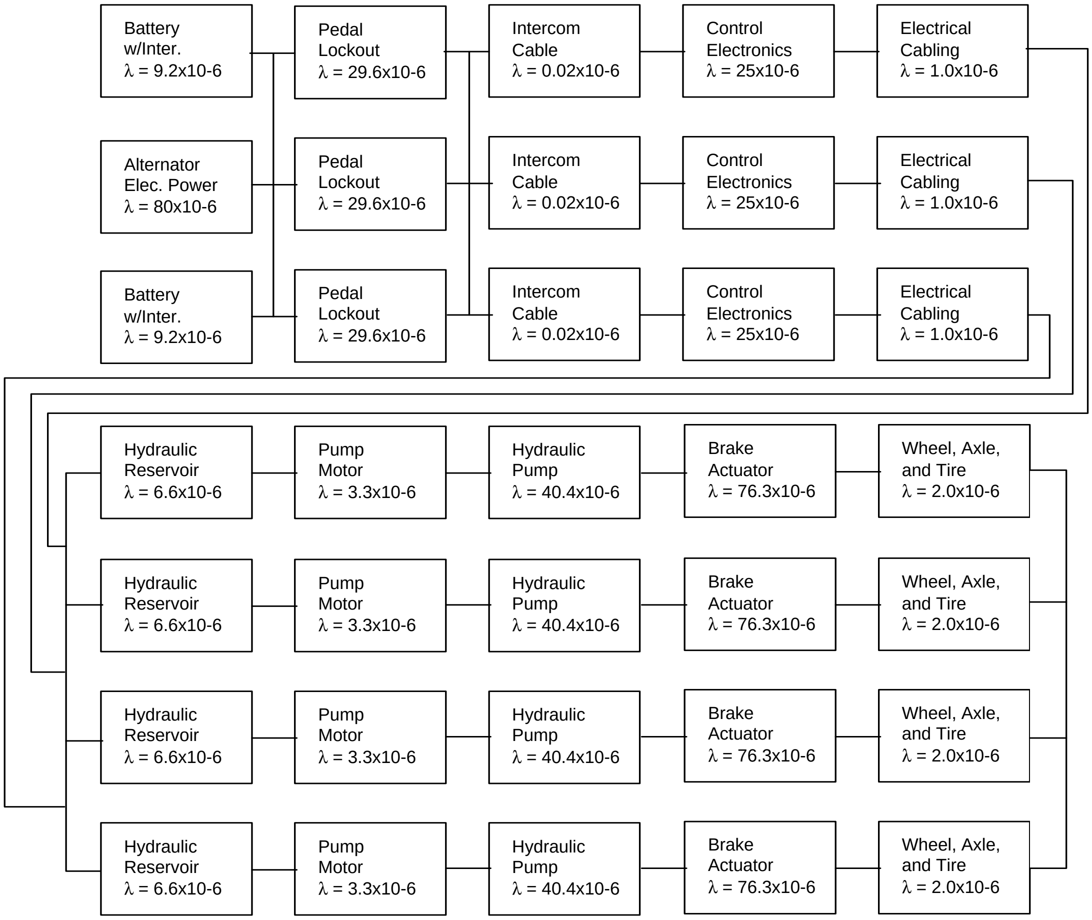
Battery w/Inter. λ = 9.2x10-6
Pedal Lockout λ = 29.6x10-6
Intercom Cable λ = 0.02x10-6
Control Electronics λ = 25x10-6
Electrical Cabling λ = 1.0x10-6
Alternator Elec. Power λ = 80x10-6
Pedal Lockout λ = 29.6x10-6
Intercom Cable λ = 0.02x10-6
Control Electronics λ = 25x10-6
Electrical Cabling λ = 1.0x10-6
Battery w/Inter. λ = 9.2x10-6
Pedal Lockout λ = 29.6x10-6
Intercom Cable λ = 0.02x10-6
Control Electronics λ = 25x10-6
Electrical Cabling λ = 1.0x10-6
Hydraulic Reservoir λ = 6.6x10-6
Pump Motor λ = 3.3x10-6
Hydraulic Pump λ = 40.4x10-6
Brake Actuator λ = 76.3x10-6
Wheel, Axle, and Tire λ = 2.0x10-6
Hydraulic Reservoir λ = 6.6x10-6
Pump Motor λ = 3.3x10-6
Hydraulic Pump λ = 40.4x10-6
Brake Actuator λ = 76.3x10-6
Wheel, Axle, and Tire λ = 2.0x10-6
Hydraulic Reservoir λ = 6.6x10-6
Pump Motor λ = 3.3x10-6
Hydraulic Pump λ = 40.4x10-6
Brake Actuator λ = 76.3x10-6
Wheel, Axle, and Tire λ = 2.0x10-6
Hydraulic Reservoir λ = 6.6x10-6
Pump Motor λ = 3.3x10-6
Hydraulic Pump λ = 40.4x10-6
Brake Actuator λ = 76.3x10-6
Wheel, Axle, and Tire λ = 2.0x10-6

Figure 9: Multi-string Brake Safety Diagram Compared to Honeywell Figure 27

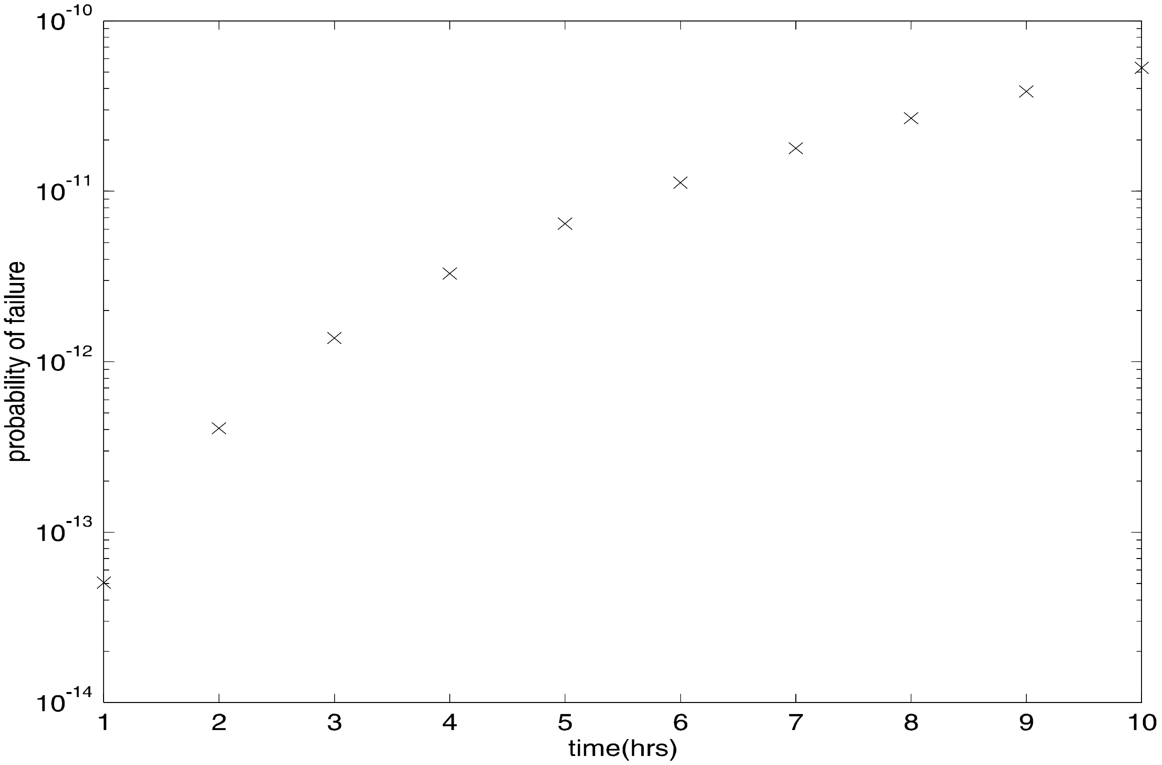

Figure 10: Probability of Failure vs. Time for Multi-string Brake Subsystem Compared to Honeywell Figure 28 (Different)

Table 5: Multi-string Brake Subsystem

Time(hrs)	Probability
1	5.0626e-14
2	4.0690e-13
3	1.3806e-12
4	3.2900e-12
5	6.4597e-12
6	1.1221e-11
7	1.7911e-11
8	2.6874e-11
9	3.8461e-11
10	5.3028e-11

Sensors: Object Detection, Lateral Position/Roadway Data, Gyros and Accelerometers

Figures 11 and 12 and Table 6 illustrates the dual object detection subsystem.

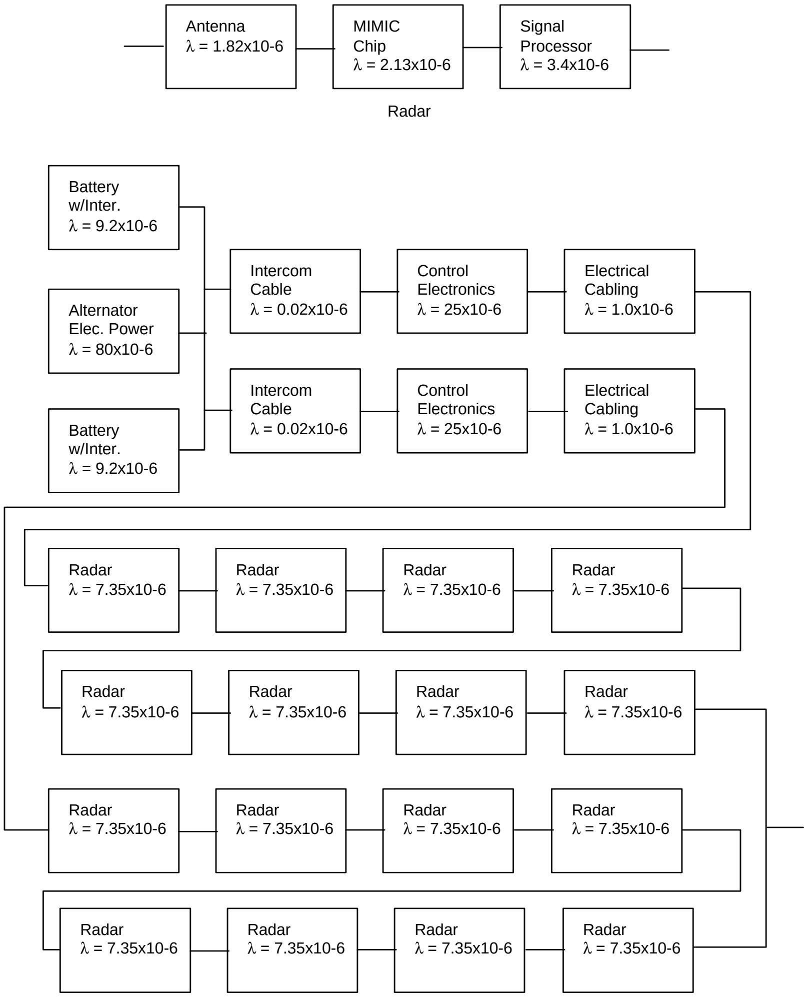

Figure 11: Dual Object Detection Safety Diagram Compared to Honeywell Figure 31

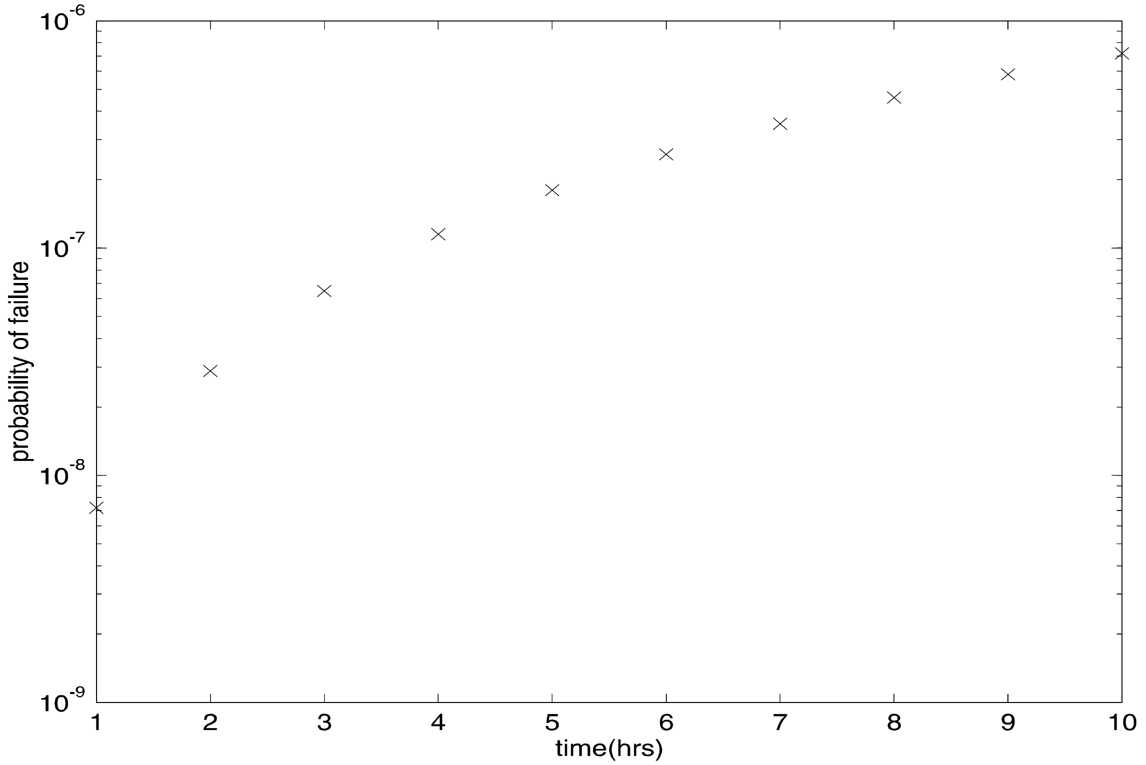

Figure 12: Probability of Failure vs. Time for Dual Object Detection Subsystem Compared to Honeywell Figure 32

Table 6: Dual Object Detection Subsystem

Time(hrs)	Probability
1	7.1938e-09
2	2.8773e-08
3	6.4734e-08
4	1.1507e-07
5	1.7979e-07
6	2.5887e-07
7	3.5232e-07
8	4.6013e-07
9	5.8231e-07
10	7.1884e-07

Triple object detection is demonstrated in Figures 13 and 14 and Table 7.

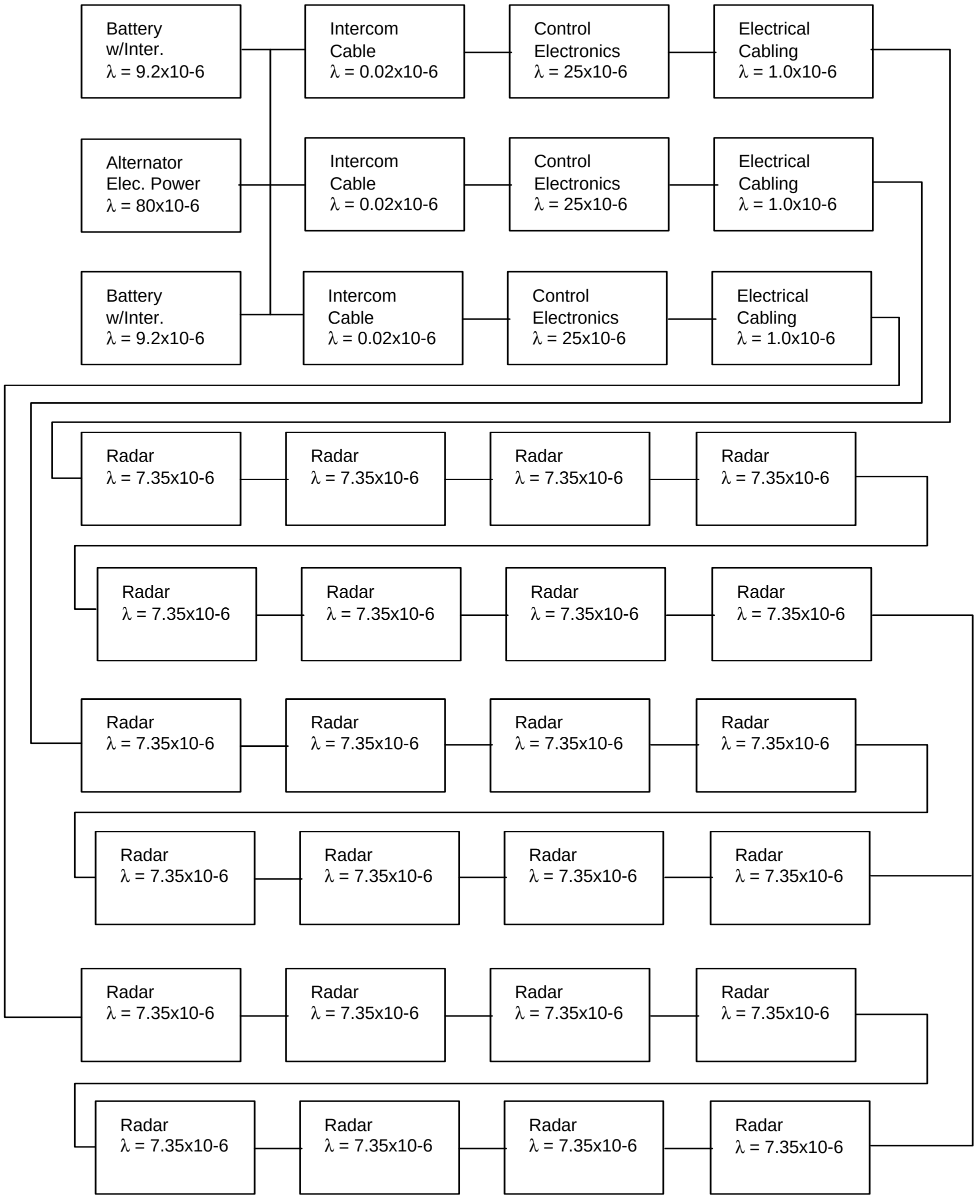

Figure 13: Triple Object Detection Safety Diagram Compared to Honeywell Figure 33

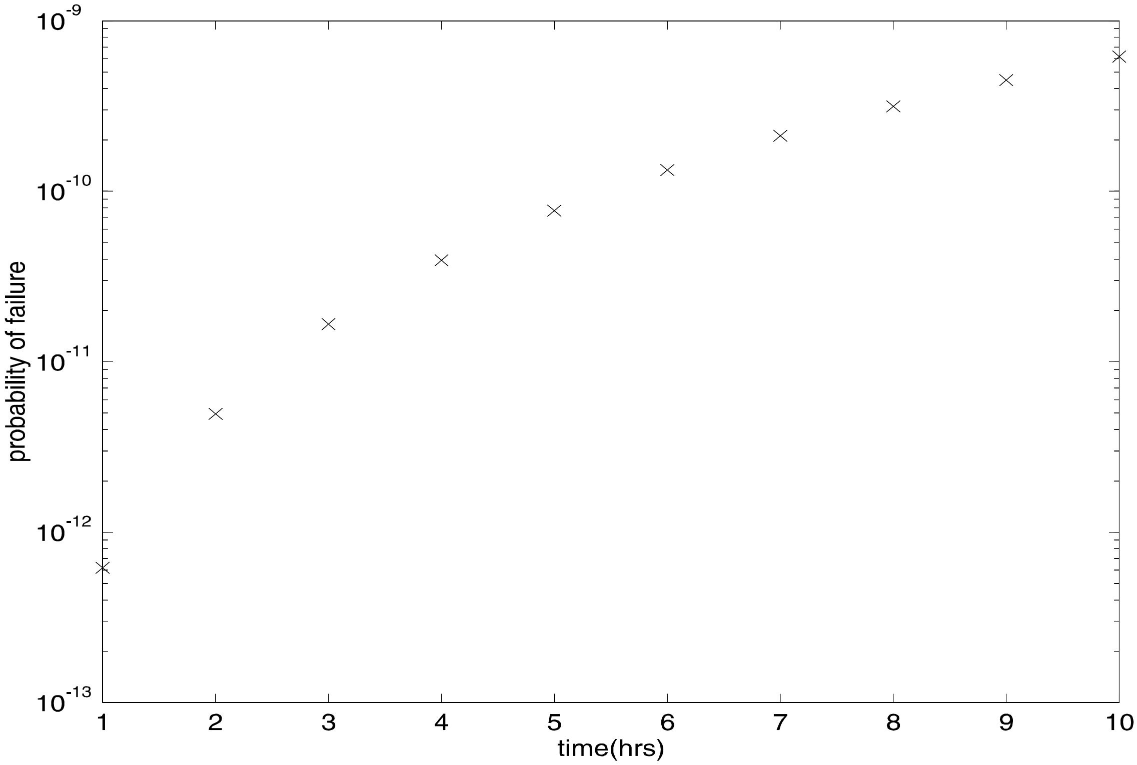

Figure 14: Probability of Failure vs. Time for Triple Object Detection Subsystem Compared to Honeywell Figure 34 (Different)

Table 7: Triple Object Detection Subsystem

Time(hrs)	Probability
1	6.1695e-13
2	4.9348e-12
3	1.6653e-11
4	3.9468e-11
5	7.7077e-11
6	1.3317e-10
7	2.1144e-10
8	3.1559e-10
9	4.4928e-10
10	6.1622e-10

The dual processor subsystem is shown in Figures 15 and 16 and Table 8.

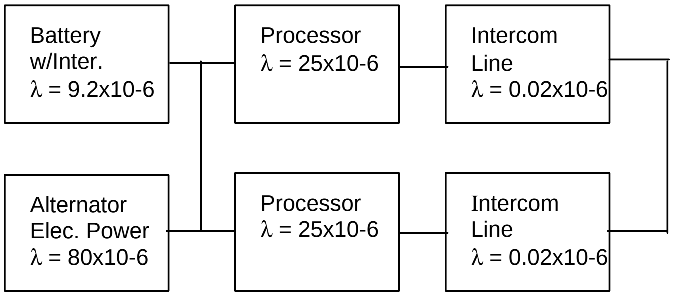

Figure 15: Dual Processor Safety Diagram

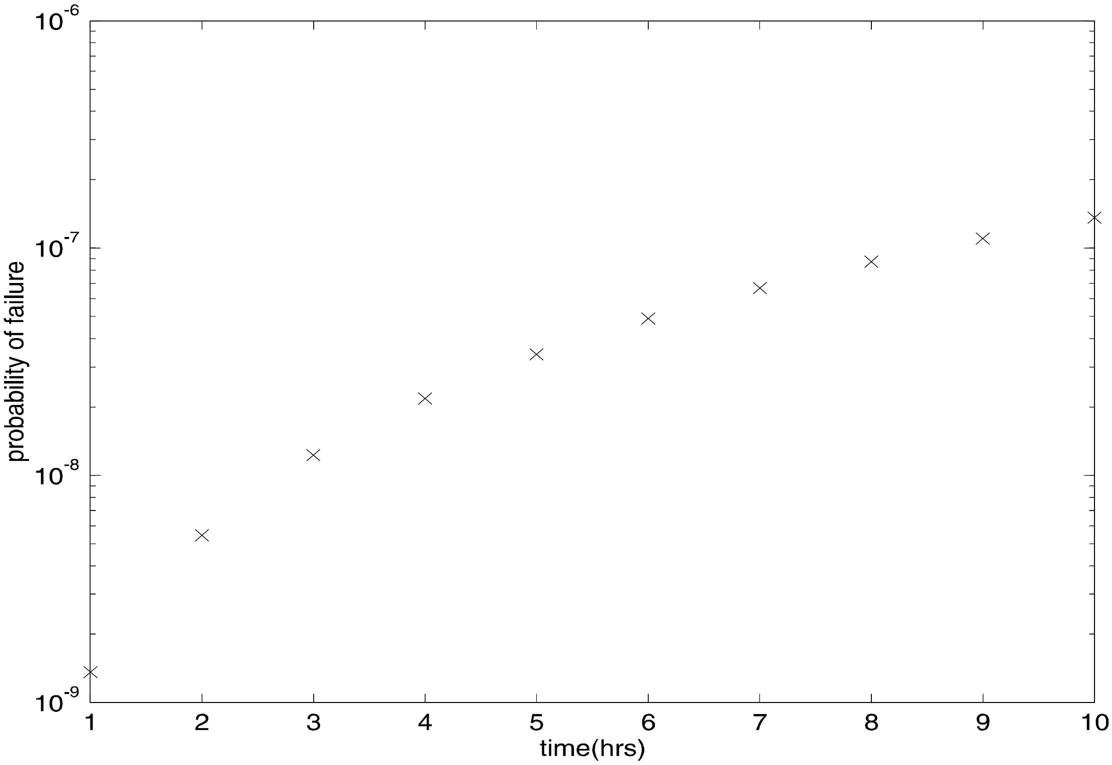

Figure 16: Probability of Failure vs. Time for Dual Processor Subsystem

Table 8: Dual Processor Subsystem

Time(hrs)	Probability
1	1.3620e-09
2	5.4476e-09
3	1.2257e-08
4	2.1789e-08
5	3.4044e-08
6	4.9022e-08
7	6.6721e-08
8	8.7143e-08
9	1.1029e-07
10	1.3615e-07

The triple processor subsystem is shown in Figures 17 and 18 and Table 9.

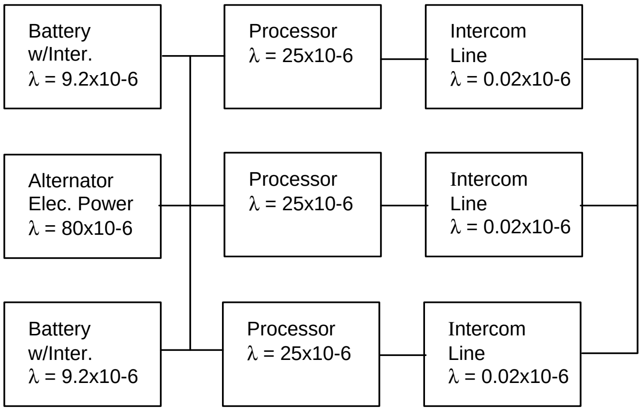

Figure 17: Triple Processor Safety Diagram Compared to Honeywell Figure 39

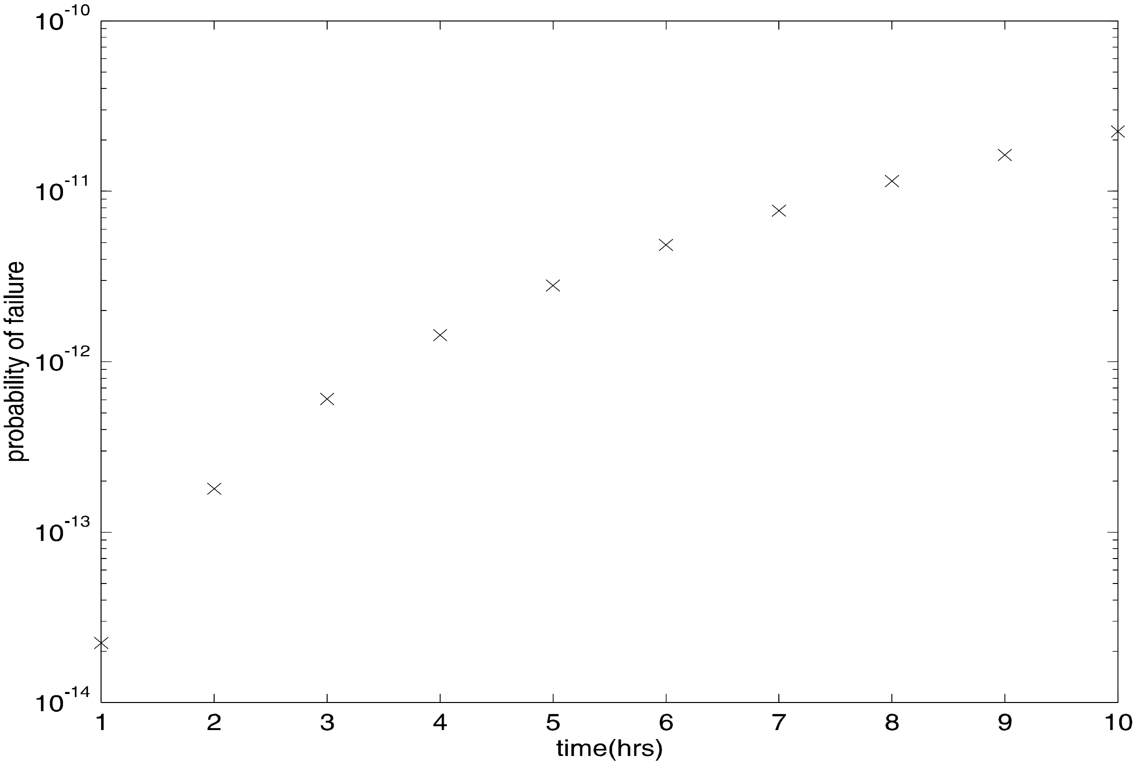

Figure 18: Probability of Failure vs. Time for Triple Processor Subsystem Compared to Honeywell Figure 40 (Different)

Table 9: Triple Processor Subsystem

Time(hrs)	Probability
1	2.2427e-14
2	1.7952e-13
3	6.0563e-13
4	1.4355e-12
5	2.8036e-12
6	4.8445e-12
7	7.6925e-12
8	1.1482e-11
9	1.6348e-11
10	2.2425e-11

Communications

The dual communications subsystem is shown in Figures 19 and 20 and Table 10.

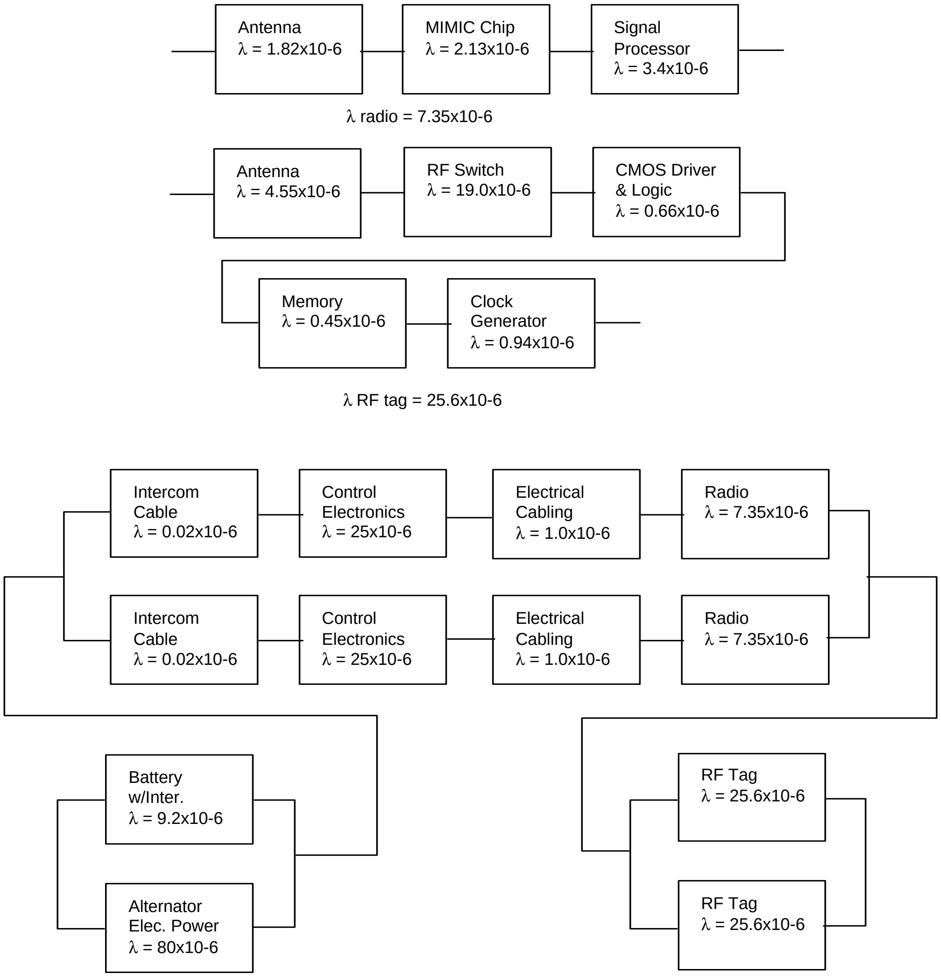

Figure 19: Dual Communications Safety Diagram

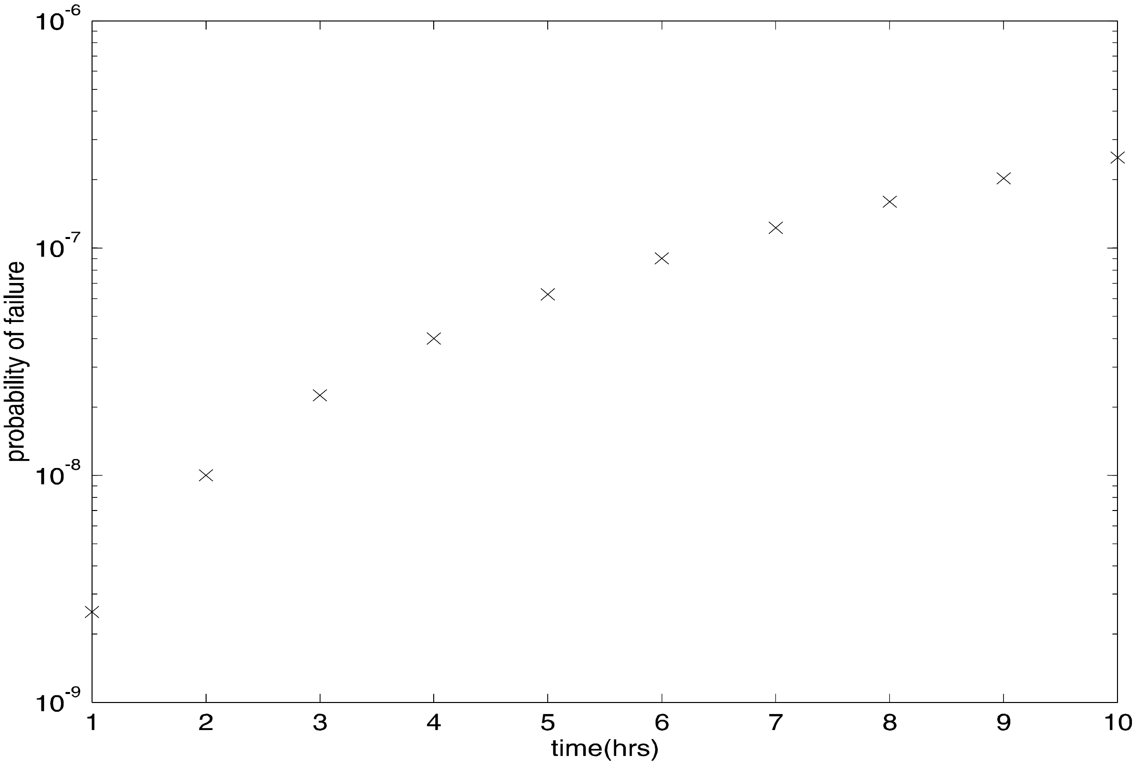

Figure 20: Probability of Failure vs. Time for Dual Communications Subsystem

Table 10: Dual Communications Subsystem

Time(hrs)	Probability
1	2.5048e-09
2	1.0019e-08
3	2.2542e-08
4	4.0073e-08
5	6.2612e-08
6	9.0158e-08
7	1.2271e-07
8	1.6027e-07
9	2.0284e-07
10	2.5040e-07

The triple communications subsystem is shown in Figures 21 and 22 and Table 11.

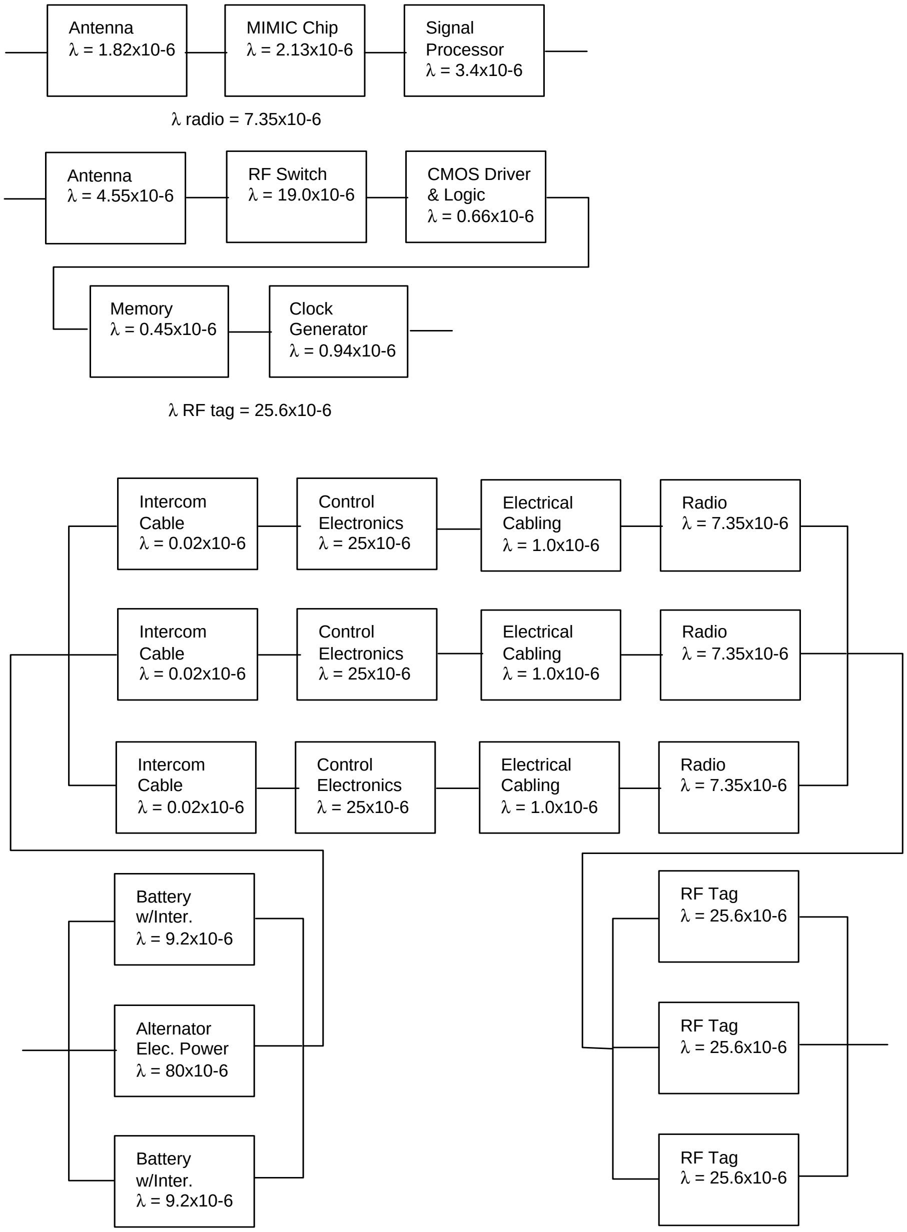

Figure 21: Triple Communications Safety Diagram Compared to Honeywell Figure 43

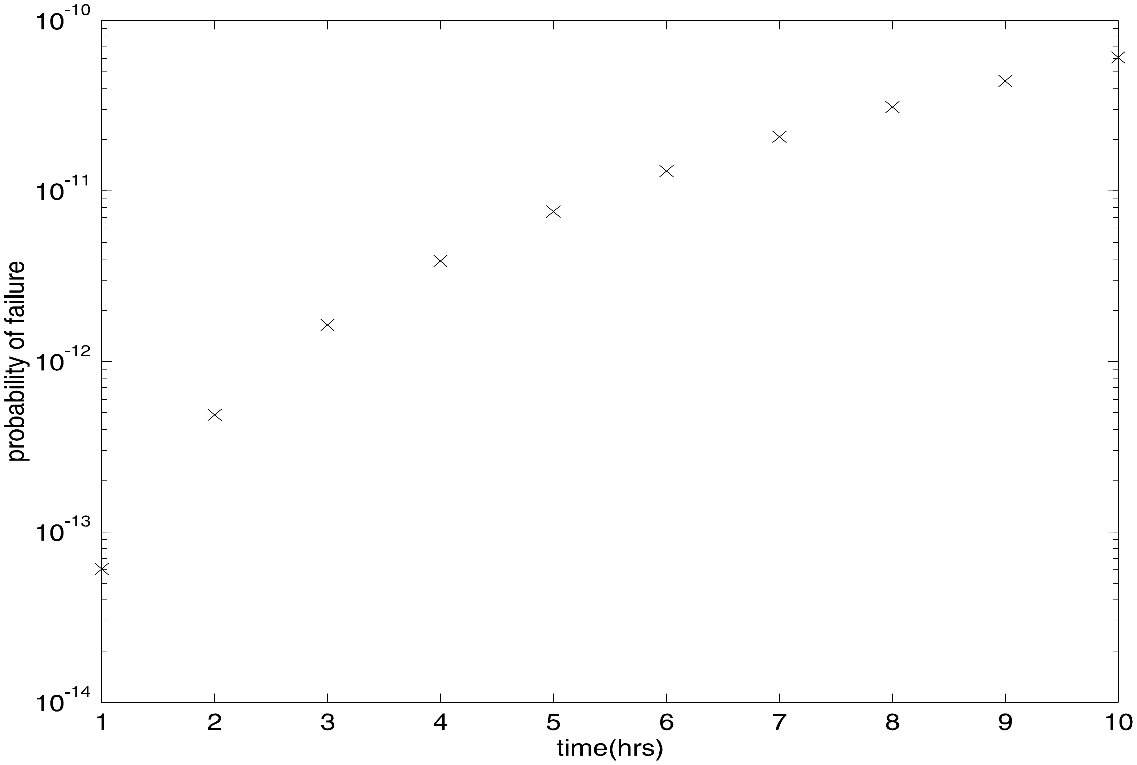

Figure 22: Probability of Failure vs. Time for Triple Communications Subsystem Compared to Honeywell Figure 44 (Different)

Table 11: Triple Communications Subsystem

Time(hrs)	Probability
1	6.0729e-14
2	4.8561e-13
3	1.6389e-12
4	3.8847e-12
5	7.5867e-12
6	1.3109e-11
7	2.0816e-11
8	3.1071e-11
9	4.4237e-11
10	6.0680e-11

Engine

Figures 23 and 24 and Table 12 show the dual power supply subsystem.

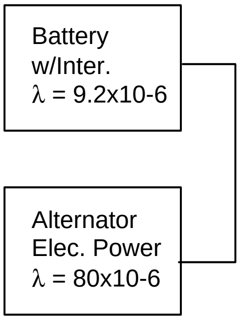

Figure 23: Dual Power Supply Safety Diagram

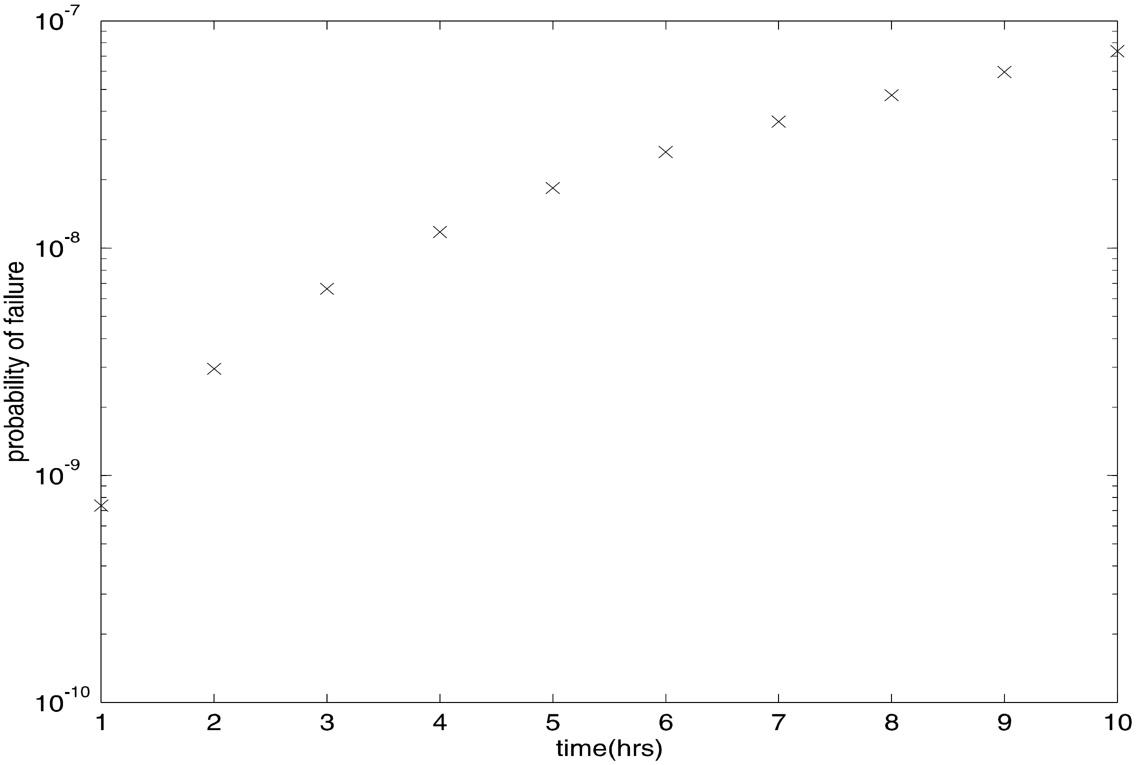

Figure 24: Probability of Failure vs. Time for Dual Power Supply Subsystem

Table 12: Dual Power Supply Subsystem

Time(hrs)	Probability
1	7.3597e-10
2	2.9437e-09
3	6.6231e-09
4	1.1774e-08
5	1.8396e-08
6	2.6489e-08
7	3.6053e-08
8	4.7087e-08
9	5.9592e-08
10	7.3567e-08

The triple power supply subsystem is shown in Figures 25 and 26 and Table 13.

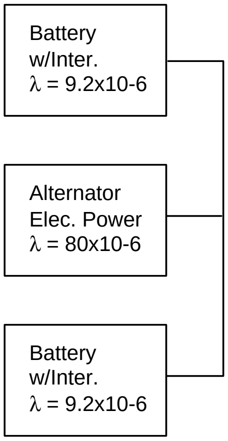

Figure 25: Triple Power Supply Safety Diagram Compared to Honeywell Figure 48

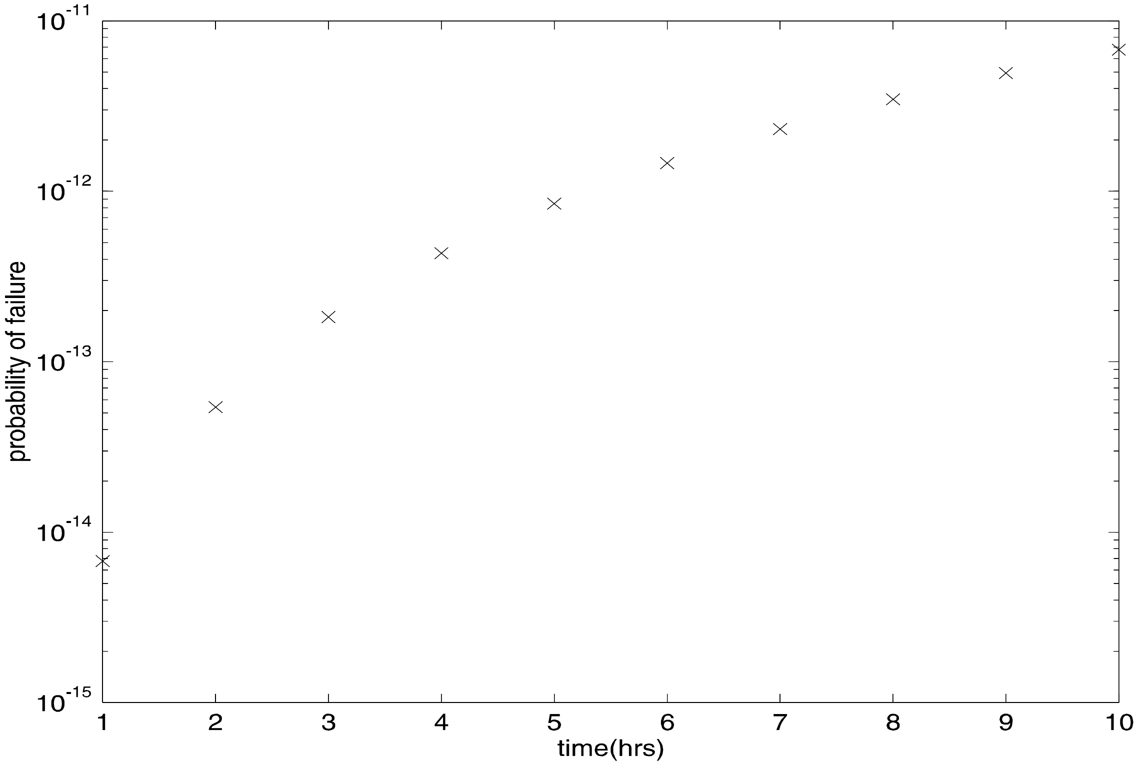

Figure 26: Probability of Failure vs. Time for Triple Power Supply Subsystem Compared to Honeywell Figure 49

Table 13: Triple Power Supply Subsystem

Time(hrs)	Probability
1	6.7724e-15
2	5.4179e-14
3	1.8274e-13
4	4.3332e-13
5	8.4621e-13
6	1.4622e-12
7	2.3217e-12
8	3.4655e-12
9	4.9341e-12
10	6.7679e-12

General Vehicle Architecture

We have proposed four different architectures for the general vehicle system. System 1 consists of dual steering, dual braking, dual object detection, dual processor, dual communication, and dual power. System 2 consists of dual steering, dual braking, dual object detection, triple processor, triple communication, and triple power. System 3 consists of partial triple steering, multi-string braking, triple object detection, triple processor, triple communication, and triple power. System 4 consists of full triple steering, multi-string braking, triple object detection, triple processor, triple communication, and triple power. Each system consists of the subsystems in series. Figures 27, 28, 29, and 30 show the probability of failure vs. time plots for these systems respectively. The data is shown in Table 14.

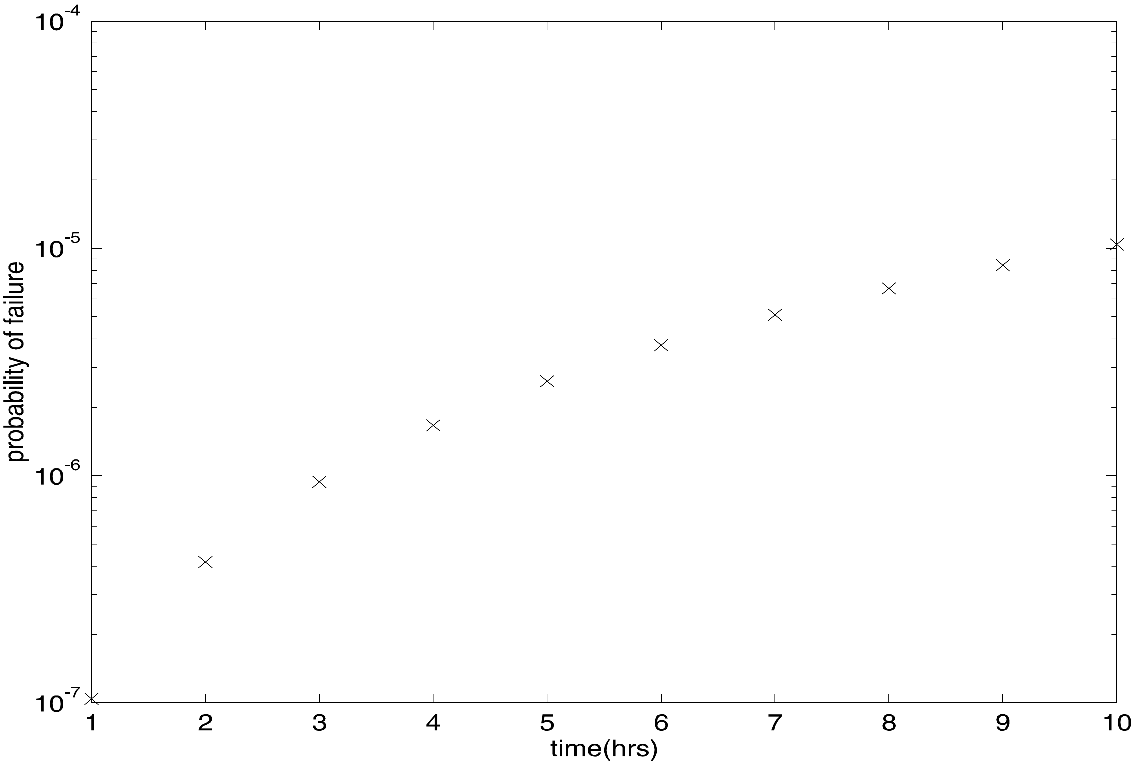

Figure 27: Probability of Failure vs. Time for System 1

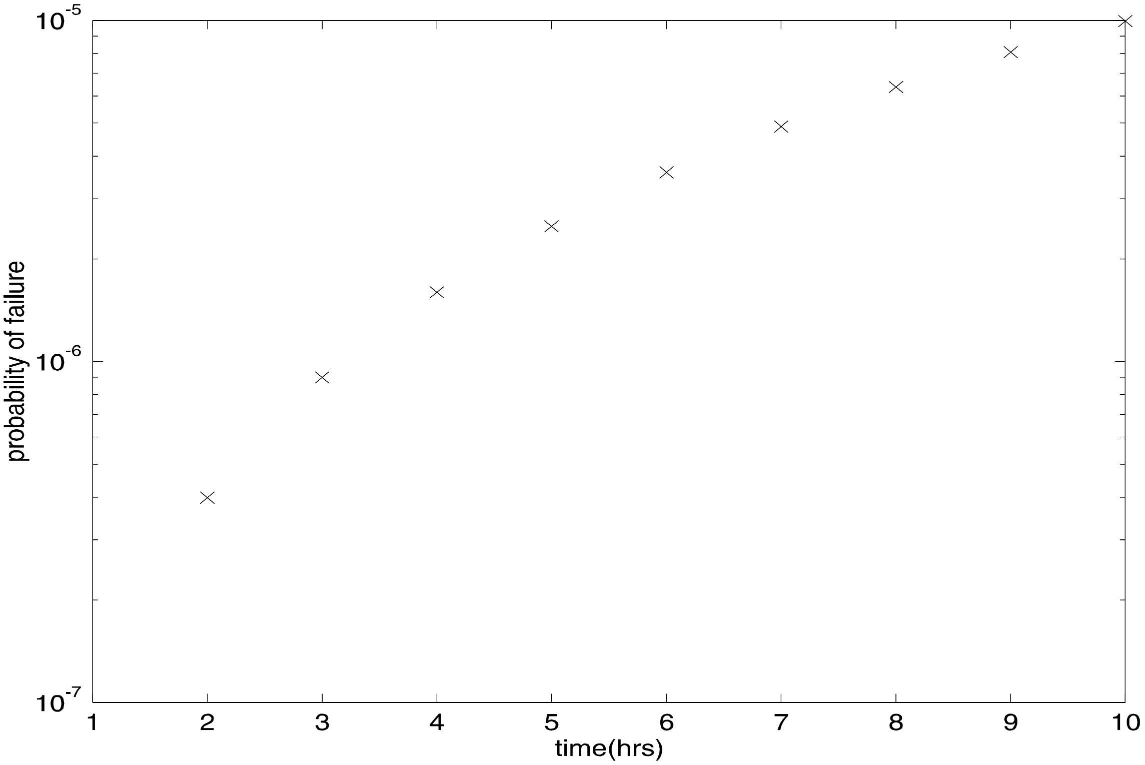

Figure 28: Probability of Failure vs. Time for System 2

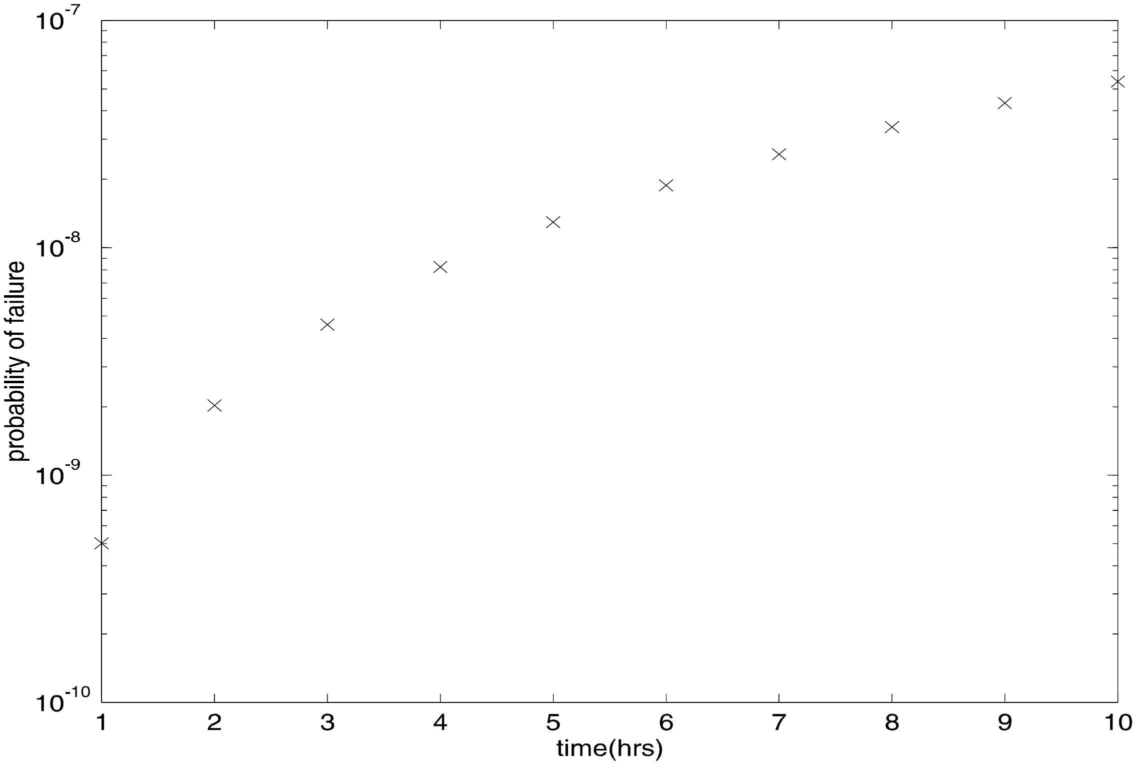

Figure 29: Probability of Failure vs. Time for System 3

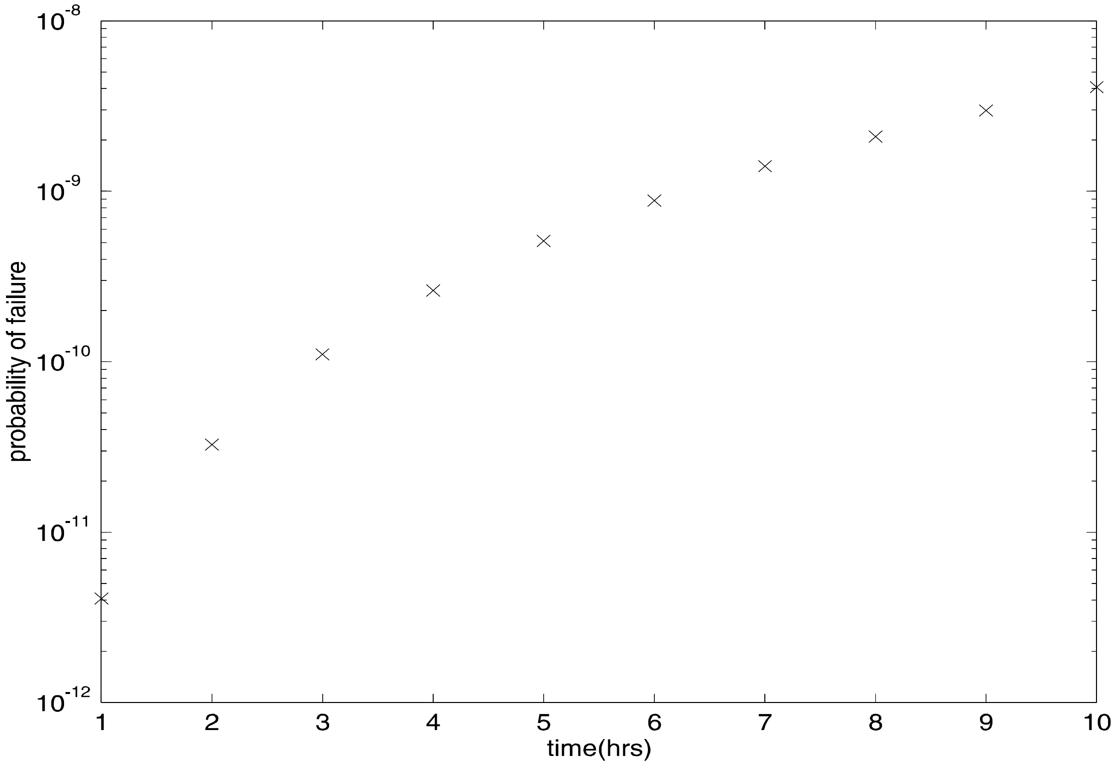

Figure 30: Probability of Failure vs. Time for System 4

Table 14: General Vehicle System

Time(hrs)	Sys. 1 Prob.	Sys. 2 Prob.	Sys. 3 Prob.	Sys. 4 Prob.
1	1.0432e-07	9.9721e-08	5.0202e-10	4.0892e-12
2	4.1721e-07	3.9880e-07	2.0244e-09	3.2708e-11
3	9.3852e-07	8.9710e-07	4.5914e-09	1.1037e-10
4	1.6681e-06	1.5945e-06	8.2274e-09	2.6159e-10
5	2.6059e-06	2.4909e-06	1.2957e-08	5.1086e-10
6	3.7517e-06	3.5861e-06	1.8804e-08	8.8264e-10
7	5.1054e-06	4.8799e-06	2.5793e-08	1.4014e-09
8	6.6669e-06	6.3724e-06	3.3949e-08	2.0916e-09
9	8.4360e-06	8.0633e-06	4.3295e-08	2.9777e-09
10	1.0413e-05	9.9525e-06	5.3856e-08	4.0841e-09

Analysis

The original Honeywell report assumed a minimum acceptable AHS failure rate of 1 x 10-6 per mission. Given this failure rate objective, both system 1 and system 2 have a mission time of approximately 3.5 hours. Similarly, for system 3 a vehicle can operate for 40 hours, and for system 4 a vehicle can operate for 63 hours without exceeding 1 x 10-6 failures per mission. These results cannot be directly compared against Honeywell's results because it is unclear how the values in Figure 51 of the Honeywell report were derived.

A major difference between the results reported here and the Honeywell report results are that we assume 100% test coverage, whereas Honeywell gives partial results for 100% test coverage, but presents conclusions assuming 95% test coverage. There is no doubt that having less than 100% test coverage will shorten mission times. However, lacking a reasonable basis to pick a test coverage number we have elected to give the optimistic 100% test coverage number. If resources are allocated to studying mission time with respect to redundancy in the future the issue of test coverage should be of prime concern.

Conclusion

In this paper we revisit the mission time computations of the Honeywell AHS Precursor System Analysis failure management report. More detailed graphs, numeric results, and Matlab programs for computing results are provided. Corrected data are presented for Figures 15, 28, 34, 40, and 44 of the Honeywell report.

As a result of using corrected data, and of assuming 100% test coverage, it was found that a system having duplex redundancy is sufficient to achieve a mission time of approximately 3.5 hours with a probability of system failure less than 1 x 10-6. Assuming that this failure rate target is adequate for AHS, the mission time seems long enough (under the set of assumptions provided) to warrant the use of less expensive duplex redundancy rather than triplex redundancy under the assumptions given in the original Honeywell report.

A major difference between the results presented here and the original Honeywell results is that we assume 100% test coverage at the start of each mission, whereas Honeywell gives results based on 95% test coverage. The issue of test coverage is critical, and can significantly affect results. Further study into what a reasonable level of test coverage might be is required before a firm recommendation can be made as to what level of redundancy is required for a safe AHS.

Acknowledgement

This research was sponsored by USDOT under Cooperative Agreement Number DTFH61-94-X-00001 as part of the National Automated Highway System Consortium.

Appendix 1: Matlab Programs

This appendix shows a sample of the programs used to generate the plots in this paper. Functions were written to calculate the reliability of individual components, series systems, and parallel systems. The code for these functions are labelled as programs 1, 2, and 3 respectively. Program 4 is the function that is used to generate the plots, given the reliabilities of the subsystem. Program 5 is an example of the m-file used to generate the probability of failure plots for each of the subsystems. And finally, program 6 is an example of the m-file used to generate the probability of failure plots for the vehicle system.

Program 1: calc_rel.m

```
%Function to calculate the reliability of each component

function[reliability] = calc_rel(lambda);

reliability = [];

for t = 1:10,
        for n = 1:length(lambda),
            reliability(t,n) = exp(-lambda(n)*t);
        end;
end;
```

Program 2: series.m

```
%Function to calculate the reliability of a series system

function [reliability] = series(series_rel);

col = size(series_rel,2);
reliability = [];

for t = 1:10,
        temp = 1;
        for count = 1:col,
            temp = temp*series_rel(t,count);
        end;
        reliability(t,1) = temp;
end;
```

Program 3: parallel.m

```
%Function to calculate the reliability of a parallel system

function [reliability] = parallel(parallel_rel);

col = size(parallel_rel,2);
reliability = [];

for t = 1:10,
        temp = 1;
        for count = 1:col,
            temp = temp*(1 - parallel_rel(t,count));
        end;
        reliability(t,1) = 1- temp;
end;
```

Program 4: make_plot.m

```
%Function to plot the probability of failure vs. time(hrs)

function [dummy] = make_plot(reliability);

unrel = 1- reliability;
semilogy(unrel,’x’);
xlabel(‘time(hrs)’);
ylabel(‘probability of failure’);
dummy = unrel;
```

Program 5: figure14.m

```
%Example m-file to plot the probability of failure of a subsystem

a = 80e-6;
b = 6.2e-6;
c = 1.4e-6;
d = .02e-6;
e = 25e-6;
f = 1e-6;
g = 6.6e-6;
h = 40.4e-6;
i = 76.3e-6;
j = 2e-6;

r1 = calc_rel([a b]);
r2 = calc_rel([c c]);
r3 = calc_rel([d e f g h i]);

p1 = parallel(r1);
p2 = parallel(r2);
s1 = series(r3);
p3 = parallel([s1 s1]);
s2 = series([p1 p2 p3]);

rel14 = s2;

x = make_plot(s2);
```

Program 6: system1.m

```
%Example m-file to calculate the probability of failure of a system

% dual steering
% dual braking
% dual object detection
% dual processor
% dual communication
% dual power

s1 = series([rel14 rel24 rel31 reldproc reldcomm reldpower]);

x = make_plot(s1);
```