

# Reliability Evaluation of the Power Supply of an Electrical Power Net for Safety-Relevant Applications

Alejandro D. Dominguez-Garcia<sup>\*</sup>, John G. Kassakian  
Joel E. Schindall

*Laboratory for Electromagnetic and Electronic Systems  
Massachusetts Institute of Technology  
77 Massachusetts Avenue, Building 10-082  
Cambridge, MA 02139  
USA*

---

## Abstract

In this paper we introduce a methodology for the dependability analysis of new automotive safety-relevant systems. With the introduction of safety-relevant electronic systems in cars, it is necessary to carry out a thorough dependability analysis of those systems to fully understand and quantify the failure mechanisms in order to improve the design. Several system level FMEAs are used to identify the different failure modes of the system and, a Markov model is constructed to quantify their probability of occurrence. A new power net architecture with application to new safety-relevant automotive systems, such as Steer-by-Wire or Brake-by-Wire, is used as a case study. For these safety-relevant loads, loss of electric power supply means loss of control of the vehicle. It is therefore necessary and critical to develop a highly dependable power net to ensure power to these loads under all circumstances.

*Key words:* Failure mode and effects analysis (FMEA); Markov model.

---

---

<sup>\*</sup> Corresponding author.

E-mail address: aledan@MIT.EDU (Alejandro Dominguez-Garcia)

## 1 Introduction

The safety-critical nature of new complex electronic systems in cars, such as Steer-by-Wire or Brake-by-Wire, mandates a thorough dependability analysis to fully understand and quantify their failure mechanisms in order to improve the design. The techniques used in the reliability analysis of complex system can be divided into qualitative and quantitative. Qualitative techniques help to identify weaknesses in the design and are used prior to a quantitative analysis, but they do not give a useful measure of the severity of system failures. Therefore, quantitative techniques must also be applied during the design phase of the system. The methodology proposed in this paper is widely used in the aircraft industry [1] and we have adapted it to the needs of the automotive industry following the previous work done by [2]. The qualitative analysis is accomplished by using several system level FMEAs, which help to identify the different failure modes of the system. Markov models are used to quantify the probability of occurrence of the identified failure modes. A new power net architecture with application to new safety-relevant automotive systems, such as Steer-by-Wire or Brake-by-Wire, is used as a case study to illustrate how the analysis is carried out.

In conventional power nets, the power supply is provided by a battery, an alternator, various switches, fuses or circuit breakers and wiring. If any of these fails, there is a chance that the power net voltage will collapse and no actuation of any electrical systems will be possible. Although this is a problem from the driver comfort point of view, the safety-relevant systems of the car, such as conventional (non electrical) steering and braking systems, will still function. With the introduction of Steer-by-Wire and Brake-by-Wire, a

loss in the power supply is no longer acceptable. Loss of electric power would mean loss of control of the vehicle, resulting in a dangerous situation for the driver. Considerable attention has been focused on the development of highly dependable Steer-by-Wire and Brake-by-Wire systems [3], [4], [5], [2], but only [5] and [2] talk about the fact that the power supply also has to be highly dependable and fault-tolerant, although their work is not focused on this issue. Current power net designs are not dependable enough for their use in safety-relevant applications. Therefore, it is important to develop new power net architectures and carry out a dependability analysis of these architectures to validate them for their use in safety-relevant applications. Some work has been done in this regard. In 1994, and anticipating the needs for future electrical loads in vehicles, [6] proposes alternative electrical distribution system architectures, already addressing the reliability issue of these new architectures. In [7], the requirements of vehicle power supply architectures are identified and, although some solutions are proposed, no further dependability analysis is done to validate them for their use in safety-critical applications.

In this paper we introduce a new power net architecture based on one of the solutions given in [7]. It is not necessarily the optimal solution for the power net in terms of reliability, but we will use it to introduce a methodology for analyzing the dependability of new automotive systems. The analysis for the power supply of this architecture is developed using several system level FMEAs to identify the different failure modes of the system, and a Markov model, including time-dependent failure rates for some of the components, to quantify the probability of occurrence of the identified failure modes. Section 2 of this paper defines the power net architecture used in the study, presenting its main differences from classical architectures. Section 3 presents some important definitions. Section 4 presents the complete system level FMEA

needed to carry out further reliability analysis. Section 5 presents a simplified system level FMEA, and Section 6 presents the associated Markov model for the power supply of the proposed new architecture. In section 7 the input parameters for the model are introduced. Section 8 presents the dependability measures used in the study, while Section 9 shows the analysis results, presenting a sensitivity analysis to changes in some model parameters. The sensitivity analysis is a very important result for improving the design of the system. Concluding remarks and future work are presented in Section 10. The notation used is listed at the end of the paper.

## 2 A case Study: Dual Battery Architecture

The proposed power net architecture is shown in Figure 1, consisting of the following elements:

- Alternator  $G$ , which generates energy for the electric loads and for charging the battery.
- Main battery  $B_1$ , which provides energy for the electric loads.
- Backup battery  $B_2$ , which is in cold standby is only switched on in case of a failure of the alternator,  $G$ , or the main battery,  $B_1$ .
- Voltage and current sensors  $S_V$  and  $S_A$  which measure the voltage of the power supply and the current flowing through the main battery  $B_1$  and alternator  $G$ .
- Switches  $SW_1$ ,  $SW_2$  and  $SW_3$ .
- Electronic control unit,  $ECU$ , which receives signals from the voltage and current sensors  $S_V$  and  $S_A$ , and sends signals to the switches  $SW_1$ ,  $SW_2$  and  $SW_3$  in case a failure occurs.
- Main wire harness,  $MWH$ , which links the power supply with the fuse box.

- Fuses,  $F$ , for short circuit protection.
- Wire harness  $H$ .
- Steer-by-Wire channels  $SbW_1$  and  $SbW_2$ .
- Conventional electric loads  $L$ .

The primary difference between the proposed and conventional power nets is the backup battery  $B_2$ , the detection and isolation system (composed of the electronic control unit  $ECU$ , the voltage and current sensors  $S_V$  and  $S_A$ , and the switches  $SW_1$ ,  $SW_2$  and  $SW_3$ ), and the redundancy introduced by having two Steer-by-Wire channels  $SbW_1$  and  $SbW_2$ . If a fault is detected in the alternator  $G$  or the main battery  $B_1$ , the detection and isolation system switches off the faulty element and switches on the backup battery  $B_2$ . Additionally, the backup battery is also switched on if there is a voltage drop in the power supply, even when no fault has been detected in the alternator  $G$  or the main battery  $B_1$ . No failure annunciation system is considered for non-catastrophic first failures, which means that the system must work for the stated period of time without maintenance.

### *2.1 Power supply subsystem definition*

As stated in Section 1, one of the aims of this paper is to assess the dependability of the power supply of the proposed dual battery architecture. Therefore, the first step in this analysis is to clearly identify the components of the power supply subsystem. These are:

- Alternator  $G$ .
- Main battery  $B_1$ .
- Backup battery  $B_2$ .

- Voltage and current sensors  $S_V$  and  $S_A$ .
- Switches  $SW_1$ ,  $SW_2$  and  $SW_3$ .
- Electronic control unit  $ECU$ .
- Main wire harness  $MWH$ .

### 3 Definitions

Some important concepts used in this paper, such as fault coverage and component coverage, are introduced in this section.

#### 3.1 Fault coverage

The fault coverage,  $c$ , is defined as the conditional probability that when a fault has occurred, it can be detected and isolated before an unrecoverable transient has been introduced into the system [8]. Equation (1) defines  $c$  mathematically as the probability of detecting and isolating a fault given that a failure has occurred. Detection and isolation are considered independent events.

$$c = P(D \cap I/F) = P(D/F)P(I/F) \quad (1)$$

#### 3.2 Alternator, Main Battery and Backup Battery Coverage

There are some operational modes in which it is possible that, even with a non-covered failure of the alternator or a non-covered failure of one of the batteries, the system will still work without reaching a catastrophic state. This will depend on the ability of the alternator or the batteries alone to be able to provide all the necessary energy. The probability of these conditions occurring are:

- Alternator coverage  $S_G$ : Probability that the alternator is able to provide all the energy.
- Main battery coverage  $S_{B_1}$ : Probability that the main battery is able to provide all the energy.
- Backup battery coverage  $S_{B_2}$ : Probability that the backup battery is able to provide all the energy.

These probabilities depend on the loads that are connected at one time and they can be computed as the ratio of the time that the alternator, main battery or backup battery can provide energy alone, to the connected loads and the evaluation time  $t_0$  of the system.

#### 4 System Level FMEA

The first step in constructing a Markov model is to develop several system level FMEAs. The first FMEA will help to identify first failures in the system, both catastrophic and non-catastrophic. The second FMEA will identify second catastrophic and non-catastrophic failure modes for the new non-catastrophic operational modes of the system defined by the first FMEA. The process will end when all the identified failure modes of an FMEA are catastrophic. To construct the system level FMEA, some simplifying assumptions are postulated:

- The backup battery  $B_2$  has zero failure rate while it is in the standby condition.
- The main battery  $B_1$  and the backup battery  $B_2$  have equal failure rates when they are working, i.e., charging or discharging .
- The fault coverage includes the switches  $SW$ , the voltage and current sen-

sors  $S_v$  and  $S_A$ , and the electronic control unit  $ECU$ .

- Since no annunciation system is considered in this architecture, repair processes for non-catastrophic failures are not considered.
- The detection and isolation system has fail-safe features, which means that if a fault occurs in the detection and isolation system, it is disabled and does not affect the rest of the system.

Table 1 corresponds to the FMEA for first failures of the system. The first column of Table 1, lists the system state with no failures. The second column associates a probability to the event of being in the state described by the first column. The third column describes all possible failure modes associated with the operational mode described in the first column, while the fourth column lists the failure rates for the different failure modes. Finally, the fifth column describes the new system states resulting from the failure modes described in the third column, and column sixth associates a probability to each of these new system states. Table 2 corresponds to the FMEA for second failures of the system. The first column of Table 2 corresponds to the non-failed states reported in column fifth of Table 1. The remaining columns of Table 2 are obtained in the same way as for Table 1. Table 3 reports third failures of the system and it is constructed in the same way as Table 2, starting with the non-failed states listed in the fifth column of Table 2.

## 5 Simplified System Level FMEA

In Section 4 a detailed system level FMEA for the power supply of the dual battery architecture was presented. It is important to note that not all the input parameters for that model were available at the time this research was done, so a simplified version of the system level FMEA was developed, for

which all the required parameters were available. Further simplifying assumptions to those state in Section 4 are needed to develop the simplified system level FMEA. The alternator  $G$ , the main battery  $B_1$  and the backup battery  $B_2$  coverage are set to zero, which means that none of this components is able to provide all the energy alone to the connected loads at any given time. There are no different failure modes for each component, which means that there are only two possible states for each component, running and failed.

Tables 4 and 5 correspond to the simplified system level FMEA for first and second failures of the system and they are obtained in the same way described in Section 5 for Tables 1, 2 and 3. This analysis provides the basis for the development of the Markov model described in Section 6.

## 6 Markov Model

Based on the simplified system level FMEA developed in Section 5, it is possible to construct a Markov model that represents the behavior of the system. The Markov model is described by a set of linear homogeneous differential equations (2).

$$\begin{aligned} \dot{P}(t) &= \Lambda(t)P(t) \\ P(0) &= [1 \ 0 \ 0 \ \dots \ 0]' \end{aligned} \tag{2}$$

$P(t)$  is the state probability vector and each component  $P_k(t)$ , for  $k = 0, 2, \dots, 15$  represents the probability of being at each system state,  $k$ , at any given time,  $t$ . The transition rate matrix  $\Lambda(t)$  is easily constructed by combining the information of Tables 4 and 5. Each coefficient  $\lambda_{ij}$  of the matrix is obtained by a combination of transition rates between system states. The transition rates

between the system state with no failure and system states with one failure are displayed in the third column of Table 4. The third column of table 5 describes the transition rates between system states with one failure and system states with two failures. A *Matlab/Simulink*<sup>®</sup> model was developed to solve the Markov Model.

## 7 Model parameters

This section presents the input parameters for the model. Table 6 shows the values of the failure rates and the detection probabilities associated with the detection algorithm used to construct the model.

### 7.1 Component failure rates

The failure rates for the main battery  $B_1$ , the backup battery  $B_2$ , the alternator  $G$ , and the main wire harness  $MWH$  are considered to be time-dependent and Weibull distributed. Their Weibull distributions were obtained from field data provided by the Allgemeiner Deutscher Automobil Club [9]. The failure rates for the rest of the components, i.e.,  $ECU$ , sensors  $S_V$  and  $S_A$ , and switches  $SW$ , are assumed to be constant and were based on typical data for automotive components [2]. Equation (3) represents the failure rate for a Weibull distribution [10], where  $\alpha$  is called the shape parameter,  $\lambda_0$  is the scale parameter and  $t$  is the time frame.

$$\lambda = \alpha\lambda_0(\lambda_0 t)^{\alpha-1} \quad (3)$$

Since the values of the failure rates for the  $ECU$ , the sensors  $S_V$  and  $S_A$ , and the switches  $SW$  are presumed, a sensitivity analysis is carried out for each of

these components to see how a change in its affects the dependability of the system. The result of the sensitivity analysis is key to improve the design of the system.

## 7.2 Fault coverage

As stated in (1), the fault coverage  $c$  depends on the ability of the detection and isolation system to detect and isolate a fault.

The detection probability,  $D$ , depends on the accuracy of the detection algorithm implemented in the *ECU*. A sensitivity analysis is carried out to study the influence of the detection probability in the performance of the system.

Isolation depends on the detection and isolation system components working on demand. Failures of components in the detection and isolation system are assumed to be independent and Poisson distributed. Equation (4) gives the Poisson distribution, representing the number of failures for a time interval  $t$  [11], where  $\lambda$  is the component failure rate.

$$P(X_t = x) = \frac{(\lambda t)^x}{x!} e^{-\lambda t} \quad (4)$$

Equations (5) and (6) give the probability of detection and isolation given that a failure has occurred, which depends on the detection algorithm successfully detecting a fault. A successful failure isolation occurs when there is no fault in the components involved in the detection and isolation system, which are the electronic control unit *ECU*, the switches *SW* and the voltage and current sensors  $S_V$  and  $S_A$ . All the switches are considered to have the same failure rate  $\lambda_{SW}$ , and the sensors have a common failure rate  $\lambda_S$ . The final result for the coverage probability calculation is given by Equation (7).

$$P(D/F) = D \quad (5)$$

$$P(I/F) = P(X_t^{Sv} = 0)P(X_t^{SA} = 0)P(X_t^{SA} = 0) \\ \cdot P(X_t^{ECU} = 0)P(X_t^{SW1} = 0)P(X_t^{SW2} = 0)P(X_t^{SW3} = 0) \quad (6)$$

$$c = De^{-(\lambda_{ECU} + 3\lambda_{SW} + 3\lambda_S)t} \quad (7)$$

## 8 Dependability measures

Two measures are used to compute the dependability of the power net architecture. The first is called the dependability rate  $\bar{\lambda}$  and has been adopted from the Federal Aviation Administration (FAA) regulations [1]. The dependability rate  $\bar{\lambda}$  of a system is given by (8). It represents the ratio of the probability of having a catastrophic failure  $F(t_0)$  before the evaluation time  $t_0$  of the system, and the evaluation time  $t_0$ . It can be thought of as an average failure rate for the system at time  $t_0$ .

$$\bar{\lambda} = \frac{F(t_0)}{t_0} \quad (8)$$

The second measure is the total failure rate of the system as a function of time, and is computed by (9).

$$\lambda_s(t) = \frac{f(t)}{1 - F(t)} \quad (9)$$

## 9 Analysis results

A vehicle life time of 15 years and an average of 400 working hours per year was considered for the simulations, which gives an evaluation time,  $t_0$ , of 6000 h. Using the parameters of Table 6, which correspond to the assumed nominal failure rate values, and the fault coverage value given by substituting the corresponding values in (7), the dependability rate  $\bar{\lambda}$  yielded by the Markov

model is  $6.1 \cdot 10^{-9}$  failures/hour. The total failure rate  $\lambda_s(t)$  obtained after 6,000 h of operation was  $2.8 \cdot 10^{-6}$  failures/hour. To gain more insight to the system failure contributions of first and second failures and also component failures, further analysis is carried out using the dependability measurement given by (8). The results are displayed in Figures 2, 3, 4, 5 and 6. Figure 2 shows the distribution of catastrophic first and second failures. It is important to note that the most important contribution to system failure is given by first failures, which correspond to uncovered failures of the main battery,  $B_1$ , alternator,  $G$ , and the main wire harness,  $MWH$ .

For a better understanding of the contributions of component first failures to system failure, Figure 3 displays the single contributions of uncovered first failures in the main battery,  $B_1$ , alternator,  $G$ , and main wire harness,  $MWH$ . The main contribution to system failure, being of  $3 \cdot 10^{-9}$  failures/hour, in this case, comes from the main battery,  $B_1$ , which is also a single point of failure.

Figures 4, 5 and 6 display the component contributions to catastrophic second failure rates. It is interesting to note that after each first failure, the contribution of the main wire harness is always the least important, at one or two orders of magnitude less than the other contributors. For example, after a covered failure in the main battery, the contribution of the backup battery is  $3.7 \cdot 10^{-12}$  failures/hour and the alternator contribution is  $1.2 \cdot 10^{-12}$  failures/hour, while the main wire harness contribution is  $2 \cdot 10^{-13}$  failures/hour.

A key result in this study is the sensitivity analysis to study the influence of the presumed failure rates of  $ECU$ , voltage and current sensors,  $S_V$  and  $S_A$ , and switches  $SW$ . The procedure followed was to change the value of each component, one at a time. The parameter multipliers used were 0.1 and 10 for all components. Figure 7 displays the sensitivity analysis results. The

influence of changes in *ECU* and voltage and current sensor,  $S_V$  and  $S_A$ , failures rates, although difficult to see in the figure, is almost the same, and it is small in comparison with the effect of changes in the switch, *SW*, failure rates. An increase in the failure rate of the switches translates to a one order of magnitude increase of the dependability rate. The rest of the failure rate changes keep the dependability rate within the same order of magnitude as that obtained using the nominal failure rates.

Figure 8 shows the sensitivity analysis for the detection probability,  $D$ , which is another important result during the design. It is interesting to see that increases in the detection probability do not produce significant changes in the dependability rate of the system for detection probabilities greater than 0.99. This analysis gives us some insight to how effective the detection algorithm should be.

Finally, Figure 9 shows the total failure rate of the system  $\lambda_s(t)$ , as a function of time. It is important to note that the  $\lambda_s(t)$  increases exponentially and it does not settle to a constant value as it does in the case when all component failure rates are constant. After 3,000 h of use of the car, the failure rate is about  $0.5 \cdot 10^{-6}$  failures/hour, a value that increases by almost a factor of 6 at the end of the life of the vehicle, yielding a value of  $2.8 \cdot 10^{-6}$  failures/hour. In the case of components constant failure rates,  $\lambda_s(t)$  does not increase so dramatically and it does settle to a constant value after an initial transient period. However it also yields a more conservative result due to the fact that component wear-out effects are neglected.

## 10 Conclusions and future work

The analysis carried out on the dual battery power net architecture shows that the influence of the detection and isolation system in the overall dependability rate is very important. As seen, the dependability rate strongly depends on the detection probability,  $D$ , when  $D$  is less than 0.99. Above 0.99,  $D$  no longer influences the dependability of the system. The switches  $SW$  are the component of the detection and isolation system that most influence the dependability rate. One way to improve the dependability of this architecture would be to improve the detection and isolation system by improving the detection algorithm to have a detection probability  $D$  of 0.99 or greater and by using switches with fault-tolerant and fail-safe features. Another way to improve the dependability would be by redesigning the link between the power supply and the main fuse box, i.e., the main wire harness in the previous design. This would prevent single failures in the main wire harness from making the system fail despite the redundancy introduced by the second battery.

The analysis results in this paper were obtained using a simplified reliability model based on available field data. An immediate way to develop a more realistic model would be to assume a non-zero failure rate for the backup battery while in standby. Another improvement would be to include more time-dependent failure rates for the rest of the components, based on field data, instead of using a sensitivity analysis. The introduction of repair features would also make the model more realistic. Finally the introduction of uncertainty in the model parameters would also give more accurate results.

## Appendix

### *Notation*

$B_1$	Main battery
$B_2$	Backup battery
$c$	Fault coverage
$DS$	Detection and isolation system
$ECU$	Electronic control unit
$F$	Fuse
$f(t)$	PDF for time to catastrophic failures in the system
$F(t)$	CDF for time to catastrophic failures in the system
$G$	Alternator
$H$	Wire harness
$L$	Conventional electrical loads
$MWH$	Main wire harness linking the power supply with the fuse box
$P(D \cap I/F)$	Probability of detection and isolation given a fault has occurred
$P(D/F), D$	Probability of detection given a fault has occurred
$P(I/F)$	Probability of isolation given a fault has occurred
$P_k$	Probability of being in state k
$S_A$	Current sensor
$S_{B_1}/S_{B_2}$	Battery coverage
$S_G$	Alternator coverage
$S_V$	Voltage sensor
$SbW_1$	Steer-by-Wire channel 1
$SbW_2$	Steer-by-Wire channel 2

$SW_1$ :	Main battery switch
$SW_2$ :	Alternator switch
$SW_3$ :	Backup battery switch
$t$ :	Time
$t_0$ :	Evaluation time
$X_t^A$ :	Number of failures in $S_A$ for an operating time of t hours
$X_t^{ECU}$ :	Number of failures in $ECU$ for an operating time of t hours
$X_t^{SW_1}$ :	Number of failures in $SW_1$ for an operating time of t hours
$X_t^{SW_2}$ :	Number of failures in $SW_2$ for an operating time of t hours
$X_t^{SW_3}$ :	Number of failures in $SW_3$ for an operating time of t hours
$X_t^V$ :	Number of failures in $S_V$ for an operating time of t hours
$\alpha$ :	Shape parameter of the Weibull distribution
$\lambda$ :	Failure rate
$\lambda_{B_1}/\lambda_{B_2}$ :	Battery total failure rate
$\lambda_{B_1}^{OC}/\lambda_{B_2}^{OC}$ :	Battery open circuit failure rate
$\lambda_{B_1}^{SC}/\lambda_{B_2}^{SC}$ :	Battery short circuit failure rate
$\lambda_G$ :	Alternator total failure rate
$\lambda_G^{OC}$ :	Alternator open circuit failure rate
$\lambda_G^{SC}$ :	Alternator short circuit failure rate
$\lambda_G^{UV}$ :	Alternator under voltage failure rate
$\lambda_G^{OV}$ :	Alternator over voltage failure rate
$\lambda_{MWH}$ :	Main wire harness failure rate
$\lambda_{ECU}$ :	Electronic control unit failure rate
$\lambda_S$ :	Sensor failure rate
$\lambda_{SW}$ :	Switch failure rate
$\bar{\lambda}$ :	Dependability rate
$\lambda_S(t)$ :	Global system failure rate

$\lambda_0$  :                Scale parameter of the Weibull distribution

## References

- [1] U.S. federal air regulations 25.1309 and the supporting advisory circular AC-25.1309.
- [2] R. Hammett, P. Babcock, Achieving  $10^{-9}$  dependability with drive-by-wire systems, SAE Technical Paper Series, Paper 2003-01-1290, 2003.
- [3] W. Harter, W. Pfeiffer, P. Dominke, G. Ruck, P. Blessing, Future electrical steering systems: Realizations with safety requirements, SAE Technical Paper Series, Paper 2000-01-0822, 2000.
- [4] R. Isermann, R. Schwarz, S. Stolzl, Fault-tolerant drive-by-wire systems, IEEE Control Systems Magazine, vol. 22, no. 5, 2002.
- [5] P. Dominke, G. Ruck, Electric power steering, the first step on the way to steer-by-wire, SAE Technical Paper Series, Paper 1999-01-0401, 1999.
- [6] K. Afridi, R. Tabors, J. Kassakian, Alternative electrical distribution system architectures for automobiles, in: Proceedings of Power Electronics in Transportation, 1994.
- [7] H. Brinkmeyer, Architecture of vehicle power supply in the throes of change, in: Proceedings of Automobile Electronics Congress, 2002.
- [8] P. Babcock, An introduction to reliability modeling of fault-tolerant systems, Tech. rep., The Charles Stark Draper Laboratory CSDL-R-1899, 1987.
- [9] M. Abele, Modellierung und bewertung von fehlertoleranzmassnahmen in kfz-energiebordnetzen fr sicherheitsrelevante verbraucher, Master's thesis, Unikassel Versitat, 2004.
- [10] A. Hoyland, M. Rausand, System Reliability Theory, John Wiley and Sons, 1994.
- [11] A. Ang, W. Tang, Probability Concepts in Engineering Planning and Design, vol. I-Basic Principles, John Wiley and Sons, 1975.

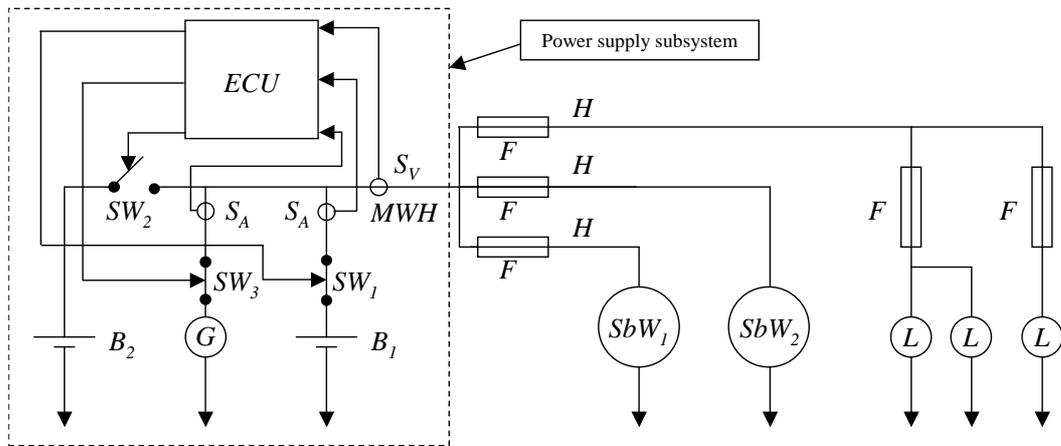


Fig. 1. Dual battery power net architecture.

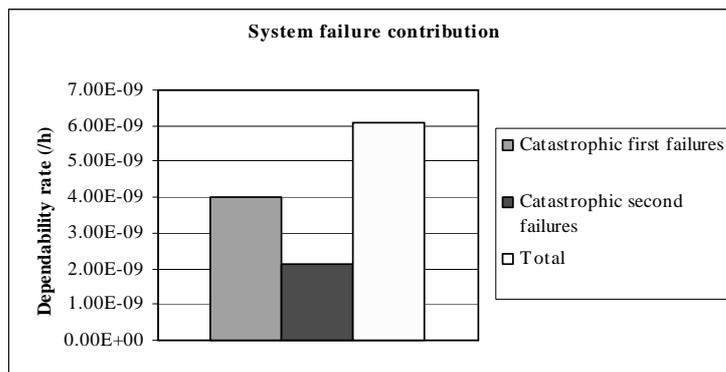


Fig. 2. Catastrophic failure contributions to the total system dependability rate  $\bar{\lambda}$ .

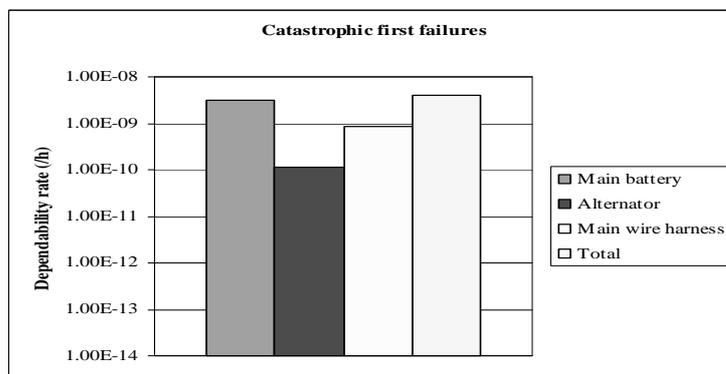


Fig. 3. Component failure contributions for catastrophic first failures.

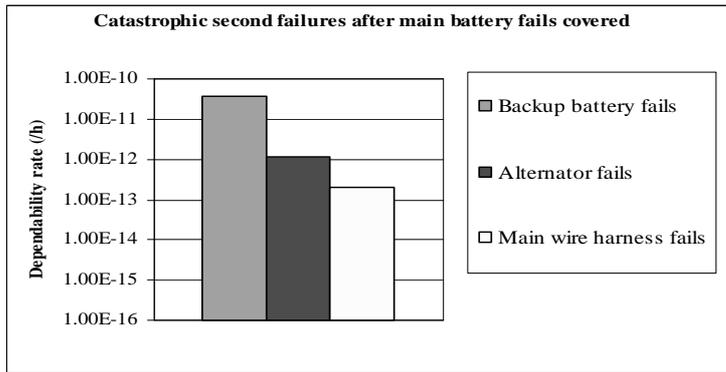


Fig. 4. Component failure contributions for catastrophic second failures after main battery  $B_1$  fails first.

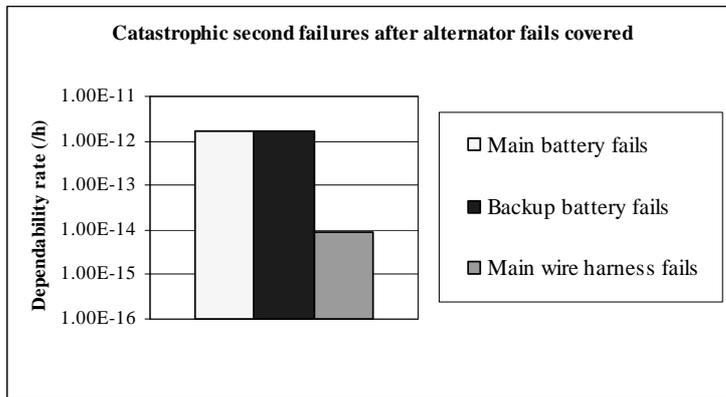


Fig. 5. Component failure contributions for catastrophic second failures after alternator  $G$  fails first.

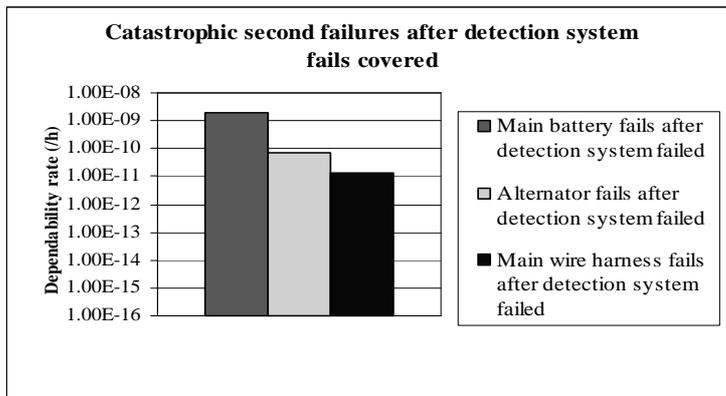


Fig. 6. Component failure contributions for catastrophic second failures after detection and isolation system  $DS$  fails first.

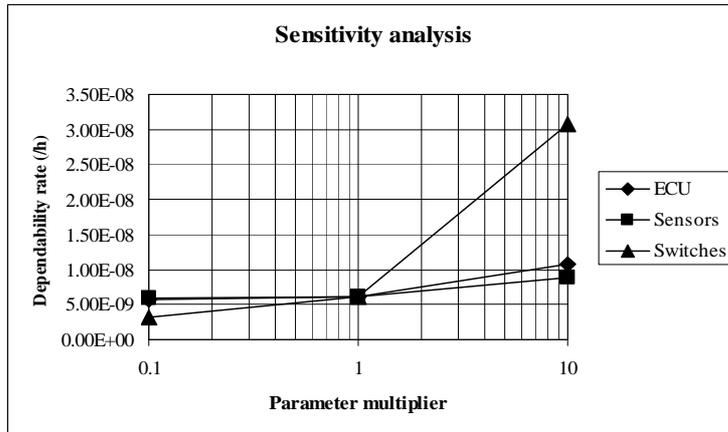


Fig. 7. Sensitivity analysis to changes in the *ECU*, the switches *SW* and the sensors *S* failure rates.

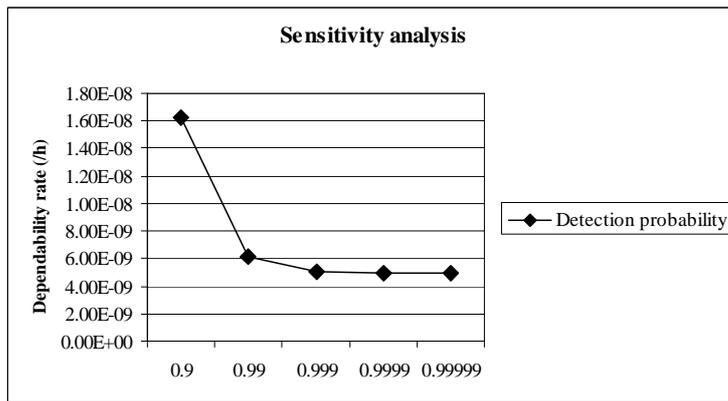


Fig. 8. Sensitivity analysis to changes in the detection probability *D*.

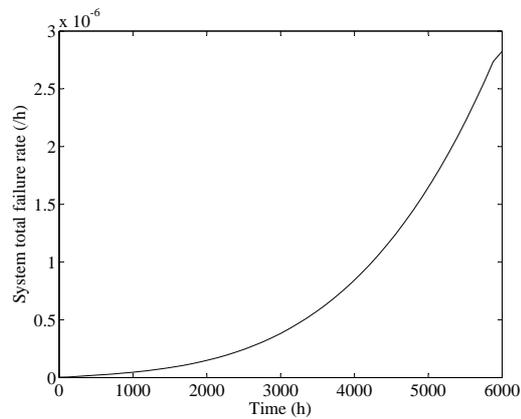


Fig. 9. System total failure rate  $\lambda_s(t)$  versus time for the nominal values.

Table 1  
System level FMEA for first failures.

System state with no failures	State probability	Failure mode	Failure rate	System state with one failure	State probability
$B_1$ Delivering energy, and $G$ generating energy, and $DS$ monitoring the system, and $MWH$ transporting energy.	$P_0$	$B_1$ fails covered.	$c\lambda_{B_1}$	$B_2$ delivering energy, and $G$ generating energy, and $MWH$ transporting energy.	$P_1$
		$B_1$ fails open circuit uncovered, and $G$ able to provide all the energy.	$(1-c)S_G\lambda_{B_1}^{OC}$	$G$ generating energy, and $MWH$ transporting energy.	$P_2$
		$B_1$ fails open circuit uncovered, and $G$ not able to provide all the energy.	$(1-c)(1-S_G)\lambda_{B_1}^{OC}$	FAILED	$P_3$
		$B_1$ fails short circuit uncovered.	$(1-c)\lambda_{B_1}^{SC}$	FAILED	$P_4$
		$G$ fails covered.	$c\lambda_G$	$B_1$ delivering energy, and $B_2$ delivering energy, and $MWH$ transporting energy.	$P_5$
		$G$ fails open circuit or fails undervoltage uncovered, and $B_1$ able to provide all the energy.	$(1-c)S_{B_1}(\lambda_G^{OC} + \lambda_G^{UV})$	$B_1$ delivering energy, and $MWH$ transporting energy.	$P_6$
		$G$ fails open circuit or fails undervoltage uncovered, and $B_1$ not able to provide all the energy.	$(1-c)(1-S_{B_1})(\lambda_G^{OC} + \lambda_G^{UV})$	FAILED	$P_7$
		$G$ fails short circuit or over voltage uncovered.	$(1-c)(\lambda_G^{SC} + \lambda_G^{OV})$	FAILED	$P_8$
		$DS$ fails.	$\lambda_{ECU} + 3\lambda_{SW} + 3\lambda_S$	$B_1$ delivering energy, and $G$ generating energy, and $MWH$ transporting energy.	$P_9$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{10}$

Table 2  
System level FMEA for second failures.

System state with one failure	State probability	Failure mode	Failure rate	System state with two failures	State probability
$B_2$ delivering energy, and $G$ generating energy, and $MWH$ transporting energy.	$P_1$	$B_2$ fails open circuit, and $G$ able to provide all the energy.	$S_G \lambda_{B_2}^{OC}$	$G$ generating energy, and $MWH$ transporting energy.	$P_{11}$
		$B_2$ fails open circuit, and $G$ not able to provide all the energy.	$(1 - S_G) \lambda_{B_2}^{OC}$	FAILED	$P_{12}$
		$B_2$ fails short circuit.	$\lambda_{B_2}^{SC}$	FAILED	$P_{13}$
		$G$ fails open circuit or fails undervoltage, and $B_2$ able to provide all the energy.	$S_{B_2} (\lambda_G^{OC} + \lambda_G^{UV})$	$B_1$ delivering energy, and $MWH$ transporting energy.	$P_{14}$
		$G$ fails open circuit or fails undervoltage, and $B_2$ not able to provide all the energy.	$(1 - S_{B_2}) (\lambda_G^{OC} + \lambda_G^{UV})$	FAILED	$P_{15}$
		$G$ fails short circuit or overvoltage.	$\lambda_G^{SC} + \lambda_G^{OV}$	FAILED	$P_{16}$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{17}$
$G$ generating energy, and $MWH$ transporting energy.	$P_2$	$G$ fails.	$\lambda_G$	FAILED	$P_{18}$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{19}$
$B_1$ delivering energy, and $B_2$ delivering energy, and $MWH$ transporting energy.	$P_5$	$B_1$ (or $B_2$ ) fails open circuit, and $B_2$ (or $B_1$ ) able to provide all the energy.	$S_{B_1} \lambda_{B_2}^{OC} + S_{B_2} \lambda_{B_1}^{OC}$	$B_1$ or ( $B_2$ ) delivering energy, and $MWH$ transporting energy.	$P_{20}$
		$B_1$ (or $B_2$ ) fails open circuit, and $B_2$ (or $B_1$ ) able to provide all the energy.	$(1 - S_{B_1}) \lambda_{B_2}^{OC} + (1 - S_{B_2}) \lambda_{B_1}^{OC}$	FAILED	$P_{21}$
		$B_1$ or $B_2$ fails short circuit.	$\lambda_{B_1}^{SC} + \lambda_{B_2}^{SC}$	FAILED	$P_{22}$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{23}$
		$B_1$ delivering energy, and $MWH$ transporting energy.	$P_6$	$B_1$ fails.	$\lambda_{B_1}$
$MWH$ fails.	$\lambda_{MWH}$	FAILED		$P_{25}$	
$B_1$ delivering energy, and $G$ generating energy, and $MWH$ transporting energy.	$P_9$	$B_1$ fails open circuit, and $G$ able to provide all the energy.	$S_G \lambda_{B_1}^{OC}$	$G$ generating energy, and $MWH$ transporting energy.	$P_{26}$
		$B_1$ fails open circuit, and $G$ not able to provide all the energy.	$(1 - S_G) \lambda_{B_1}^{OC}$	FAILED	$P_{27}$
		$B_1$ fails short circuit.	$\lambda_{B_1}^{SC}$	FAILED	$P_{28}$
		$G$ fails open circuit or fails undervoltage, and $B_1$ able to provide all the energy.	$S_{B_1} (\lambda_G^{OC} + \lambda_G^{UV})$	$B_1$ delivering energy, and $MWH$ transporting energy.	$P_{29}$
		$G$ fails open circuit or fails undervoltage, and $B_1$ not able to provide all the energy.	$(1 - S_{B_1}) (\lambda_G^{OC} + \lambda_G^{UV})$	FAILED	$P_{30}$
		$G$ fails short circuit or overvoltage.	$\lambda_G^{SC} + \lambda_G^{OV}$	FAILED	$P_{31}$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{32}$

Table 3

System level FMEA for third failures.

System state with two failures	State probability	Failure mode	Failure rate	System state with three failures	State probability
$G$ generating energy, and $MWH$ transporting energy.	$P_{11}$	$G$ fails.	$\lambda_G$	FAILED	$P_{33}$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{34}$
$B_2$ delivering energy, and $MWH$ transporting energy.	$P_{14}$	$B_2$ fails.	$\lambda_{B_2}$	FAILED	$P_{35}$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{36}$
$B_1$ or ( $B_2$ ) delivering energy, and $MWH$ transporting energy.	$P_{20}$	$B_1$ (or $B_2$ ) fails.	$\lambda_{B_1} + \lambda_{B_2}$	FAILED	$P_{37}$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{38}$
$G$ generating energy, and $MWH$ transporting energy.	$P_{26}$	$G$ fails.	$\lambda_G$	FAILED	$P_{39}$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{40}$
$B_1$ delivering energy, and $MWH$ transporting energy.	$P_{29}$	$B_1$ fails.	$\lambda_{B_1}$	FAILED	$P_{41}$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{42}$

Table 4

Simplified system level FMEA for first failures.

System state with no failures	State probability	Failure mode	Failure rate	System state with one failure	State probability
$B_1$ Delivering energy, and $G$ generating energy, and $DS$ monitoring the system, and $MWH$ transporting energy.	$P_0$	$B_1$ fails covered.	$c\lambda_{B_1}$	$B_2$ delivering energy, and $G$ generating energy, and $MWH$ transporting energy.	$P_1$
		$B_1$ fails uncovered.	$(1 - c)\lambda_{B_1}$	SYSTEM FAILS	$P_2$
		$G$ fails covered.	$c\lambda_G$	$B_1$ delivering energy, and $B_2$ delivering energy, and $MWH$ transporting energy.	$P_3$
		$G$ fails uncovered.	$(1 - c)\lambda_G$	SYSTEM FAILS	$P_4$
		$DS$ fails.	$\lambda_{ECU} + 3\lambda_{SW} + 3\lambda_S$	$B_1$ delivering energy, and $G$ generating energy, and $MWH$ transporting energy.	$P_5$
		$MWH$ fails.	$\lambda_{MWH}$	SYSTEM FAILS	$P_6$

Table 5

Simplified system level FMEA for second failures.

System state with one failure	State probability	Failure mode	Failure rate	System state with two failures	State probability
$B_2$ delivering energy, and $G$ generating energy, and $MWH$ transporting energy.	$P_1$	$B_2$ fails.	$\lambda_{B_2}$	FAILED	$P_7$
		$G$ fails.	$\lambda_G$	FAILED	$P_8$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_9$
$B_1$ delivering energy, and $B_2$ delivering energy, and $MWH$ transporting energy.	$P_3$	$B_1$ fails.	$\lambda_{B_1}$	FAILED	$P_{10}$
		$B_2$ fails.	$\lambda_{B_2}$	FAILED	$P_{11}$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{12}$
$B_1$ delivering energy, and $G$ generating energy, and $MWH$ transporting energy.	$P_5$	$B_1$ fails.	$\lambda_{B_1}$	FAILED	$P_{13}$
		$G$ fails.	$\lambda_G$	FAILED	$P_{14}$
		$MWH$ fails.	$\lambda_{MWH}$	FAILED	$P_{15}$

Table 6  
Component failure rates and detection probabilities used in the development of the simplified Markov model.

Component	Description	$\alpha$	$\lambda_0$ (/h)	$\lambda$ (/h)	D
Alternator	$G$	2.68	$0.32 \cdot 10^{-5}$	$\frac{2.68}{3.1 \cdot 10^5} \left( \frac{t}{3.1 \cdot 10^5} \right)^{1.68}$	0.99
Main battery/backup battery	$B_1/B_2$	3.56	$0.21 \cdot 10^{-4}$	$\frac{3.56}{4.8 \cdot 10^4} \left( \frac{t}{4.8 \cdot 10^4} \right)^{2.56}$	0.99
Main wire Harness	$MWH$	1.95	$0.32 \cdot 10^{-6}$	$\frac{1.95}{3.1 \cdot 10^6} \left( \frac{t}{3.1 \cdot 10^6} \right)^{0.95}$	-
Electronic control unit	$ECU$	1	$5 \cdot 10^{-7}$	$5 \cdot 10^{-7}$	-
Voltage and current sensors	$S_V/S_A$	1	$10^{-7}$	$10^{-7}$	-
Switches	$SW_1/SW_2/SW_3$	1	$10^{-6}$	$10^{-6}$	-