The Fault Avoidance and The Fault Tolerance Approaches for Increasing the Reliability of Aerospace and Automotive Systems

Marcelo Lopes de Oliveira e Souza
National Institute for Space Research - INPE / Space Mechanics and Control Division - DMC. Av. dos Astronautas, 1758, CEP: 12201-970, Jardim da Granja. São José dos Campos – SP – Brasil. marcelo@dem.inpe.br

Terezinha Ribeiro de Carvalho
National Institute for Space Research - INPE / Space Systems Division - DMC. Av. dos Astronautas, 1758, CEP: 12201-970, Jardim da Granja. São José dos Campos – SP – Brasil. tere@dss.inpe.br

ABSTRACT

In this work we discuss the fault avoidance and the fault tolerance approaches for increasing the reliability of aerospace and automotive systems. This includes: the basic definitions/concepts (reliability, maintainability, availability, redundancy, etc.), and characteristics (a priori analysis, a posteriori analysis, physical/hardware redundancy, analytical/software redundancy, etc.) of both approaches, their mathematical background and models (exponential, Weilbull, etc.), their basic theory, their methods and techniques (fault trees, dependence diagrams, Markov chains, etc.), some of their standards (SAE-ARP4761, AC 25.1309, etc.) and simulation environments (Cafta, etc.), and their applications to the reliability analysis and reliability improvement of aerospace and automotive vehicles. This is illustrated by some examples driven from the aerospace and automotive industries.

INTRODUCTION

Since its beginning, the aerospace industry became one of the main users and beneficiaries of the System Engineering, stimulating and permitting the development of procedures and tools even more powerful. Among them, one of the most relevant is the Systems Reliability. This intends to capture the requirements of reliability of all partners of a product, process, etc., unfold them down into specifications for all phases of its development, and provide means of analysis for the verification of the phases, and for the validation and certification of the product, process, etc. Systems Reliability has revealed itself as a powerful contributor to the Safety Assessment in the phases from the specification to the accreditation; and to orient decisions and actions of modification, modernization, suspension and even cancellation of the product, process, etc.

Motivated for such uses, lets state the Systems Reliability Problem, the Fault Avoidance Approach and the Fault Tolerance Approach to solve it; summarize the basic concepts, methods, techniques, languages, environments used on them; discuss both Approaches for increasing the reliability of aerospace and automotive systems; and illustrate them by some examples driven from the aerospace and automotive industries.

BASIC DEFINITIONS/CONCEPTS, TYPES, CHARACTERISTICS, ETC.

Reliability - The probability that a device or system will perform a required function_under stated conditions for a stated period of time.

This is the basic property of a system which we seek to enhance through the concept of fault tolerance. It is stated in statistical terms - as a probability - which reflects the fact that failures occur at unpredictable times. This establishes at the outset the fact that much of the analysis in this paper will have to be statistical in nature.

Maintainability - The probability that a device or system will be retained in or restored to operational

condition in a specified period of time with prescribe procedures and resources.

When applied to a component of a system, maintainability is a property not only of the design of the component but also of its installation in the system. It is expressed as a probability - reflecting the uncertainty in the time required for maintenance actions. The phrase “will be retained in” is included in the definition in addition to “or restored to” to reflect the false alarm situation in which maintenance action is requested when, in fact, no equipment failure has occurred.

Availability -The probability that a system is capable of performing its required function at a stated instant in time.

This is the property of most direct consequence in many mission situations - such as a ballistic missile which may be commanded to launch at any time or an aircraft at the gate which is loaded and scheduled to depart. The same idea is embodied in the term **operational readiness,** which is often used in the context of military systems and is defined in different ways which are meaningful in specific application areas. **The availability of a system clearly depends on both the reliability and the maintainability of that system.**

Redundancy - The property of a device or system wherein it has more than one means of performing its function.

This is the property of a system which allows it to tolerate a failure of one or more of its components. A system which has no redundancy is often termed **simplex**. Notice that this definition, unlike that given in [1], does not require that the redundancy be in the form of additional components, usually called **physical/hardware redundancy**. This reflects the fact that an alternative is additional data processing which provides more than one way to derive needed information; this is usually called **analytical/software redundancy**.

Redundant components can be operated in two fundamentally different ways in a system. **Active redundancy** refers to a system configuration in which all components are operating at all times. In this case, redundant sets of components can be used to check for consistency in their operation. The alternative is **standby redundancy**, wherein the redundant components are inoperative until needed and are then switched into service. In this case, the decision that a standby component is required must be made by some other means not utilizing the information which the redundant component could provide.

Coverage -The property of a system which defines its ability to tolerate failures of a specified subset of its components.

Redundant systems may be designed to provide coverage for failures of some of its components but not all of them. A system may also be designed to cover the first failure of a component of a certain type, but not the second. The coverage provided by a system is a specific description of its level of redundancy.

In addition to these fundamental concepts related to reliability, there are several commonly used acronyms which we shall define at this point.

BITE - Built-In Test Equipment. This refers to special monitoring circuits or other means of indicating directly the operating condition of some components or subsystems. It is often true that BITE signals indicate some modes of component failure but not others. It is also true that BITE equipment is itself subject to failure.

MTBF – Mean Time Between Failures. This common indicator of the reliability of components and systems is defined in the context of mission situation wherein equipment that has failed is repaired and returned to service. In that context, MTBF is the expected time during which the component will perform properly between failures. The same concept applies in situations which do not admit repairs - which case it would be more meaningful to call this expected operating time the **Mean Time To Failure (MTTF)**.

It is, of course, possible that the mean time to the first failure of a component (MTTF) is different from the mean time to another failure following a failure and repair. It depends on whether or not the repaired component is “as good as new” -meaning that its lifetime characteristics after repair are essentially the same as for a new component of that type. In practice, one rarely has enough information to distinguish MTBF from MTTF, and the two terms will generally be used interchangeably in this paper.

MTTR - Mean Time To Repair. This is the expected time it will take to return a device or system to service following a call for maintenance. This statistic plays the same role for maintainability that MTTF does for reliability.

FDI - Failure Detection and Isolation. This is the function of detecting the occurrence of component failures in operating systems and isolating or identifying the component which has failed. FDI implies a decision-making process; it is implemented in some forms of fault-

tolerant systems but not all. This will be the subject of considerable discussion and analysis in subsequent papers.

MATHEMATICAL BACKGROUND AND MODELS

In performing a quantitative assessment of the reliability of a system, which we have concluded must be statistical in nature, the fundamental starting point is a statistical description of when in time the components may be expected to fail. For each component, this description must reflect what is known about that class of components - in terms of actual life time history if there is one established, or in terms of anticipated performance in the case of a new design. There are several functional forms which are often used to represent these failure distributions; the most popular of them will be presented in this section.

The best way to characterize components of a given type is to make a number of them - as many as possible - and put them on life test. When this is done, the data are often recorded in the form of one data point recorded in each of the time intervals indicated on the time axis. The plotted data are called "**Relative Rate of Failure**;" these points have been defined in the following manner: the number of components operating at the beginning of each time interval have been noted - define N_O to be the number operating at t_O. Then the number of components that fail in the following interval (t_O, $t_O + \Delta t$) are noted -call it N_F. The Relative Rate of Failure in that interval is then defined to be

$$\text{Relative Rate of Failure} = \frac{N_F}{N_O \Delta t} \qquad (1)$$

which is in general a function of to. Results of lifetime tests for most components may be expected to have the general character of a "**bath tube curve**". The curve may not be flat in the central region, but it is likely to have a larger rate of failure in the beginning, a lower rate for some succeeding period of time, and an increasing rate later on.

The Relative Rate of Failure as defined above would appear to depend on the data observation interval, Δt, as well as to. If this were so, the data would be hard to interpret in general terms because Δt is quite arbitrary. However, one would surely expect the typical number of failures in the interval, N_F, to decrease with decreasing Δt, and one might even expect that if Δt is small enough, the number of failures in the interval should be proportional to Δt. This is indeed generally true, and in that case the Relative Rate of Failure has a well-defined limit as the interval width approaches zero. That limit is, of course, independent of the length of any arbitrary time interval and is a generally useful measure of the lifetime characteristics of the component. One must also recognize that enough data must be taken so the random fluctuations in number of failures can be averaged out. The resulting limit based on the expected number of failures in the interval is known as the **failure rate**.

$$\text{Failure rate} = \lim_{\Delta t \to 0} \; E\left(\frac{N_F}{N_O \Delta t}\right) = \lambda(t_O) \qquad (2)$$

In some writings, this quantity is referred to as the **hazard rate**.

lf the failure rate for a certain type of component is given for all t, the reliability properties for that type of component are fully defined. Call the time at which the component fails T; it is a random variable. Also let P(E) denote the probability of the event E. From the definition of the failure rate given above, we can see that

$$\lim_{\Delta t \to 0} P(t < T \leq t+\Delta t \mid T > t) = \lim_{\Delta t \to 0} \lambda \Delta t \qquad (3)$$

or, from the definition of conditional probability,

$$\lim_{\Delta t \to 0} \lambda \Delta t = \lim_{\Delta t \to 0} \frac{P(t < T \leq t + \Delta t), T > t}{P(T > t)}$$

$$= \lim_{\Delta t \to 0} \frac{P(t < T \leq t + \Delta t)}{P(T > t)} \qquad (4)$$

since the event $T > t$ is implied by the event $t < T \leq t+\Delta t$.

Now define the **reliability** of the component to be the probabi1ity, as a function of time, t, that the component will perform properly over the interval (0,t).

$$\text{Reliability} = R(t) = P(T > t) \qquad (5)$$

Then Eq. (4) can be rewritten in terms of the component reliability as:

$$\lim_{\Delta t \to 0} \lambda(t) \Delta t = \lim_{\Delta t \to 0} \frac{R(t) - R(t + \Delta t)}{R(t)}$$

$$\lambda(t)R(t) = \lim_{\Delta t \to 0} \frac{R(t) - R(t + \Delta t)}{\Delta(t)} = - \frac{dR(t)}{dt} \qquad (6)$$

This is a simple first-order differential equation for the component reliability which has the solution

$$R(t) = \exp\left(-\int_0^t l(t)dt\right) \qquad (7)$$

This solution reflects the initial condition R(0) = 1 which implies the assumption that the component is working at the initia1 time represented by t = 0.

So the complete history of the component reliability is defined by the history of failure rate. A related function which conveys the same information is the probability density function for the random variable **T - the time of failure**. If we call this **probability density function f(t)**, we can write its relation to reliability as

$$R(t) = \int_t^\infty f(t)dt \qquad (8)$$

or alternatively

$$f(t) = -\frac{dR(t)}{dt} \qquad (9)$$

Comparison with Eq. (6) gives another useful relation

$$f(t) = \lambda(t)R(t) \qquad (10)$$

The probability density function expresses, in a limiting sense, the unconditional probability that the component will fail in the vicinity of time t whereas the failure rate expresses in the same sense the conditional probability of that event, given that the component is still working at t.

A typical failure rate history shows the characteristic, which we have described as typical, of a higher initial failure rate followed by a period of lower failure rate, which may be nearly constant, and an eventual rise in failure rate. Also shown on such figures are failure rate histories due to three commonly distinguished causes. The initial large failure rate is usually ascribed to defects which have escaped notice during the manufacturing process. These failures are called **early failures** and the period in which they occur is often called the **"infant mortality"** period. Because the defects tend to cause the components to fail early, they can be largely eliminated, or "weeded out," by operating the components for a period of time before putting them into service. This practice, called "burning in" the components, *is* universal in applications requiring high reliability. *Since* most of the early failures are taken during the burn-in period, we shall not concern outselves with a mathematical model of the failure rate in that interval. Rather, we shall suppose that *in* all cases of high reliability systems, the components, and perhaps the system as a whole, have been subjected to a burn-in test, and we will think of the time scale of importance to the system as beginning at the end of the burn-in period when most of the defective components have been weeded out.

The failures which occur *in* the mid part of the life of a component -which may represent a large fraction of the component's lifetime - are usually called **chance failures**. This technology *is* not accurate because these failures are due to chance no more than are the other failures. We agreed in the previous section that all failures are due to causes, and it *is* only the unpredictability of the times of failures and the specific cause of each failure that requires us to treat failures as random events. Nevertheless we will use the rather standard terminology of "chance failures" *in* referring to the failures which are not due to specific defects -which tend to cause early failures -nor due to wearout effects -which are responsible for the rising failure rate later on. The failure rate *in* the chance failure region is more nearly uniform than in the early or late periods - and may be usefully approximated as constant in many instances.

The most common form of probability density function used to represent the statistics of failure times in this interval is the **Weibull distribution**. By appropriate choice of its parameters, the Weibull distribution can model a constant failure rate or monotonically increasing or decreasing failure rates. The form of this probability density function as used in failure modeling is

$$f(t) = kmt^{m-1}\exp(-kt^m) \qquad t \geq 0$$

$$= 0 \qquad t < 0 \qquad (11)$$

with k > 0, m > 0, and neither k nor m is restricted to integers. The corresponding failure rate is

$$\lambda(t) = kmt^{m-1} \qquad (12)$$

and the reliability is

$$R(t) = \exp(-kt^m) \qquad (13)$$

By proper choice of the parameters k and m, one can fit failure rate curves which are constant or are either increasing or decreasing with time.

The case of constant failure rate, m = 1 in the Weibull distribution, deserves special attention. From the expressions above we see that in this case,

$$\lambda(t) = k \qquad (14)$$

$$f(t) = k \exp(-kt) \quad (15)$$

$$R(t) = \exp(-kt) \quad (16)$$

Because of the exponential form of the probability density function, this distribution of time to failure is called the **exponential distribution**. This distribution is widely used in reliability analyses because many components display failure rates which are nearly constant for a large part of their lifetime. Moreover, the exponential is a limiting distribution in failure modeling in much the same way that the normal is a limiting distribution in other statistical contexts. Just as the Central Limit Theorem requires, under certain conditions, that the distribution of the sum of independent random variables tend toward the normal, so too does the reliability of a component or system which *is* subject to failure due to a large number of independent causes tend toward the exponential form under certain conditions.

The use of the exponential distribution of failures is widespread in reliability analyses because of its analytic simplicity as well as its fidelity in modeling actual failure distributions. Many of the test procedures required by military specifications to evaluate the reliability of components or systems are based on the assumption of constant failure rate and the resulting exponential distribution of time to failure.

As discussed in the previous section, a statistic associated with the failure distribution which is often subject to specification, or is cited as a general indicator of the lifetime of a component, is the expected value of the failure time. This is called **the mean time to failure, or MTTF**, in situations where component repairs are not possible, and **mean time between failures, or MTBF**, in situations where failed components are repaired and returned to service. This quantity is defined by the relation

$$\overline{T} = \int_0^\infty t f(t) dt \quad (17)$$

which can also be expressed as

$$\overline{T} = \int_0^\infty R(t) dt \quad (18)$$

provided that $\lim_{\Delta t \to 0} tR(t) = 0$. For the general Weibull distribution, the mean time to failure is

$$\overline{T} = \frac{1}{k^{1/m}} \Gamma\left(\frac{1}{m} + 1\right) \quad \text{(Weibull)} \quad (19)$$

where $\Gamma(x)$ is the Gamma function. For the exponential distribution,

$$\overline{T} = \frac{1}{l} \quad \text{(Exponential)} \quad (20)$$

It is often the case that the interval of chance failures is long enough relative to the mission time or to the useful lifetime of a component so that **wearout failures** are not considered in reliability analyses. In those cases where wearout failures are significant, the Weibull distribution can be used to model them because for $m > 1$ it produces an increasing failure rate with time. A distribution more commonly used for this purpose is the **truncated normal distribution** which is the normal distribution truncated to positive values of its argument. In terms of the normalized normal probability density function

$$f(t) = \frac{1}{\sqrt{2p}} \exp(-t^2/2) \quad (21)$$

and the standard normal probability integral

$$f(t) = \int_{-\infty}^{t} f(x) dx \quad (22)$$

the truncated normal probability density function is a

$$f(t) = \frac{a f[a(t - t_m)]}{f(at_m)} \quad (23)$$

The parameter a controls the spread of the distribution; it plays a role similar to the reciprocal of the standard deviation in the usual normal distribution. The corresponding reliability is

$$R(t) = \frac{f[a(t_m - t)]}{f(at_m)} \quad (24)$$

and the failure rate is

$$l(t) = \frac{a f[a(t - t_m)]}{f[a(t_m - t)} \quad (25)$$

The mean time to failure for this distribution is

$$\overline{T} = t_m + \frac{f(at_m)}{af(at_m)} \qquad (26)$$

Many other failure distributions have been suggested as applicable to particular types of components. The interested reader will find a variety of them in References.

If one wishes to account **for both chance and wearout failures** and use a different failure model to represent each, one can treat the failure rates as additive.

$$l(t) = l_C(t) + l_W(t) \qquad (27)$$

This is equivalent to modeling the failures of the two types as independent, since Eq. (7) then gives

$$R(t) = R_C(t)R_W(t) \qquad (28)$$

In most cases the resulting probability density function for the failure time is not of simple form. It is given by

$$f(t) = R_C(t)f_W(t) + R_W(t)f_C(t) \qquad (29)$$

The reliability given in Eq. (28) is the unconditional probability that the failure time will be greater than t. One is often more interested in the conditional probability that the component or system will operate properly over an interval (t_O,t) given that it is operating at to. This models the usual mission situation in which one determines through some check-out tests that the equipment is functioning properly at the start of the mission, and one is interested in the probability that it will function properly during the mission given that facto The distinction between this conditional probability and the unconditional probability is often forgotten or ignored because in the commonly assumed case of the exponential distribution of failure times the two are the same. The conditional reliability of a component over the interval (t_O,t) given that it is operating at time t_O, is

$$P(T > t|T > t_O) = \frac{P(T > t, T > t_O)}{P(T > t_O)}$$

$$= \frac{P(T > t)}{P(t > t_O)}$$

$$= \frac{R(t)}{R(t_O)} \qquad (t \geq t_O) \qquad (30)$$

For the exponential distribution,

$$P(t > t|T > t_O) = \frac{\exp(-kt)}{\exp(-kt_O)}$$

$$= \exp[-k(t - t_O)] \qquad (31)$$

This shows that the absolute time in the life of a component with exponential failure characteristics is not important -it has the same reliability characteristics following any time at which it is determined that the component is working as it does from time zero when it is first put into service.

But this is not true of other failure distributions, and especially when one accounts for wearout failures the actual age of the component is of obvious importance. For the truncated normal distribution,

$$P(T > t|T > t_O) = \frac{f[a(t_m - t)]}{f[a(t_m - t_O)]} \qquad (32)$$

For a given mission duration, t – t_O, this probability decreases as the age of the component at the start of the mission, t_O, increases.

When both chance and wearout failures are accounted for, the conditional reliability has the form

$$P(T > t|T > t_O) = \frac{R_c(t)R_W(t)}{R_c(t_O)R_W(t_O)} \qquad (33)$$

If chance failures are modeled as exponential and wearout failures as truncated normal, this becomes

$$P(T > t|T > t_O) = \frac{f[a(t_m - t)]}{f[a(t_m - t_O)]}\exp[-k(t - t_O)] \qquad (34)$$

With the parameters of this distribution (a, t_m, k) given for a component or system, a family of curves of conditional reliability vs. mission time for various values of age at the start of the mission can be prepared. These curves would be similar to the previous ones but would account for chance failures as well as wearout failures. Having these data, one can determine the maximum age of the component, t_O, which will give a specified reliability over a given mission time. This is the basis for **preventive maintenance** programs in which parts are replaced at a certain age even if they are functioning normally at that time.

METHODS AND TECHNIQUES

The standard SAE-ARP4761 treats the safety assessment of civil aircraft. As such, it includes and describes the following safety analysis methods: the Fault Tree Analysis-FTA, Dependence Diagram-DD, Markov Analysis-MA, Failure Modes and Effects Analysis-FMEA, Failure Modes and Effects Summary-FMES, and Common Cause Analysis-CCA. CCA is composed of Zonal Safety Analysis-ZSA, Particular Risk Analysis-PRA, and Common Mode Analysis-CMA. Some of them include reliability analysis as described below.

Having described the most common models used to characterize the reliability properties of components, we turn now to the analysis of the reliability of systems comprised of a number of such components.

The Direct Combinatorial Method discussed in this section is most applicable to relatively simple situations - where the system configuration is not too complex, where it is not necessary to consider a multiplicity of failure modes for each component, and where the possible imperfections of a failure detection mechanism are not considered.

In most of this section, and indeed in most reliability analyses, the assumption is used that component failures are independent of each other. The assumption of independence should be considered carefully in each situation. It is entirely possible, in the case of systems employing a number of components of the same type, that the mode of failure of these components may be the same. That is, when these components fail, they tend to fail for the same reason. But the existence of a common cause of failure for a group of components does not necessarily imply statistical dependence among the failure times for these components. On the other hand, an environmental stress which is common to a group of components would tend to produce dependent failures. It is also some - times true that failure of one component creates an abnormal condition in the system which tends of induce further component failures. Whether or not this type of dependence must be considered in analyzing the reliability of the system depends on the configuration of the system: if the first failure of a component of this type causes failure of the system, then the analysis stops with the first component failure and the subsequent failure of additional components is of no consequence. If, however, the component is in a redundant configuration where the first component failure does not imply system failure, then the possible dependent failures of additional components is important to the continued operability of the system.

The simplest system configuration to analyze, and probably the most common configuration, is the **simplex system** (also referred to as a "single-string" system) wherein there is no redundancy. This implies that every component must function if the system is to function. We are considering here the simplest case in which we recognize only two states for each component and also for the system as a whole - working or failed. It is meaningful in some situations to identify a number of modes of failure for each component with each failure mode having a different degree of impact on the operability of the system. But for the two-state case and a simplex configuration, the system reliability function is the probability of the event that all of its components are working - and under the assumption of independence of component failures, that probability is the product of the reliabilities of all the components.

$$R_S(t) = \prod_i R_i(t) \qquad \text{(simplex system)} \quad (33)$$

This relation makes it clear why reduction of parts count is so important in the design of reliable systems. Even if each part is quite reliable, the system may not be very reliable if a large number of parts are required. For example, if the reliability of each component of a system is 0.999 over a specified mission time, the reliability of the system is 0.905 if 100 components are involved and is only 0.368 if 1000 components are required.

If each of the components of a simplex system is characterized by a Weibull distribution of time to failure, with possibly different values of the parameters k and m introduced in Eq. (11), then the system reliability is

$$\mathrm{R_S(t) = \prod_i \exp[-k_i t^{m_i}] = \exp[-\sum_i k_i t^{m_i}]} \quad (34)$$

If the parameters m_i of the component distributions are all equal, this becomes

$$R_S(t) = \exp[-(\sum_i k_i)t^m] \qquad (35)$$

and we see that in this case the system also has the Weibull distribution of time to failure with the same value of m as for the components and with k equal to the sum of the k_i for the components. In particular, if all the component failure times are exponentially distributed (m_i= 1), the system failure time is also exponentially distributed and k in this case is equal to the system failure rate:

$$k = l_S = \sum_i l_i \qquad \text{(exponential distribution)} \quad (36)$$

Equivalently, the system MTTF can be expressed in terms of the component MTTFs as

$$\frac{1}{\overline{T}_S} = \sum_i \frac{1}{\overline{T}_i} \qquad \text{(exponential)} \qquad (37)$$

Recall that all of this is based on independence of component failures.

The Reliability Block Diagram Method. In the analysis of the reliability of more complex system configurations it is helpful to portray the effects of component failures in a pictorial manner which one can readily visualize. We will call such a representation a reliability block diagram. A simplex system, as discussed above, fails if any of its components fail. This characteristic is naturally associated with a series configuration in which the path from one end to the other is broken if any of the elements in the series breaks. This is pictured in Figure 2.3-1.

It is essential to understand that the topology of a reliability block diagram is usually different from that of the system it models. For example, a feedback amplifier may consist of a collection of transistors, resistors and capacitors connected in a complex manner with local groups of components connected in series, others in parallel, and with one or more closed feedback loops. Nevertheless, if the amplifier functions properly only if all of its components do, then the reliability block diagram of the feedback amplifier is just a series configuration.

The alternative to a simplex system is a **redundant system** for which by definition there is more than one combination of system components that enable the system to perform its function. The simplest form of redundancy is direct replication in which several copies of a component are installed in the system, any one of which can perform the required function. A common example of this is a spacecraft attitude control system with duplicate sets of reaction control jets and their related plumbing and gas supplies. Both sets of jets are commanded to operate by the attitude control system and the system can function satisfactorily if either jet system performs properly.

Directly redundant links of the simplest type where there is no need to decide that an element has failed and take action to bring a redundant element into operation, have reliability block diagrams of parallel structure as shown in Figure 2.3-2. This diagram conveys the message that the link functions if any of the elements in parallel functions. The link then fails only if all the elements in parallel fail, and for independent failures the link unreliability (1 -R) is the product of the component unreliabilities. Call the unreliability Q(t); this is the probability that a component or system has failed by time t.

$$Q(t) = P(T < t) = 1 - R(t) \qquad (38)$$

For a parallel reliability block diagram,

$$Q_S(t) = \prod_i Q_i(t) \qquad \text{(parallel diagram)} \qquad (39)$$

or equivalently,

$$R_S(t) = 1 - \prod_i [1 - R_i(t)] \qquad \text{(parallel)} \qquad (40)$$

These expressions assume independent component failures.

Unlike the case of a series configuration, a link with elements in parallel does not have the exponential distribution of time to failure even when all of its elements do. The mean time to failure for the parallel group can be calculated when the individual components all are exponentially distributed, but even that result is complex when the failure rates of the components are not the same. But the case of most common interest involves identical components in parallel. Then the failure rate for each component is the same and the mean time to failure for the parallel combination is

$$\overline{T}_S = \frac{1}{l} \sum_{k=1}^{n} \frac{1}{k} \qquad \text{(exponential)} \qquad (41)$$

Direct redundancy can be quite helpful with failures considered independent. For example, if the reliability of each component over a given mission time is 0.8, the reliability of a parallel group of 3 of them is 0.992. Similarly, the mean time to failure for a parallel set of 3 exponentially distributed components is 11/6 times the mean time to failure for each component.

Another situation of common interest is exemplified by a system having n power supplies with m < n required to supply the load. If these components are identical and failures are considered independent, then the probability that exactly k of them are functioning is

$$\text{P (k work)} = \frac{n!}{k!(n-k)!} R^k (1-R)^{n-k} \qquad (42)$$

To compute the probability that m or more of the units work, this probability must be summed over k from m to n.

The parallel reliability block diagram corresponds to the case of active redundancy in that all units are considered to be functioning all of the time. Each component then accumulates failure probability from the beginning of the problem. An alternate form of redundancy is use of **inactive spares** wherein only one component is operative at any one time, and when it fails a spare is called upon to take over its function. This arrangement is also referred to as **standby redundancy**. An idealization of this situation is the case in which we have n identical components, only one of which is operative at any one time, and in which we assume that inactive spares have zero failure rate. Each component then begins to accumulate failure probability only when it is placed into service. If the components are further assumed to have the exponential distribution of time to failure, the reliability of this configuration is

$$R_S(t) = e^{-lt}[1 + lt + \frac{1}{2} l^2 t^2 + \cdots + \frac{(lt)^{n-1}}{(n-1)!}] \quad (43)$$

which is a Gamma distribution.

According to standard SAE-ARP4761, other methods are:

The Fault Tree Analysis Method-FTA It "uses Boolean logic gates to show the relationship of failure effects to failure modes. The two most common logic gates are the AND-gate and the OR-gate. An AND-gate represents a condition in which the coexistence of all inputs is required to produce an output representing the higher level event. An OR-gate represents a condition in which one or more outputs produce an output representing the higher level event.". This analysis technique uses probability to assess whether a particular system configuration or architecture will meet the mandated requirements.

The Dependence Diagrams Method–DD It "replaces the FTA logic gates by paths to show the relationship of the failures; parallel paths are equivalent to the AND-gates and series paths are equivalent to the OR-gates". "They are essentially equivalent to FTAs and the selection of one over the other is left to the personal preference of the analyst.".

The Markov Analysis Method-MA It "calculates the probability of the system being in various states as a function of time. A state in the model represents the system status as a function of both the fault-tree and faulty components and the system redundancy. A transition from one state to another occurs at a given transition rate, which reflects component failure rates and redundancy. A system changes state due to various events such as component failure, reconfiguration after detection of failure, completion of repair, etc. Each state transition is a random process which is represented by a specific differential equation. The differential nature of the model limits the computation at any point in the analysis tot the probability of transitioning from any defined state to another state. The probability of reaching a defined final state can be computed by combinations of the transitions required to reach that state." It is suited to treat more complex situations with computer help. They are often useful when dealing with deferred maintenance scenarios.

The Failure Modes and Effects Analysis Method-FMEA It "is a systematic, bottom-up method of identifying the failure modes of a system, item, or function and determining the effects on the next higher level. It may be performed at any level within the system (e.g., piece-part, function, blackbox, etc.). Software can also be analyzed quantitatively using a functional FMEA approach. Typically, na FMEA is used to address failure effects resulting from single failures." It is a useful tool to examine total system integrity using a bottom-up approach. Certain parts of systems may be subject to scrutiny as they represent single point failures and as such more detailed analysis is warranted.

The Failure Modes and Effects Summary-FMES It "is a grouping of single failure modes which produce the same failure effect (i.e., each unique failure effect has a separate grouping of single failure modes). An FMES can be compiled from the aircraft manufacturer's, system integrator's or equipment supplier's FMEAs. Furthermore, an FMES should be coordinated with the user to adequately address the need for inputs to higher level FMEAs and/or System Safety Assessment FTAs."

The Common Cause Analysis-CCA It ".provides the tools to verify the independence, or to identify specific dependencies between functions, systems or items to satisfy the safety requirements. In particular, the CCA identifies individual failure modes or external events which can lead to a catastrophic or hazardous/severe-major failure condition. Such common cause events must be precluded for catastrophic failure conditions and must be within the assigned probability budget for hazardous/severe-major failure conditions.".

SOME STANDARDS

The standard SAE-ARP4761 describes "guidelines and methods of performing the safety assessment for certification of civil aircraft. It is primarily associated with showing compliance with Federal Aviation Regulations-FAR/ Joint Airworthiness Requirements-JAR 25.1309. The methods outlined there identify a systematic means, but not the only means, to show compliance. A subset of such

material may be applicable to non-25.1309 equipment. The concept of Aircraft Level Safety Assessment is introduced and the tools to accomplish this task are outlined. The overall aircraft operating environment is considered.”.

The Part 25 airworthiness standards are “based on, and incorporate, the objectives, and principles or techniques, of the fail-safe design concept, which considers the effects of failures and combinations of failures in defining a safe design. Section 25.1309(b) and (c) sets forth certain objective safety requirements based on this design concept. Many systems, equipment, and their installations have been successfully evaluated to the applicable requirements of Part 25, including § 25.1309(b), (c), and (d), without usiny structured means for safety assessments. However, in recent years there has been an increase in the degree of system complexity and integration, and in the number of safety-critical functions performed by systems. Difficulties had been experienced in assessing the hazards that could result from failures of such systems, or adverse interactions amony them. These difficulties led to the use of structured means for showing compliance with § 25.1309(b). For this and other reasons, guidance was needed on acceptable means of-compliance with § 25.1309(b), (c), and (d).

The Advisory Circular AC 25.1309 describes “various acceptable means for showing compliance with the requirements of § 25.1309(b), (c), and (d) of the Federal Aviation Regulations (FAR). These means are intended to provide guidance for the experienced engineering and operational Judgment that must form the basis for'compliance findings. They are not mandatory. Other means may be used if they show compliance with this section of the FAR.”.

Besides these standards that include reliability analysis, we highlight among others:

MIL-STD-690C Failure Rate Sampling Plans and Procedures This standard provides procedures for failure rate qualification, sampling plans for establishing and maintaining failure rate levels at selected confiden ce levels, and lot conformance inspection procedures associated with failure rate testing for the purpose of direct reference in appropriate military electro nic parts established reliability (ER)specifications. Figures and tables through out this standard are based on exponential distribution.

MIL-STD-721C Definition of Terms for Reliability and Maintainability This standard defines terms and definitions used most frequently in specify ing Reliability and Maintainability (R & M). Provides a common definition for the Department of Defense and defense contractors.

MIL-STD-756B Reliability Modeling and Prediction This standard establishes uniform procedures and ground rules for the gene rating mission reliability and basic reliability models and predictions for electronic, electrical, electromechanical, mechanical, and ordnance systems and equipments. Model complexity may range from a complete system to the simplest subdivision of a system. It details the methods for determining service u se (life cycle), creation of the reliability block diagram, construction of the mathematical model for computing the item reliability.Some simple explanations on the applicability and suitability of the various prediction sources and methods are included.

MIL-STD-781D Reliability Design Qualification and Production Accept ance Tests: Exponential/ Distribution This document covers the requirements and provides details for reliability testing during the development, qualification, and production of systems and e quipment with an exponential time-to-failure distribution. it establishes the tai lorable requirements for reliability testing performed during integrated test programs specified in mil-std-785. task descriptions for reliability development/ growth testing (rd/gt), reliability qualification testing (rqt), produ ction reliability acceptance tests (prat), and environmental stress screen ing(ess)are defined.test time is stated in multiples of the design mean time between failures (mtbf). specifying any two of three parameters, i.e., lower test mtbf,upper test mtbf,or their ratio, given the desired decision risks, de termines the test plan to be utilized. this standard is applicable to six broad categories of equipment, distinguished according to their field service applications.

SOME SIMULATION ENVIRONMENTS

As the other sections may suggest, any method of evaluating the reliability of a system in terms of the reliability of its components becomes extremely laborious for systems with reasonably complex reliability block diagrams. The best approach in such cases would be use of a computerized algorithm based on techniques of graph theory.One can attempt to use computer help either to produce a computable expression for the system reliability or to obtain numerical results via **Monte Carlo Analysis**. In either case one needs an algorithm to analyze the connectedness of networks under various failure states , and the necessary software is not simple. So, it will be treated in this section. Among them we highlight:

Reliability Prediction Programs
Detailed Stress Prediction Programs
Parts Count Prediction Programs
Mechanical Prediction Programs

Non-Operating Prediction Programs
Other Electronic Prediction Method Programs

System Modeling Programs
Reliability Modeling Programs
Availability Modeling Programs
Markov Modeling Programs
Other Programs
FMECA/FMEA Programs
Fault Tree Analysis Programs
Reliability Testing/Data Analysis Programs
FRACAS Programs
Maintainability Prediction Programs
Computerized Maintenance Management Systems
Logistics Programs
Safety Analysis Programs
Worst Case Analysis Programs
Sneak Circuit Analysis Programs
ESD Susceptibility Programs
Root Cause Analysis Programs

Examples are:

1) ITEM ToolKit: (See http://www.itemsoft.com/) ITEM ToolKit is a fully integrated Reliability and Safety Analysis software program, conforming to well established and recognised techniques. It consists of the following modules:

-Reliability Prediction MIL-HDBK-217 (Electronic)
-Bellcore (Electronic)
-NSWC-98/LE1 (Mechanical)
-RDF 2000 (Electronic)
-China 299B (Electronic)
-Failure Mode Effects and Criticality Analysis (FMECA)
-Reliability Block Diagram (RBD)
-Fault Tree Analysis (FTA)
-Event Tree Analysis (ETA)
-Binary Decision Diagram (BDD)
-Markov Analysis (MKV)
-MIL-HDBK-472 (MTTR)
-Spares Scaling and Ranging
-AvailabilitySimulation

2) Life Data Analysis (Weibull Analysis). (See http://www.weibull.com/). In life data analysis (also called "Weibull analysis"), the practitioner attempts to make predictions about the life of all products in the population by "fitting" a statistical distribution to life data from a representative sample of units. The parameterized distribution for the data set can then be used to estimate important life characteristics of the product such as reliability or probability of failure at a specific time, the mean life for the product and failure rate. Life data analysis requires the practitioner to:

-Gather life data for the product.
-Select a lifetime distribution that will fit the data and model the life of the product.
-Estimate the parameters that will fit the distribution to the data.
-Generate plots and results that estimate the life characteristics, like reliability or mean life, of the product.

3) Relex Software. (see http://www.relexsoftware.com/customers/index.asp). the relex reliability suite includes reliability prediction software and reliability analysis software - to improve the design, build, and test phases of product development. in addition, relex fracas for corrective action management to ensure that information from actual product deployments can be used to improve the next generation of product design. for larger-scale, web-based deployments, reles offers enterprise solutions quality management systems.

4) CAFTA for Windows (See http://www.saic.com) Cafta is a comprehensive PC-based fault tree workstation with support for all phases of systems analysis. Includes full screen editor, multilevel reli ability database, plotting, cut set generator, cut set results editor. Ex tensive syntax and logic checking, logical editing, supports macros, calculates unavailability from failure rate and exposure times, user de finable fields, truncates on cut set probability or size, allows user se lectable gate transfers & page breaks. Program also supports sensiti vity studies.

DISCUSSION OF THE FAULT AVOIDANCE AND THE FAULT TOLERANCE APPROACHES

The System Reliability Problem, the Fault Avoidance Approach and the Fault Tolerance Approach for its solution are best illustrated by an example: A large commercial airliner descends through heavy fog toward a landing at a major airport. There are several hundred passengers aboard. The ceiling and visibility are zero-zero. The pilot is absolutely dependent upon the automatic landing system to get the plane down safely (CAT.3). This is no time for one of the components of that system to fail! So, this allow us to state

The System Reliability Problem: The design of a device or system that will perform a required function under stated conditions for a stated period of time.

Following **the Fault Avoidance Approach**, those components have been designed to the highest standards for long life, have been manufactured under the strictest quality control requirements, have been thoroughly tested before being put into service, and have been maintained on

a regular schedule. In spite of all this, an amplifier fails at this critical time as the airplane approaches the runway.

This event could spell disaster with hundreds of lives lost. But instead, following **the Fault Tolerant Approach,** the aircraft continues smoothly on its path to a safe landing. The passengers are not even aware that a failure has occurred. The Flight Engineer knows of it because a message has appeared on his display stating that **a failure** of the amplifier **has been detected and that the system has been reconfigured** to continue operation without the use of that channel.

This is an example of a fault-tolerant control system in action. Such a system is designed with **redundant capacity** to perform its mission; that is, it can do its job using more than one configuration of its components and information processing capability. **Redundancy** can be realized in the form of additional components beyond the minimum number required to perform the needed functions, usually called **physical/hardware redundancy;** or in the form of supplemental data processing capacity which is used to process information in the system in different ways depending on what components are functioning, usually called **analytical/software redundancy**. Fault tolerance is a system property which is corning into increasing prominence in the thinking of those who specify the requirements for new systems and of those who design then. There are many application areas, in addition to the **blind landing system**, where **ultra-high reliability** is necessary or desirable. One such area is the control of **nuclear power plants** where the consequences of improper control system behavior may be serious indeed. There are **space missions** for which the desired operational lifetime of the spacecraft is many years. The **air traffic control system** and many **military systems** are also subject to **high reliability** requirements. There is also a desire for **increased reliability** in computerized **banking systems, telephone systems, chemical process control systems, medical monitoring systems**, and many more. As a result, growing attention is being given to

The Fault Avoidance Approach: the design of systems and components for long life, with quality control during manufacture, with testing and maintenance policies which enhance reliable operation.

But because all that is still not enough to meet some reliability requirements, there is increasing interest in

The Fault Tolerance Approach: The design of systems which can tolerate component failures and continue to function.

A good overview of both approaches for the space area is presented by Wertz and Larson (1999) Lets summarize it:

"DESIGN FOR FAULT AVOIDANCE

Fault avoidance is most effective when there are only a very small number of significant failure modes. Common fault avoidance techniques are shown in Table 1, and application guidance is provided below.

Table 1. Representative Methods for Fault Avoidance.

Technique	Most Suitable for	Limitations
Process Control	Current deficiencies exist	User must be able to influence process
Design Margins, etc.	Know failure risk	Adds weight and cost
Coding Techniques	Memory upset	Digital components only
Part Selection and Screening	Modest improvement required	Critical measurements must be known

Process Control

Control of the manufacturing process can only be exercised where parts are specifically manufactured for the spacecraft.

Design Margins, Derating and Environmental Protection

Design margins and derating accomplish the same goal: prevention of component failure due to higher than expected external stresses or other deviations from the nominal conditions.

Coding Techniques

Coding provides robustness by permitting continued operation in the presence of a defined spectrum of errors, primarily in memory and data transmission.

Part Selection and Screening

Screening (selection of parts by test) is a process that eliminates units that have a higher likelihood of failing in service than the other units in the lot.

DESIGN FOR FAULT TOLERANCE

Fault tolerance protects against a wider spectrum of failure modes than fault avoidance. In most cases it also requires much more resources. A summary of the suitability and limitations of representative fault tolerance techniques is shown in Table 2.

TABLE 2. Representative Fault Tolerance Techniques.

Technique	Protection Against	Limitations
Same Design Redundancy	Random failures	High production cost, weight
Diverse Design Redundancy	Random and design failures	Same, plus design and logistic cost
K-Out-Of-N Redundancy	Random failures	Applicable only where multiple Copies of an article are present
Functional Redundancy	Random and design failures	Diverse methods to accomplish a Function must be available
Temporal Redundancy	Transient, intermittent failures	Time required for recovery

Same Design Redundancy

Same design redundancy involves installation of two or more identical components together with switching to make one of them active.

Diverse Design Redundancy

Installation of two or more components of different design (called *diverse design redundancy*) to furnish the same service has two advantages: it offers high protection against failures due to design deficiencies, and it can offer lower cost if the back-up unit is a "lifeboat", with lower accuracy and functionality, but still adequate for the minimum mission needs.

Functional and Temporal Redundancy

Functional redundancy **(sometimes called *analytic redundancy*)** involves furnishing a service by diverse means. An example is the determination of attitude rate from a rate gyro assembly (direct), and from observation of celestial bodies (indirect).

Temporal redundancy involves repetition of an unsuccessful operation. A common example is a retry after a failure within the computing process. The same technique is applicable to acquisition of a star, firing of a pyrotechnic device, or communication with the ground.".

EXAMPLES FROM AEROSPACE AND AUTOMOTIVE INDUSTRIES

Among the many examples now available, we highliht:

Schweizer (1985) presents "the design of a fault management system (FMS) for an unmanned and untethered platform. The system must automatically detect, diagnose, localize and reconfigure the system to cope with failures. Traditional fault tolerant approaches used in telephone switching, manned and unmanned satellites, commercial banking, airline reservations, air traffic control, and others are reviewed by them. Expert systems technology is used to extend these traditional approaches to achieve a highly reliable design capable of sustaining operation over many months with little or no communication. An existing simulator has been modified to allow fault injection and to model fault propagation. This provides a testbed for evaluating system candidates. A specific fault management hardware and software architecture has been selected. Expert system diagnostic rules, which run on the fault tolerant base, are discussed by them. Diagnostic rule performance in detecting, localizing, and recovering from Autonomous Systems (AS) sensor, actuator, and computer subsystem failures during as operation is analyzed by them.".

Lussier,et alli (2005) consider that "autonomous systems are starting to appear in space exploration, elderly care and domestic service; they are particularly attractive for such applications because their advanced decisional mechanisms allow them to execute complex missions in uncertain environments. However, systems embedding such mechanisms simultaneously raise new concerns regarding their dependability. They aim in that paper to present these concerns and suggest possible ways to resolve them. They address dependability as a whole, but focus specifically on fault tolerance. They present some particularities of autonomous systems and discuss the dependability mechanisms that are currently employed. They then concentrate on the dependability concerns raised by decisional mechanisms and consider the introduction and assessment of appropriate fault tolerance mechanisms.".

Avizienis (1997) states that "as computing and communications become irreplaceable tools of modern society, one fundamental principle emerges: The greater the benefits these systems bring to our well-being and quality of life, the greater the potential for harm when they fail to perform their functions or perform them incorrectly. Consider air, rail, and auto-mobile traffic control; emergency response systems; airline flight controls; nuclear power plant safety systems; and most of all, our rapidly growing dependence on health care delivery via high-performance computing and communications. When these systems fail, lives and fortunes may be lost. At the same time, threats to dependable operation are growing in scope and severity. Leftover design faults (bugs and glitches) cause system crashes during peak demand, resulting in service disruptions and financial losses. Complex systems suffer stability problems due to unforeseen interactions of over-lapping fault events and mismatched defense mechanisms. Hackers and criminally minded individuals invade systems, causing disruptions, misuse, and damage. Accidents result in severed communication links, affecting entire regions. Finally, we face the possibility of systems damage by "info-terrorists." Fault tolerance is our best guarantee that high-confidence systems will not betray the intentions of their builders and the trust of their users by succumbing to physical, design, or human-machine interaction faults, or by allowing viruses and malicious acts to disrupt essential services.".

Baleani et alli (2003) argue that "fault-tolerant electronic sub-systems are becoming a standard requirement in the automotive industrial sector as electronics becomes pervasive in present cars. They address the issue of fault tolerant chip architectures for automotive applications. They begin by reviewing fault-tolerant architectures commonly used in other industrial domains where fault-tolerant electronics has been a must for a number of years,

e.g., the aircraft manufacturing industrial sector. They then proceed to investigate how these architecture could be implemented on a single chip and they compare them with a metric that combines traditional terms such as cost, performance and fault coverage with exibility, i.e. the ability of adapting to changing requirements and capturing a wide range of applications, an emerging criterion for platform design. Finally, they describe in some details a cost effective dual lock-step platform that can be used as a single fail-operational unit or as two fail-silent channels trading fault-tolerance for performance.".

Shirvani and McCluskey (1998) describe "the ARGOS project at Stanford CRC. The primary goals of this project are to collect data on the errors that occur in digital integrated circuits in a space environment, to determine the tradeoffs between fault-avoidance and fault-tolerance, and to see if radiation hardening can be avoided by using fault tolerance techniques. Their experiments will be carried out on two processor boards on the ARGOS experimental satellite. One of the boards uses radiation-hardened components while the other uses only commercial off-the-shelf (COTS) parts. Programs and data can be uploaded to the boards during the mission. This capability allows them to evaluate different software fault-tolerance techniques. Their report reviews various error detection techniques. Software techniques that do not require any special hardware are discussed. The framework of the software that they are developing for error data collection is presented.".

Dias (1998) presents "a systematics of product project for reliability. It aims at structuring a model which takes into account the concept of reliability in the project process, particularly in informational and conceptual project stages. The proposition has been applied to a mains gas project in the metropolitan area of Curitiba, Paraná, Brazil. Through its application, it was possible to highlight the importance of understanding the existing principles and correlations in the attribute reliability for the project process. In order to do so, some points have been considered: the meaning of the terms which make up the definition of reliability; the correlation with project process stages; and the way of classifying the activity to guarantee reliability along the life cycle. The work also presents information regarding the failure rate of the items used in the mains, the reliability model and the alterations recommended for the mains conceptual project, ai ming to increase reliability in gas supply for consumers.".

Heidergott (2005) affirms that "development of highly reliable and available systems requires consideration of the occurrence of single event upsets-SEUs, the effects they have on system performance, and strategies for their prevention and mitigation. Methods of systems engineering process and the application and validation of techniques for fault tolerance are discussed as elements in the elimination and mitigation of single event upsets.".

Müller and Plankensteiner (2002) defends that "without doubt, fault-tolerance is one of the major challenges that must be met for the design of dependable or safety critical electronic systems. Formerly treated as just one aspect of the functional requirements, it has become increasingly obvious that fault-tolerance is a design property of its own right, and that creating and handling the fault-tolerance in a system requires a clear methodology no less rigid than reliable functional design. The Time-Triggered Architecture utilizes an approach to systematic fault-tolerance: out of non-fault-tolerant components, a highly predictable distributed system - a time-triggered network – can be designed, and the fault-tolerance properties of such a system (as well as many functional aspects) can be verified by formal means. For many systems, the redundant use of simple components is superior in both cost and reliability to a singe fault-tolerant component. Time-Triggered Architecture systems can be designed and implemented with hardware and software products available on the market today.".

INPE (2001) presents a document and its annexes that "contain the data for the System Requirements Review (SRR) of the Brazilian Multi-Mission Platform (MMP).
The objective of the corresponding meeting is to perform a System Requirements Review (SRR) of the Multi-Mission Platform. The Multi-Mission Platform (MMP) was conceived to be a versatile platform to be used in several application satellite missions of the PNAE. Among the missions that will use the MMP are SSR-1, SCD-3, SSR-2 and possibly SABIA (or ABE), depending on the task distribution between Brazil, Argentina and Spain. The first satellite to use the MMP will be the SSR-1, an equatorial mission to monitor the Amazon region. With development of the MMP, INPE will acquire the technology of three-axis stabilized satellites with fine pointing accuracy. This is a fundamental step towards the Brazilian autonomy in satellite technology field."
That document includes a reliability analysis section that "presents the MMP reliability analysis used to support the MMP reliability subsystems allocation. MMP has a reliability figure of 0.8000 for 4-year life time. Based on this figure the reliability allocation was performed to each subsystem. The reliability allocation process included the failure rate/reliability estimation and the mathematical model implementation in accordance with the MMP reliability block diagram. The result of this reliability analysis made possible the subsystem allocation and the reliability summary analysis.".

CONCLUSIONS

In this work we discussed the fault avoidance and the fault tolerance approaches for increasing the reliability of aerospace and automotive systems. This included: the basic definitions/concepts (reliability, maintainability, availability, redundancy, etc.), and characteristics (a priori analysis, a posteriori analysis, physical/hardware redundancy, analytical/software redundancy, etc.) of both approaches, their mathematical background and models (exponential, Weilbull, etc.), their basic theory, their methods and techniques (fault trees, dependence diagrams, Markov chains, etc.), some of their standards (SAE-ARP4761, AC 25.1309, etc.) and simulation environments (Cafta, etc.), and their applications to the reliability analysis and reliability improvement of aerospace and automotive vehicles. This was illustrated by some examples driven from the aerospace and automotive industries.

BIBLIOGRAPHICAL REFERENCES

1-IEEE, IEEE Standard Dictionary of Electrical and Electronics Terms, Wiley - Interscience, New York, 1977.

2-The Reliability Design Handbook, No. RDH376, Rome Air Development Center, Griffiss Air Force Base, NY, 1976.

3-Moir, I., Seabridge, A. Aircraft Systems: Mechanical, Electrical, and Avionic Subsystems Integration. AIAA, Reston, VA, USA, 2001.

4-Vesely, W. E.,Goldberg, F. F.,Roberts, N. H., Haasl, D. F. Fault Tree Handbook NUREG-0492,US Nuclear Regulatory Comission. Washington, DC,1981.

5-Drenick, R.F. The Failure Law of Complex Equipment, Journal of SIAM, Vol. 8, 1960, p. 680.

6-Lloyd, D.K. and M. Lipow: Reliability: Management, Methods and Mathematics, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1962.

7-Mann, N.R., R.E. Shafer and N.D. Singpurwella: Methods for Statistical Analysis of Reliability and Life Data, Wiley, N.York, 1974.

8-Singpurwella, N.D.: "Statistical Fatigue Models: A Survey," IEEE Transactions on Reliability, Vol. R-20, pp. 185-189, 1971.

9-Amoroso, A.L. Um Método de Análise, e Especificação de Sistemas com Requisitos de Desempenho, Custo e Confiabilidade, Aplicado a Rodas a Reação. INPE, SJC, SP, Brasil, 04/10/1999 (INPE-7517-TDI/730).

10-Wertz, J.R., Larson, W. J. (eds.) Space Mission Analysis and Design (3rd. edition). Microcosm Press, CA, and Kluwer Academic Pub., Dordrecht, Holland, 1999.

11-Schweizer, P. F. Knowledge Based Management of Failures in Autonomous Systems. Westinghouse R&D Center, Pittsburgh, PA 15235, 1985.

12-Lussier, B., Lampe, A., Chatila, R., Guiochet, J., Ingrand, F., Killijian, M. O., Powell, D. Fault Tolerance in Autonomous Systems: How and How Much. LAAS, France, 2005.

13-Avizienis, A. Toward Systematic Design of Fault-Tolerant Systems. University of California – Los Angeles, April 1997.

14-Baleani, M., Ferrari, A., Mangeruca, L., Sangiovanni-Vincentelli, A., Peri, M., Pezzini, S. Fault-Tolerant Platforms for Automotive Safety-Critical Applications. Proceedings of the 2003 International Conference on Compilers, Architecture and Synthesis for Embedded Systems. pp. 170-177. San Jose, California, USA, 2003.

15-Shirvani, P. P., and McCluskey, E. J. Fault-Tolerant Systems in a Space Environment: The CRC ARGOS Project. Center For Reliable Computing, Computer Systems Laboratory, Department of Electrical Engineering and Computer Science, Stanford University, Stanford, California, December 1998. (CRC Technical Report No. 98-2) (CSL TR No. 98-774).

16-Heidergott, W. SEU Tolerant Device, Circuit and Processor Design. General Dynamics C4 Systems, Scottsdale, Arizona, USA, 2005.

17-Müller, A., and Plankensteiner, M. Fault-Tolerant Components versus Fault-Tolerant Systems. TTTech Computertechnik AG, Vienna, 2002.

18-INPE. Multi-Mission Platform Data Package For System Requirements Review (SRR). INPE, S.J.Campos, SP, 2001.

ABOUT THE MAIN AUTHOR

Dr. Marcelo Lopes de Oliveira e Souza is an Electronics Engineer by the Instituto Tecnológico de Aeronáutica-ITA, at São José dos Campos, São Paulo, Brazil in 1976. Since then, he is a Registered Professional

Engineer in Brazil by the Federal Council of Engineering, Architecture and Agronomy-CONFEA, Section of São Paulo-CREA-SP. He joined the National Institute of Space Research-INPE at São José dos Campos, São Paulo, Brazil in 1977 in the first group to learn and work with satellites there. He was at the first satellite technical mission of INPE/Brazil to learn and work at the Centre National D´Etudes Spatiales-CNES, in Toulouse, France in 1979. He is a Master in Space Sciences/Orbital Mechanics by INPE in 1980. He is a Ph.D. in Aeronautics and Astronautics by the Massachusetts Institute of Technology-MIT at Cambridge, Massachusetts, USA, in 1985. He is a Professor & Senior Researcher of the Space Mechanics and Control Division-DMC of INPE since 1991, where he is coordinating the Laboratory for Simulation, Identification and Modeling Environments-LABSIM2 of Attitude and Orbit Control Systems-AOCS since 2002. Since 1977 he has worked and supervised works in various aspects of AOCS; and later, on Modeling, Identification, Simulation and Control of Dynamic (mainly Aerospace) Systems, and their Development Environments. He is a senior member of prestigious societies like the AIAA, ISA, MIT Alumni Association, etc. in whose journals and congresses he has published many works on those and related areas. Write to marcelo@dem.inpe.br or:

Marcelo L. O. Souza
Professor and Senior Researcher
National Institute for Space Research-INPE
Division of Space Mechanics and Control-DMC
Av. dos Astronautas, 1758 Satellite Building, Room 27
São José dos Campos, São Paulo, 12227-010, Brazil