Évitement des défaillances, tolérance aux pannes

Par le Dr William Marshall, Éditeur Contenu Central Semiconducteurs

Après l'annonce et le lancement des microcontrôleurs de « sécurité » Texas Instruments, Freescale et Infineon, le** Dr William Marshall présente **ici le premier volet d'une série d'articles sur la théorie et les techniques pratiques qui se cachent derrière la fiabilité et la redondance en matière de systèmes de sécurité critique.

Dans le dernier quart du 20e siècle, le terme « ordinateur » est devenu synonyme de manque de fiabilité. Chaque fois qu'un système tombait en panne, la faute était attribuée à une erreur informatique. Cette causalité souvent injustifiée est devenue une excuse facile pour couvrir les erreurs humaines commises par les programmeurs ou les opérateurs. L'ordinateur est ainsi devenu le bouc émissaire de nos propres échecs et cette situation semblait satisfaire tout le monde, tant que les soi-disant « erreurs informatiques » n'étaient pas à l'origine de blessures ou de décès. Mais la technologie a évolué et les ordinateurs ont trouvé leur place dans les voitures, puis dans les avions, où la gestion de fonctions non critiques en terme de sécurité, telles que les essuie-glaces et la navigation, leur a été confiée. Tout a changé avec l'informatisation des systèmes de contrôle aérien : dans un premier temps pour les avions militaires, puis civils, comme l'Airbus A320. Aujourd'hui, même les voitures sont équipées d'une multitude de microcontrôleurs chargés de gérer leurs fonctions de sécurité, telles que le freinage d'urgence et l'activation des airbags. Google a récemment démontré que les voitures sans chauffeur étaient tout à fait possibles dans la pratique. En quoi cela a-t-il changé l'attitude du public vis-à-vis des erreurs informatiques ?

Les constructeurs d'avions et d'automobiles ont heureusement réalisé qu'il n'était pas acceptable de qualifier de « simples erreurs informatiques » les accidents responsables de centaines de morts. Au cours des cinquante dernières années, de nombreuses recherches visant à rendre les ordinateurs « infaillibles » ont suivi deux angles d'attaque : l'évitement des pannes, puis la tolérance aux pannes, grâce à des machines plus intelligentes.
En tant que concept, la fiabilité informatique peut avoir autant de définitions qu'il existe d'opérateurs et d'utilisateurs. Ces définitions dépendent également du point de vue : un installateur informatique pourra considérer que son système est fiable si les performances répondent dans l'ensemble aux exigences. L'avis de l'opérateur pourra être beaucoup moins favorable si, pour obtenir ces performances, il doit corriger des erreurs et régulièrement faire appel à un technicien de maintenance pour remplacer des composants. Le technicien de maintenance pourra juger que le système n'est pas du tout fiable s'il doit prendre des mesures préventives, localiser des pannes potentielles et résoudre d'autres pannes avant que des erreurs n'apparaissent « en aval ». Cette approche humaine traditionnelle de la fiabilité n'est tout simplement pas satisfaisante dans le cas des systèmes de sécurité, tels que les systèmes de contrôle aérien.

Définition du terme fiabilité
• **La fiabilité** est la probabilité qu'un système donné accomplisse une fonction requise dans des conditions déterminées pour une durée défi nie dans le temps. Elle est donc fonction du temps et varie entre 1 (totalement fiable) et 0 (pas du tout fi able). L'objectif du concepteur est de maintenir ce chiffre le plus près possible du 1 pour le système, et ce le plus longtemps possible, ou du moins jusqu'à la fi n de la mission ou de la durée de fonctionnement requise. Au cas où quelque chose ne fonctionnerait pas sur le système, des définitions de base sont nécessaires pour les termes panne, défaillance et erreur :

• Le terme **panne** fait référence à la cause directe d'un fonctionnement incorrect du système. Il peut s'agir d'une panne de matériel, de synchronisation ou de logiciel (bogues). Elle peut également être de nature permanente ou transitoire.
• Le terme **défaillance** fait référence à un écart par rapport aux spécifications du système en raison d'une panne. Cela signifie que le processeur passe à un état incorrect après un certain nombre d'états corrects.
• Le terme **erreur** fait référence à la manière dont la défaillance de la machine se manifeste dans un calcul de programmation particulier.
Pendant la conception d'un système, les causes possibles de pannes doivent être prises en compte. On parle alors de « menaces ».
• Le terme **menace** fait référence au stress qui produit une panne. Il peut s'agir d'une erreur environnementale normale, anormale ou d'une erreur de conception.
Deux hypothèses sont nécessaires pour obtenir une fonction mathématique de la fiabilité : d'une part, les défaillances du dispositif sont aléatoires et donc statistiquement indépendantes les unes par rapport aux autres et, d'autre part, le taux de défaillance, exprimé en nombre de défaillances par heure, est une constante pendant tout le cycle de vie de l'équipement. Bien que fragiles, ces deux hypothèses ont prouvé qu'elles étaient raisonnablement valides pour les analyses de systèmes, à condition que certaines conditions soient remplies.

L'indépendance statistique suppose qu'une défaillance de composant n'augmentera pas le stress subi par un composant voisin et n'augmentera donc pas son taux de défaillance.

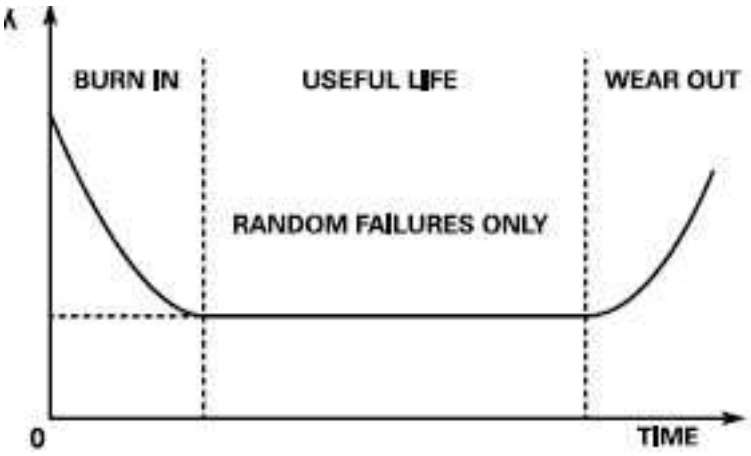


Figure 1. Taux de défaillance d'un composant en fonction du temps
Lorsque les ordinateurs étaient fabriqués à partir de transistors, de résistances et d'autres composants discrets, un court circuit aux bornes d'un condensateur, par exemple, pouvait provoquer une surcharge sur un transistor et entraîner une suite de défaillances. Les éléments logiques des circuits intégrés sont moins susceptibles d'entraîner des dommages en cascade et devraient se rapprocher davantage du modèle de fiabilité. La constance du taux de défaillance peut être obtenue en ignorant les phases de « rodage » et d'« usure » du cycle de vie du système et en utilisant uniquement la partie plate de la courbe. La phase de rodage devrait éliminer la totalité des défauts intrinsèques aux composants, des erreurs de conception matérielle et des « bogues » de programmation. La fiabilité théorique d'un module de système non redondant en fonction du temps s'exprimera donc ainsi :
R(t) = e-lt où l correspond à un taux de défaillance constant.
Ceci permet d'obtenir la courbe exponentielle de la figure 2. Le module est en théorie parfaitement fi able. R(t) = 1 lorsque le temps = 0, c'est-à-dire lorsque le système entre dans la phase de taux de défaillance constant de son cycle de vie (figure 1).

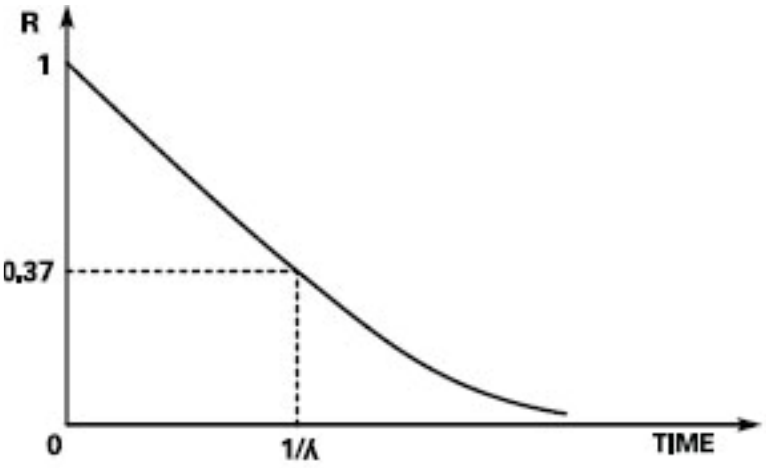


Figure 2. Fiabilité d'une unité simplex

Évitement des pannes

Il est bien sûr nécessaire de trouver un moyen de déterminer le moment où le taux de défaillance du système devient constant. Une méthode coûteuse consiste à tester le système jusqu'à ce qu'il quitte sa phase de rodage. Seuls les constructeurs d'équipements militaires ou critiques pour la santé réalisent généralement ce type de test. Dans le cas des systèmes commerciaux et domestiques, les nouveaux produits sont souvent testés sur les consommateurs et le calcul de fiabilité ajusté en fonction des plaintes reçues. Fréquemment utilisée comme paramètre de fiabilité, la durée moyenne entre les pannes(MTBF) correspond tout simplement à l'inverse du taux de défaillance. Pour déterminer le paramètre I ou la durée MTBF d'un module, les taux de défaillance de tous les composants sont ajoutés, conformément à l'hypothèse d'indépendance statistique. La courbe de la fi gure 2 montre que lorsque t = MTBF, R(t) = 0,37. En d'autres termes, lorsque l'âge du système se rapproche de la durée MTBF, la probabilité d'un fonctionnement sans défaillance continu est de 37 % seulement. Les processus traditionnels d'évitement des pannes et de tolérance aux pannes visent à augmenter la durée MTBF du système en améliorant les durées MTBF de chacun de ses modules et composants. Cette méthode est utilisée jusqu'à ce que le temps de mission ou le cycle de vie requis pour l'équipement soit considérablement inférieur à la durée MTBF du système, d'où une probabilité de fonctionnement correct de
90-99 %, par exemple. Le temps de mission sert généralement de base de calcul, notamment dans le cas des avions militaires, où la durée MTBF peut être de quelques heures seulement. Il existe plusieurs moyens d'éviter les pannes :

• Contrôle de la qualité des composants. Ceci signifie de nos jours une vigilance accrue face aux pièces de contrefaçon.
• Réduction importante de la puissance nominale des composants (en n'utilisant que 10 % des capacités de puissance, par exemple).
• Utilisation des composants à plages de températures automobiles et militaires.
• Réduction du stress environnemental à l'aide de systèmes de refroidissement, etc.
• Réduction du nombre de composants utilisés pour chaque tâche au minimum (conception efficace, sans redondance).

Ces techniques ont été fréquemment utilisées dans les applications militaires à cause de la nécessité de réduire le poids, quel que soit le prix. Le besoin d'une fiabilité durable était généralement secondaire, les temps de mission de ce secteur étant souvent de quelques heures seulement, voire de quelques minutes ou secondes pour les systèmes d'armement, tels que les missiles guidés. Dans le domaine de la défense, la faible détérioration des systèmes stockés sans alimentation pendant de longues durées est plus importante. La sécurité est également moins importante que dans le secteur civil.

Le temps de mission des projets automobiles et aérospatiaux civils peut peut-être lui aussi être court, mais le coût associé à la conception d'un système d'évitement des pannes peut être prohibitif. Heureusement, les circuits intégrés à grande échelle offrent une perspective de tolérance aux pannes abordable, avec des systèmes d'auto-surveillance, de pièces de rechange embarquées et un ré-établissement automatique. Dans les applications non militaires, la tolérance aux pannes rendra le développement de véhicules sans chauffeur non seulement possible, mais également sûr. Dans la deuxième partie de ce dossier, nous examinerons les implications théoriques et pratiques des designs tolérants aux pannes. Nous utiliserons des exemples issus de l'aviation avec l'Airbus, ainsi que de l'exploration spatiale avec la navette et les robots d'exploration planétaire.

www.rs-components.com/electronics