Sécurité fonctionnelle : le point sur la législation

par William Marshall, RS Components

Les systèmes électroniques à sécurité fonctionnelle produiront une sortie prévisible, quelle que soit l'entrée. Tous les systèmes qui prétendent offrir ce type de sécurité doivent être développés et validés conformément à la norme internationale CEI 61508.

Qu'est-ce que la sécurité fonctionnelle ?
À une certaine époque, la sécurité électronique, notamment sur le marché des appareils domestiques, se limitait essentiellement au réglage des composants contre les risques d'électrocution, de surchauffe et d'incendie.
Par exemple, il n'y a pas si longtemps, l'unique appareil électronique des voitures était l'autoradio, et celui-ci ne nécessitait pas de « sécurité fonctionnelle », les pannes d'autoradio ne représentant pas généralement de danger pour la sécurité. Les erreurs imprévues de système de distribution de la force de freinage ou de contrôle de la stabilité dynamique peuvent quant à elles avoir des conséquences fatales, d'où la nécessité de respecter les exigences de la norme CEI 61508 ou de normes plus spécifiques, telles que la norme ISO 26262 relative aux véhicules automobiles. Celle-ci vient juste d'entrer en vigueur et tous les développeurs de systèmes automobiles doivent s'assurer que leurs produits respectent ses dispositions.

Implications liées à la conformité
La sécurité coûte cher. Avant de commencer à développer et à fabriquer un système nécessitant une sécurité fonctionnelle, il est important de comprendre que le respect des normes de sécurité applicables concerne toutes les étapes du processus, de la conception initiale aux tests finaux.
Lorsque l'on travaille avec une conception embarquée, il peut être tentant d'utiliser la déclaration de conformité ISO 61508 SIL 3 du fabricant de puce, par exemple, comme preuve de la conformité de l'ensemble du système. Ceci n'est cependant pas du tout le cas : l'ensemble du système doit être conforme, et non uniquement ses composants individuels. Cela inclut le matériel et les logiciels. Les logiciels correctement développés ne « s'usent » pas et ne font pas l'objet de pannes aléatoires. Les logiciels qui n'ont pas été correctement testés présentent souvent ce type de pannes une fois mis en service, parfois au bout de quelques mois, souvent en raison d'un dépassement négatif ou positif de capacité de pile. Les normes fournissent des directives concernant le niveau de test systématique nécessaire pour atteindre une classe de sécurité particulière.

Dispositions des normes de sécurité fonctionnelle
• Fournissent des processus d'évaluation des risques et d'attribution de cibles de sécurité.
• Aident à réduire les pannes systématiques en indiquant les bonnes pratiques de développement.
• Fournissent un cadre pour l'analyse des taux de pannes aléatoires.
• Fournissent un cadre pour l'analyse de l'efficacité des diagnostics.
• Fournissent des procédures permettant de garantir le maintien des niveaux de sécurité après la livraison du système.

Niveau d'intégrité de sécurité (CEI 61508)
L'une des premières tâches à accomplir lors du développement d'un système nécessitant une sécurité fonctionnelle consiste à réaliser une évaluation des risques et des dangers de l'application cible. Cela signifie déterminer la probabilité de détection de panne acceptable avec arrêt contrôlé du système. Ce taux appelé SFF (Safe Failure Fraction) indiquera le

niveau d'intégrité de sécurité cible (SIL). Sa valeur dépend de la technologie utilisée pour la conception, ainsi que du type de tolérance aux pannes matérielles.

• Type A : tous les mécanismes de panne sont connus.
• Type B : existence de certains mécanismes de panne inconnus

On suppose que la plupart des dispositifs à semi- conducteurs sont de type B.

SFF	**Tolérance aux pannes matérielles**		
	0	**1**	**2**
< 60%		**SIL 1**	**SIL 2**
60 % à < 90 %	**SIL 1**	**SIL 2**	**SIL 3**
90 % à < 99 %	**SIL 2**	**SIL 3**	**SIL 4**
≥ **99%**	**SIL 3**	**SIL 4**	**SIL 4**

Tableau 1. Niveaux d'intégrité de sécurité atteignables avec taux SFF calculé et niveau de tolérance aux pannes matérielles prévu.

Le tableau 1 montre que plus on augmente la tolérance aux pannes d'un système (redondance modulaire triple, par ex.), moins le taux SFF nécessaire pour atteindre un niveau SIL cible particulier est élevé.
Cela ne signifie pas que des composants de mauvaise qualité pourront être spécifiés dans les architectures tolérantes aux pannes. Il s'agit de normes de sécurité, non de fiabilité. Elles sont conçues pour garantir un fonctionnement sûr et un arrêt contrôlé en cas de panne, le cas échéant. Les systèmes informatiques destinés aux véhicules spatiaux robotisés doivent être fiables et leur disponibilité optimale. Des techniques de redondance matérielle peuvent être utilisées pour améliorer cette disponibilité, mais ceci ne servira à rien si les composants utilisés possèdent un taux de défaillance élevé. De la même manière, les automobilistes ne seraient pas impressionnés si leur voiture devait passer la plupart de son temps
au garage, même si les pannes sont sans danger pour leur sécurité !

Un microcontrôleur conforme au niveau SIL 3 IEC 61508 : Texas Instruments TMS570

Le TMS570 est un microcontrôleur à double coeur qui a été conçu pour une intégration dans un système SIL 3. Pour atteindre le niveau SIL 3, une logique de contrôle et de correction des erreurs poussée a été incorporée avec des circuits de test intégrés et les coeurs de processeur ont été dupliqués.

• Le code correcteur élimine les erreurs de mémoire 1 bit au fur et à mesure qu'elles apparaissent.
• Le code correcteur détecte et indique les erreurs d'interconnexion et de mémoire 2 bits.
• La parité est vérifi ée en cours d'exécution pour les tampons et les queues périphériques.
• Le contrôleur CRC de la mémoire permet de valider l'intégrité du code à tout moment.
• Microcontrôleurs et contrôleurs de RAM dédiés.
• Deux coeurs de processeur Cortex-R4F identiques exécutent le même programme avec un léger décalage.

Les deux coeurs de processeur suggèrent une redondance modulaire double (DMR).
Ceci n'est cependant pas le cas. Un coeur de processeur jouant le rôle de « maître » envoie la sortie au microcontrôleur. L'autre coeur est un « esclave » qui exécute le même programme avec un décalage d'1,5 cycle d'horloge par rapport au maître. La sortie provenant de l'esclave sert uniquement à réaliser une comparaison avec le maître : en cas de différence, un signal d'erreur sera déclenché. La sortie du maître est retardée d'1,5 cycle pour permettre l'alignement des entrées dans le dispositif de comparaison. L'objectif de ce «

décalage » est de piéger les erreurs transitoires aléatoires dont la cause pourrait toucher simultanément les deux processeurs.

Les deux coeurs ne sont pas installés dans le même sens sur la matrice pour éviter les pannes liées à une cause physique commune. Ils sont également protégés contre le couplage capacitif par des anneaux de garde individuels.

Sécurité logicielle

Comme nous l'avons suggéré plus haut, les efforts fournis pour concevoir un matériel sûr ne servent pas à grand chose si le logiciel ne subit pas la même rigueur de développement. Prouver que le logiciel d'application répond aux normes de sécurité applicables peut s'avérer long et coûteux. Il est par conséquent recommandé d'utiliser un système d'exploitation préqualifi é pour faciliter son développement. Les systèmes d'exploitation
RTOS (Real-Time Operating Systems) sont de plus en plus utilisés dans les conceptions embarquées en temps réel et sont disponibles en plusieurs versions, un grand nombre d'entre eux étant liés à des familles de microcontrôleurs particulières. Le système RTOS multiplateforme « freeware » FreeRTOS fait partie des systèmes les plus utilisés pour les expérimentations initiales et une version de sécurité, SafeRTOS®, a été certifi ée conforme aux applications SIL3. Basé sur le Cortex-M3, le microcontrôleur Stellaris proposé par Texas Instruments intègre le système SafeRTOS® dans sa ROM, ce qui facilite considérablement les travaux de conception.

Normes

CEI 61508
Sécurité fonctionnelle des systèmes électriques/électroniques et électroniques programmables, CEI 2000
ISO 26262 Véhicules de route – Sécurité fonctionnelle, ISO 2011

POUR EN SAVOIR PLUS
Rendez-vous à l'adresse suivante : rswww.fr/electronique