Comment effacer les obstacles au processus de certification de sécurité fonctionnelle selon l'ISO 26262

Les spécifications de sûreté de fonctionnement de la norme ISO 26262 garantissent que les applications complexes embarquées dans les automobiles fonctionnent de manière sûre. Toutefois, les conceptions conformes et l'obtention de la certification sont des processus qui s'avèrent longs et coûteux. Pour pallier cette difficulté, l'industrie des semi-conducteurs propose aux équipementiers et fournisseurs de l'industrie automobile des « écosystèmes » de sécurité fonctionnelle complets qui minimisent les coûts, les risques et le temps de développement pour mener à bien la certification.

La norme ISO 26262 englobe les spécifications relatives à la sûreté de fonctionnement des systèmes électriques et/ou électroniques installés dans les véhicules routiers de série (à l'exclusion des cyclomoteurs). Publiée en 2011 et révisée en 2018 pour inclure une section sur les semi-conducteurs, cette norme ISO impose un processus de développement allant de la spécification à la mise en production. Les équipementiers et fournisseurs automobiles doivent donc suivre et documenter ce processus lorsqu'ils qualifient des dispositifs destinés à fonctionner à l'intérieur de véhicules routiers nécessitant une sûreté de fonctionnement.

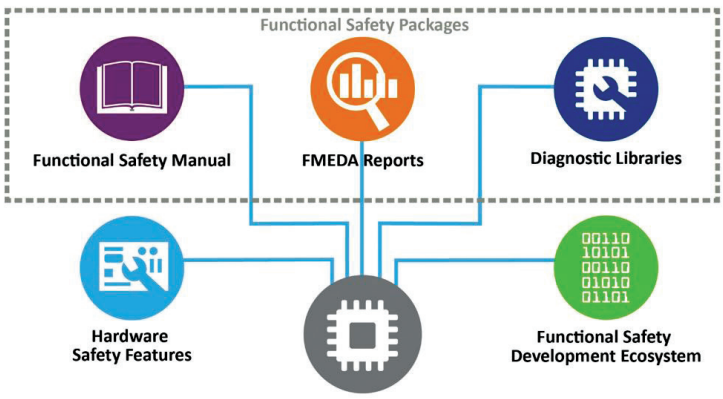
La certification des systèmes est obtenue grâce à la confirmation par un évaluateur indépendant que le système est conforme aux exigences de la norme ISO 26262. Les applications au sein du véhicule sont ainsi classées selon différents niveaux d'intégrité de sûreté automobile (ASIL, Automotive Safety Integrity Level) en fonction de leur niveau de criticité en matière de sûreté et de sécurité. Les niveaux, allant de A à D, sont fondés sur la gravité et la probabilité de blessures potentielles, et sur la mesure dans laquelle elles peuvent être contrôlées. Parallèlement, il existe des exigences de sûreté associées aux composants sous-jacents. Dans ce cadre, le niveau ASIL D représente le plus haut degré de risque automobile pour des applications comme les airbags, le freinage ABS et la direction assistée. De leur côté, les composants tels que ceux utilisés pour les feux arrière sont classés ASIL A, ceux pour les phares et les feux de stop sont généralement classés ASIL B, tandis qu'un système comme le régulateur de vitesse est classé ASIL C. En général, plus le niveau ASIL est élevé, plus les exigences en matière de redondance matérielle sont importantes. A ce niveau, les fournisseurs de composants peuvent contribuer de multiples façons pour accélérer la conception et la certification ISO 26262 d'une application de sécurité (figure 1). Tout d'abord, les dispositifs doivent être soigneusement sélectionnés pour englober les ressources de sécurité fonctionnelle nécessaires. Ces ressources comprennent les rapports d'analyse des modes de défaillance, des effets et des diagnostics (FMEDA, Failure Modes, Effects, and Diagnostic Analysis) et les manuels de sûreté. Ensuite, les dispositifs doivent également être pris en charge par un écosystème de développe-

AUTEUR

Jacob Lunn Lassen, ingénieur de l'équipe technique, Sécurité fonctionnelle, Microchip Technology.

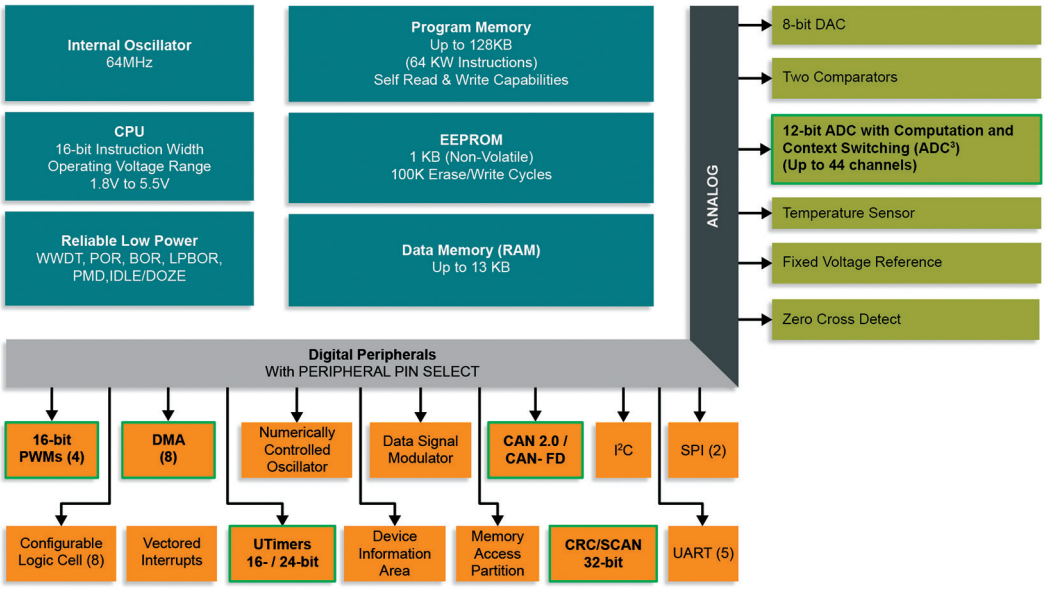
1 RESSOURCES ET ÉCOSYSTÈME DE SÛRETÉ DE FONCTIONNEMENT

Les ressources de sûreté de fonctionnement nécessaires comprennent les rapports d'analyse des modes de défaillance, des effets et des diagnostics (FMEDA) et les manuels de sécurité.



2 MICROCONTRÔLEUR 8 BITS À CARACTÉRISTIQUES MATÉRIELLES DE SÉCURITÉ FONCTIONNELLE

Les microcontrôleurs 8 bits comprennent souvent un sous-système de gestion du bus CAN FD et sont généralement utilisés comme contrôleurs d'interface utilisateur pour les boutons mécaniques et capacitifs dans l'habitacle, le volant, la console centrale ou pour l'accès sans clé, avec en sus des fonctions de sécurité matérielle intégrées.



ment qualifié pour la création d'applications critiques pour la sûreté de fonctionnement.

Aptitude à la sécurité fonctionnelle pour les circuits 8 bits et les DSC

Parmi les nombreux circuits intégrés utilisés dans les automobiles d'aujourd'hui, les microcontrôleurs sont particulièrement répandus et font partie de toutes les unités de commande électronique des voitures afin d'ajouter des fonctions d'assistance à la conduite et autres fonctionnalités sophistiquées. Ces microcontrôleurs vont des systèmes 8 bits optimisés pour les performances, l'efficacité énergétique et le contrôle en temps réel, tout en ajoutant des interfaces tactiles à base matérielle, jusqu'aux circuits 32 bits capables d'exécuter des applications multithreads et dotées de fonctionnalités graphiques, de connectivité et de sécurité. En outre, il existe des contrôleurs de signaux numériques qui combinent un microcontrôleur avec un moteur DSP (Digital Signal Processing) pour assurer des performances déterministes et rapides destinées à la gestion de capteurs, de moteurs ou pour la conversion d'énergie.

Chacun de ces circuits intégrés doit d'abord satisfaire aux normes de qualification automobile en matière de fabrication et de performances, établies notamment par l'Automotive Electronics Council (AEC). Les normes AEC-Q100 définissent un processus de qualification de tests sous contrainte, fondé sur des mécanismes de défaillance aux différentes classes de température. En fonction des applications, un microcontrôleur devra être qualifié AEC Q100 Classe 2, Classe 1 ou Classe 0. (Classe 0 = 150°C, Classe = 125°C, et Classe 2 = 105°C).

Au-delà de la qualification AEC, les exigences supplémentaires pour les fonctionnalités dédiées à la sûreté de fonctionnement dépendent du dispositif et de l'application. À titre d'exemple, les microcontrôleurs 8 bits comprennent souvent un sous-système de gestion du bus CAN FD qui relie des interfaces graphiques avec les réseaux de capteurs intelligents. Ils sont généralement utilisés comme contrôleurs d'interface utilisateur pour les boutons mécaniques et capacitifs dans l'habitacle, le volant, la console centrale ou pour l'accès sans clé. Les fonctions de sécurité matérielle intégrées dont ces circuits ont besoin s'appliquent généralement à la mémoire, à la réinitialisation du système, à l'exécution sécurisée du code, à la communication sécurisée et à la protection des entrées/sorties à usage général. Elles sont ajoutées par l'intégration de périphériques indépendants du noyau et par des fonctions additionnelles comme la réinitialisation à la mise sous tension (POR, Power On Reset), la réinitialisation à la mise hors tension (BOR, Brown-Out Reset), la temporisation « chien-de-garde à fenêtre » (WWDT, Windowed Watch Dog Timer) et le contrôle de redondance cyclique (CRC, Cyclic Redundancy Check), afin d'améliorer la sécurité opérationnelle et la fiabilité (figure 2).

En montant dans l'échelle des circuits jusqu'aux DSC 16 bits compatibles avec la sûreté de fonctionnement, les caractéristiques de sécurité matérielle requises comprennent généralement une mémoire à détection et correction d'erreurs, un autotest intégré à la mémoire (MBIST, Memory Built-In Self Test), une surveillance d'horloge et un oscillateur redondant et d'autres fonctionnalités comme la détection de pannes, des capacités d'autodiagnostic et de diagnostic système et des fonctions d'atténuation des défauts. Ces dispositifs prêts pour la sûreté de fonctionnement permettent de concevoir des applications embarquées, d'interfaçage de capteurs, de puissance numérique et de commande de moteurs à haute performance et à sûreté critique. Les applications typiques sont notamment les systèmes de conversion continu/continu, les chargeurs embarqués (OBC, On Board Charger), les actionneurs et les capteurs (position, pression…), les unités tactiles et autres unités de commande visant la conformité ASIL B ou ASIL C (figure 3).

Aptitude à la sécurité fonctionnelle pour les circuits 32 bits

Comme tous les microcontrôleurs compatibles avec la sûreté de fonctionnement, les systèmes 32 bits ont aussi besoin de caractéristiques matérielles, notamment d'une mémoire à code de correction d'erreurs (ECC, Error Correcting Code) et d'injection de panne, d'un autotest

intégré à la mémoire, de systèmes d'horloge avec oscillateurs de secours, d'une détection de panne d'horloge et de GPIO avec protection contre les décharges électrostatiques (figure 4).

Les moniteurs système sont également importants, notamment les fonctions POR, BOR, WDT et CRC matérielles, ainsi qu'une unité de protection de la mémoire. Les microcontrôleurs 32 bits servent à de nombreuses applications, allant des systèmes embarqués aux systèmes avancés d'aide à la conduite (ADAS), en termes de sécurité fonctionnelle. Il est même possible d'atteindre les niveaux de sûreté ASIL C/D avec des microcontrôleurs et des DSC standard en combinant ces deux types de circuits - DSC primaire associé un microcontrôleur secondaire ou un coprocesseur de sécurité. Pour ce faire, on utilise le principe de décomposition de l'ASIL. Car combiner deux sous-systèmes conformes ASIL B peut permettre d'atteindre un niveau ASIL plus élevé, comme ASIL C/D :

ASIL C = ASIL B (C) + ASIL A (C)

ASIL D = ASIL B (D) + ASIL B (D) = ASIL C (D) + ASIL A (D)

La décomposition est obtenue en divisant les exigences de sûreté en fonction des dispositifs réels.

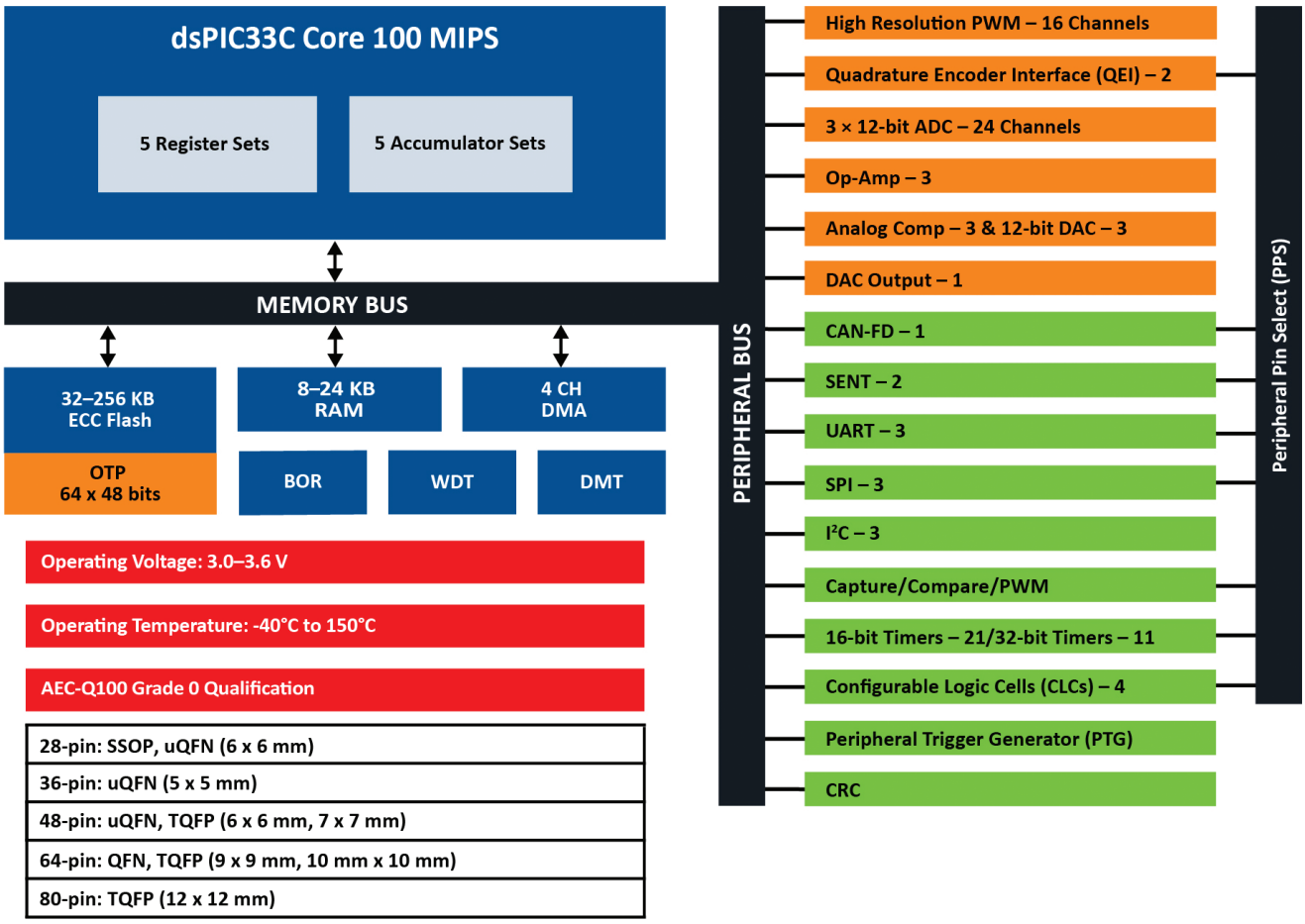
Outils de développement et soutien à la certification

Côté programmation, des ensembles d'outils de conception certifiés pour la sûreté de fonctionnement dans le cadre d'un écosystème de développement complet peuvent faciliter le respect des exigences de vérification et de validation spécifiées dans la norme ISO 26262. C'est particulièrement vrai pour les conceptions à base de microcontrôleurs et de DSC. Les fournisseurs d'outils travaillent à ce niveau avec des organismes indépendants d'évaluation et de certification pour certifier les compilateurs de sécurité fonctionnelle. Ce qui s'accompagne généralement de documents supplémentaires tels que certificat, manuel de sûreté, plan de sécurité et rapports de classification et de qualification des outils pour les compilateurs, l'environnement de développement intégré, les débogueurs et les programmeurs. Ce dossier de sûreté simplifie la qualification des outils et la certification de l'application finale.

Idéalement, un outil de couverture de code doit aussi être utilisé dans le processus de conception pour évaluer la qualité des tests du code et déterminer les parties du logiciel qui ont été exécutées ou non. L'outil de couverture de code doit également être inclus dans les rapports de classification et de qualification. Cet outil doit être capable de tester l'application en une seule fois, sans décomposer le code en blocs et sans nécessiter de modification importante du matériel, ni de mettre en

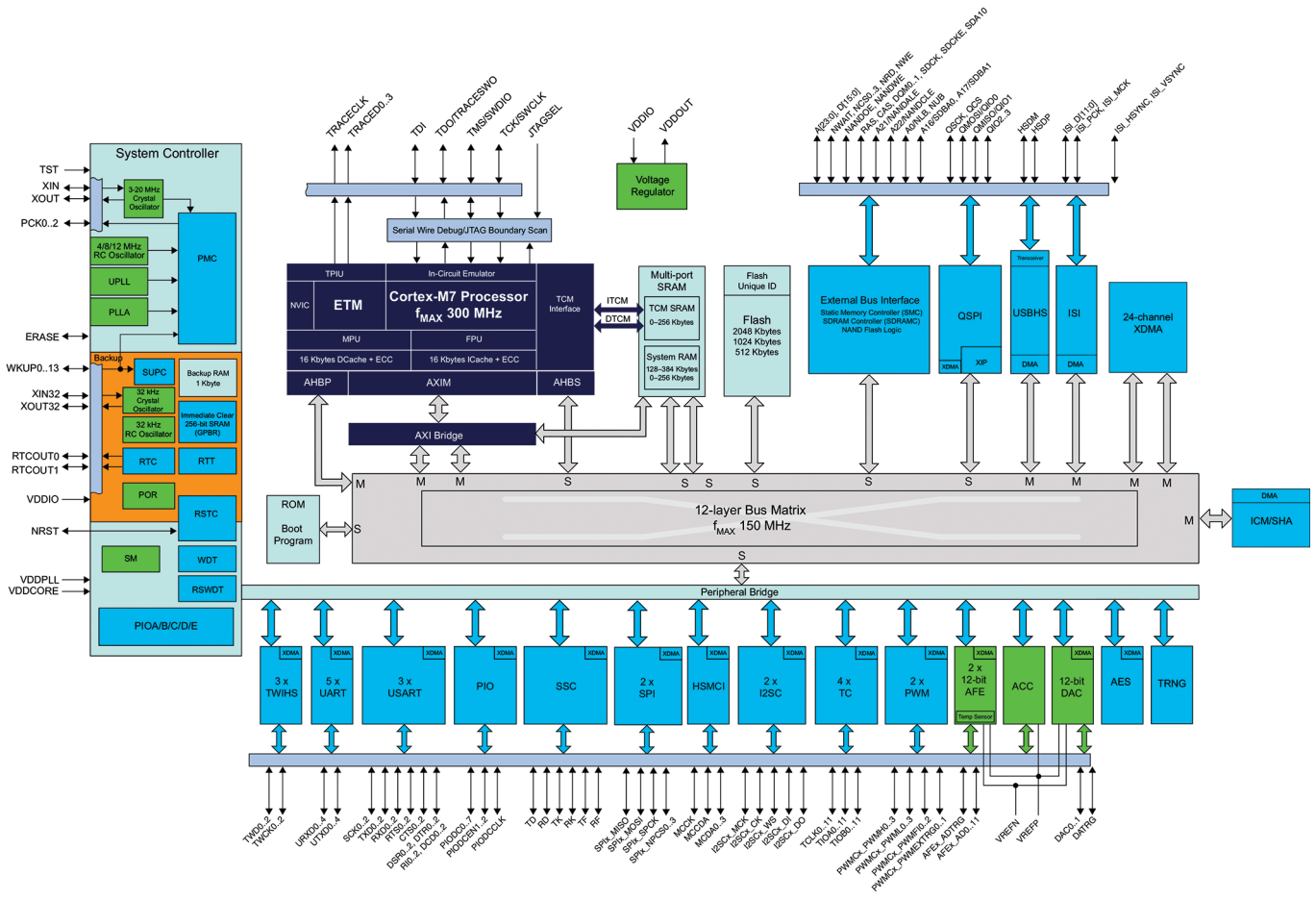
3 EXEMPLE DE CARACTÉRISTIQUES D'UN DSC COMPATIBLE AVEC LA SÛRETÉ DE FONCTIONNEMENT

Les circuits DSC 16 bits compatibles avec la sûreté de fonctionnement doivent intégrer des caractéristiques de sécurité matérielle comme une mémoire à détection et correction d'erreurs, un autotest intégré à la mémoire (MBIST, Memory Built-In Self Test), une surveillance d'horloge et un oscillateur redondant.



4 EXEMPLE D'UN MICROCONTRÔLEUR 32 BITS COMPATIBLE AVEC LA SÛRETÉ DE FONCTIONNEMENT

Les systèmes 32 bits ont besoin de caractéristiques matérielles pour la sécurité fonctionnelle notamment d'une mémoire à code de correction d'erreurs et d'injection de panne, d'un autotest intégré à la mémoire, de systèmes d'horloge avec oscillateurs de secours, d'une détection de panne d'horloge, et d'entrées/sorties généralistes avec une protection contre les décharges électrostatiques.



place des logiciels additionnels coûteux, ni d'efforts importants pour rechercher des informations pertinentes dans de gros fichiers de données. Les outils de couverture de code à passage unique jouent donc un rôle important dans la rationalisation du processus et l'accélération des lancements commerciaux.

Des ressources spécifiques nécessaires…

Pour développer une application automobile conforme à la norme ISO 26262, un ingénieur aura aussi besoin de plusieurs ressources supplémentaires de la part du fournisseur de semi-conducteurs, en plus de la fiche technique du dispositif. La disponibilité de packages de sûreté de fonctionnement permet à ce niveau aux constructeurs et fournisseurs automobiles de disposer de tout ce dont ils ont besoin aux différents stades du cycle d'évaluation et de conception. Ces packages comprennent des manuels de sécurité certifiés, des rapports FMEDA et, dans certains cas, des logiciels de diagnostic tels que des bibliothèques d'autotest certifiées pour les niveaux ASIL concernés.

Parmi ces documents, le rapport FMEDA quantifie les modes de défaillance des dispositifs, la distribution du taux de panne dans le temps et les méthodes de détection correspondantes pour aider à créer un plan de couverture. Une autre ressource importante est le manuel de sûreté. Il fournit des détails sur les méthodes de détection des pannes citées dans le rapport FMEDA et offre des recommandations sur la manière dont l'appareil doit être utilisé pour un fonctionnement le plus sûr possible. Il comprend notamment une description des défaillances dépendantes et des caractéristiques matérielles permettant de détecter les défaillances systématiques qui peuvent servir à développer des bibliothèques de diagnostic. Les bibliothèques de diagnostic de sécurité fonctionnelle permettent enfin d'évaluer l'état opérationnel d'un système en condition de panne, de détecter les pannes aléatoires du système et d'atteindre les objectifs de sûreté.

En résumé, idéalement, un kit de démarrage de sécurité fonctionnelle pour une conception à base de microcontrôleur doit inclure un FMEDA certifié ASIL B Ready, un manuel de sûreté et des bibliothèques de diagnostic conformes ASIL B/C, ainsi qu'une application de référence permettant aux concepteurs de comprendre comment ces ressources peuvent être utilisées pour développer une application critique pour la sûreté, tout en suivant le processus ISO 26262. Un package complet peut également inclure des bibliothèques de diagnostic certifiées contenant le code source et les rapports d'analyse de sécurité pertinents pour les conceptions jusqu'à ASIL B ou C. Autant de ressources qui accélèrent le processus de certification et le cycle de conception d'une application conforme aux niveaux ASIL B ou C. ■

Bibliothèque d'auto-test certifiée SIL 2/3 pour la sécurité fonctionnelle

Simplifiez le développement et la certification de vos systèmes

La sécurité fonctionnelle est essentielle dans le domaine des commandes industrielles, des robots, des capteurs, des détecteurs de gaz et des détecteurs de fumée, ce qui fait de la norme de sécurité fonctionnelle CEI 61508 un pré-requis pour ces applications.

Notre vaste portefeuille de microcontrôleurs (MCU) 32 bits SAM et PIC32, et de contrôleurs de signaux numériques (DSC) dsPIC33C dispose de bibliothèques de diagnostic (bibliothèques d'auto-test) certifiées par TÜV Rheinland pour les conceptions visant jusqu'à SIL 3, des manuels de sécurité et/ou d'AMDEC CEI 61508, qui sont disponibles dans un package complet.

Utilisez l'ensemble complet de documentation et les bibliothèques logicielles certifiées pour simplifier et accélérer le développement de votre système, tout en économisant les coûts et en réduisant le temps nécessaire à la certification.

Avantages des bibliothèques de diagnostic IEC 61508 de Microchip :

- Les bibliothèques de diagnostic certifiées par TÜV Rheinland peuvent servir à mettre en œuvre un niveau de sécurité fonctionnelle SIL 2 dans des applications à un seul canal, ou un niveau de sécurité fonctionnelle SIL 3 dans des applications à deux canaux
- Détecte les défaillances matérielles aléatoires dans le cœur, la mémoire Flash, la SRAM et les autres périphériques
- Les bibliothèques de diagnostic SIL 2/3 font partie d'un ensemble global de sécurité fonctionnelle, comprenant un manuel de sécurité fonctionnelle de logiciel, ainsi qu'une checklist applicable aux conceptions à sécurité fonctionnelle CEI 61508
- Code source complet pour les MCU PIC® et AVR® et les DSC dsPIC33C, et fichiers binaires pour MCU 32 bits PIC32C et SAM

MICROCHIP

microchip.com/IEC61508