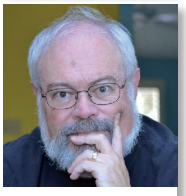
Huit raisons d'utiliser des FPGA dans les applications à sureté de fonctionnement

Réaliser un produit à sûreté de fonctionnement efficace demande beaucoup de rigueur. L'utilisation de FPGA permet une plus grande souplesse de conception et une meilleure optimisation système que ce qu'il est possible d'envisager avec des composants standard. Accompagnés d'un flot de conception certifié apte à maintenir le niveau de rigueur exigé, les FPGA peuvent aussi faciliter l'obtention du précieux sésame qu'est la certification vis-à-vis des normes de sûreté de fonctionnement.

Les technologies FPGA, Asic et CPLD jouent un rôle croissant dans le développement de produits à sûreté de fonctionnement. Les normes internationales de sureté de fonctionnement telles que la norme CEI 61508 intègrent des consignes destinées aux fournisseurs de FPGA quant aux exigences du standard, décrivent aux organismes et sociétés d'évaluation comment certifier les conceptions basées sur FPGA, et guident les utilisateurs avec des conseils sur la manière d'utiliser des FPGA dans leurs applications à sûreté de fonctionnement. Voici donc huit raisons d'utiliser des FPGA en lieu et place de microcontrôleurs ou de DSP dans un projet à sureté de fonctionnement conforme à la norme CEI 61508.

AUTEUR



Ron Wilson, ingénieur technique, Intel Programmable Solutions Group.

- **Flexibilité**

Les clients disposant d'un système déjà en production sont souvent amenés à effectuer une mise à jour pour atteindre un niveau précis de sûreté de fonctionnement (Safety Integrity Level, SIL). Pour cela, il existe deux manières de procéder: en ajoutant une carte spécifique à une conception existante, ou en recommençant une nouvelle conception. L'ajout d'une carte d'extension signifie une augmentation des coûts et peut générer des problèmes d'interfaçage.

L'autre approche consiste à repartir sur une conception complète tout en respectant une certaine rétrocompatibilité. L'industrie fait souvent appel à des canaux fonctionnels redondants pour répondre aux exigences de sûreté, une technique qui marche mais qui n'est pas assez efficace car elle peut être source d'erreurs dues aux éléments communs aux deux canaux, comme les alimentations et les horloges.

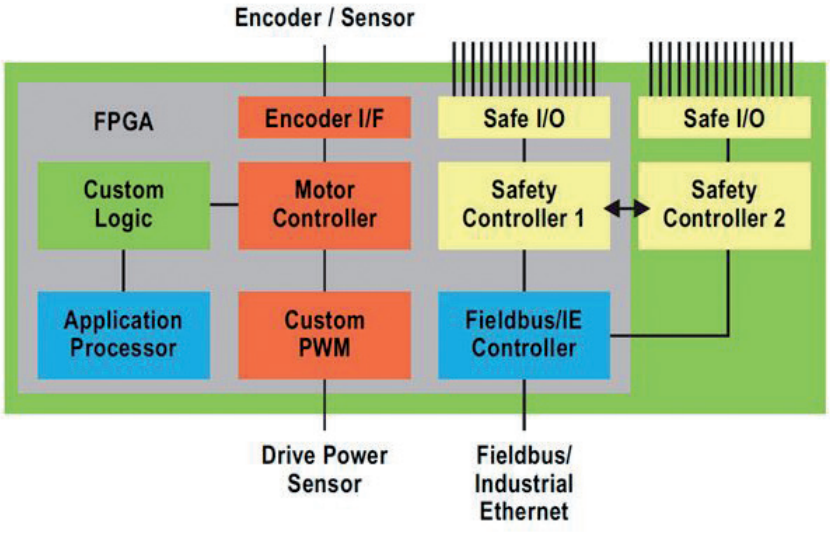
Les FPGA offrent davantage d'options en termes d'architecture et d'implémentation. Les conceptions simples peuvent s'appuyer sur deux canaux fonctionnels et une logique d'arbitrage. Des architectures plus intelligentes peuvent utiliser une circuiterie résistante aux fautes, ce qui réduit la probabilité de défaillances dues à des caractéristiques communes. La conception peut également s'interfacer très facilement avec des produits existants non sécurisés, en utilisant autant d'E/S et de fonctions autres qu'il est nécessaire pour fournir une solution complète. L'utilisation de FPGA signifie également que les concepteurs ne sont pas limités aux fonctionnalités définies par un composant standard.

- **Intégration**

La figure 1 montre une application typique de contrôleur industriel. Il intègre des fonctions standard (non sécurisées) et des fonctions de sécurité avec peu de composants sur la carte autres qu'un FPGA, tel que le FPGA Altera Cyclone IV, et un cœur de processeur logiciel comme le processeur softcore Nios II. Cette approche amène une réduction du coût global de possession (TCO) ainsi qu'une diminution conséquente des dimensions de la carte et

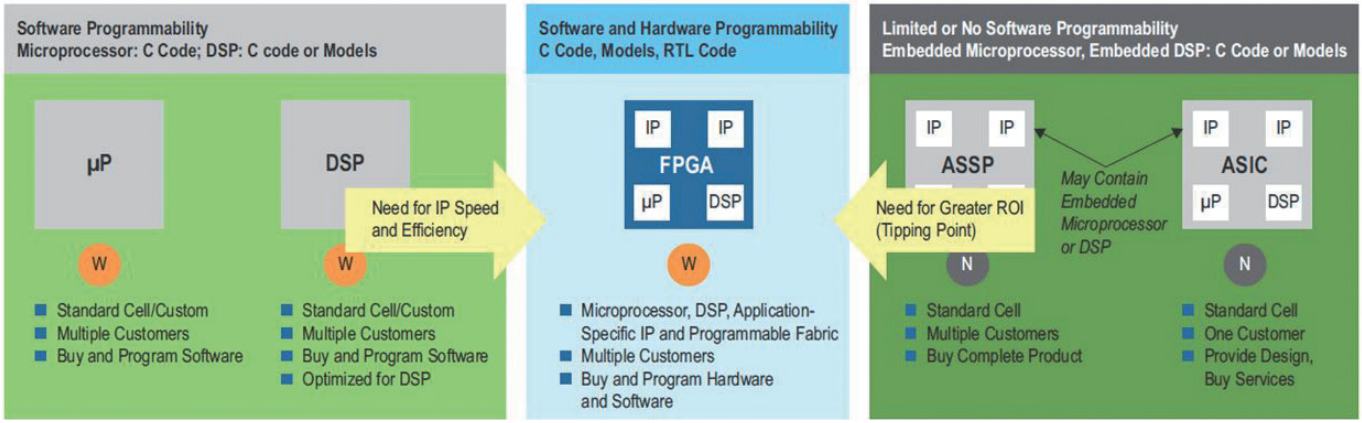
1 SYSTÈME INDUSTRIEL TYPIQUE «SÉCURISÉ» SELON LE NIVEAU DE SÛRETÉ DE FONCTIONNEMENT SIL3

L'utilisation d'un FPGA amène ici une réduction du coût global de possession (TCO) ainsi qu'une diminution conséquente des dimensions de la carte et de la consommation d'énergie, tout en répondant aux exigences de sûreté de fonctionnement.



2 MIGRATION DES APPLICATIONS À SÛRETÉ DE FONCTIONNEMENT VERS LES ARCHITECTURES À BASE DE FPGA

Les composants standard que sont les microcontrôleurs et les DSP, souvent sur- ou sous-spécifiés, ne correspondent pas forcément aux besoins exacts d'un concepteur. Avec les FPGA, les concepteurs utilisent seulement les blocs qui sont essentiels pour obtenir la certification de leur système.



de la consommation d'énergie, tout en répondant aux exigences de sûreté de fonctionnement.

• L'effet de gamme

L'approche standard pour la production de microcontrôleurs ou de processeurs de signaux numériques conformes à la norme CEI 61508 est de développer une gamme de produits ayant la qualification nécessaire, d'obtenir la certification pour « un élément à sûreté de fonctionnement hors contexte » et de fournir la documentation afférente. Cependant, ces composants standard, souvent sur- ou sous-spécifiés, ne correspondent pas forcément aux besoins exacts du concepteur (figure 2). Avec les FPGA, les concepteurs utilisent seulement les blocs qui sont essentiels pour obtenir la certification de leur système. Il en résulte une conception plus efficace qui permet en parallèle de faire appel à des composants traditionnels standard plutôt que certifiés pour la sûreté de fonctionnement, ce qui réduit le risque d'obsolescence.

• Performance

La vitesse est une caractéristique majeure dans une conception à sûreté de fonctionnement car il faut s'assurer que les décisions peuvent être prises assez rapidement pour éviter des dommages. C'est le cas avec les algorithmes de contrôle particulièrement intensifs en calculs qui sont au cœur d'un système de contrôle intelligent gérant des problèmes de sécurité bien plus complexes que les simples fonctions basiques « Arrêt d'urgence » ou « Absence sûre du couple ».

Les problèmes de sûreté doivent également être gérés lorsque le système fonctionne normalement. Par exemple, un système qui peut exécuter des diagnostics tout en étant en mode opérationnel nécessite des performances supérieures à celles d'un système qui ne dispose pas de ces capacités de diagnostic. Ces performances supplémentaires peuvent être assurées à l'aide d'un FPGA. Ainsi, une combinaison de cœurs de processeur, matériels ou logiciels, et de logique dédiée peut répondre aux exigences de timing ou de latence et permettre des diagnostics, préalables ou en cours d'exécution, sans affecter le fonctionnement du système.

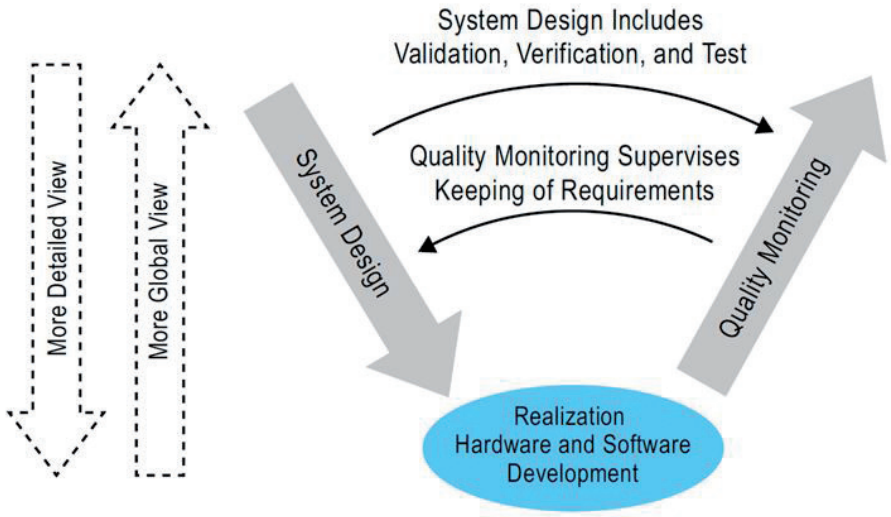
• Outils et méthodologie

La conception d'un produit sûr exige la prise en compte de la sûreté de fonctionnement dans tous les aspects du développement des produits, comme la prise en compte de normes de gestion de la qualité, l'élaboration d'une méthodologie de conception « sûre » et l'application de concepts de sûreté de fonctionnement.

Le modèle en V (figure 3) est couramment utilisé pour répartir les phases de spécification du produit selon les étapes de test, de vérification, de validation et d'intégration, tout en améliorant les processus de rétroaction et de supervision. Ce modèle en V comporte donc un ensemble d'étapes à franchir tout au long du cycle de vie d'un projet et commence par la déclinaison détaillée des exigences et la définition claire de toutes les spécifications néces-

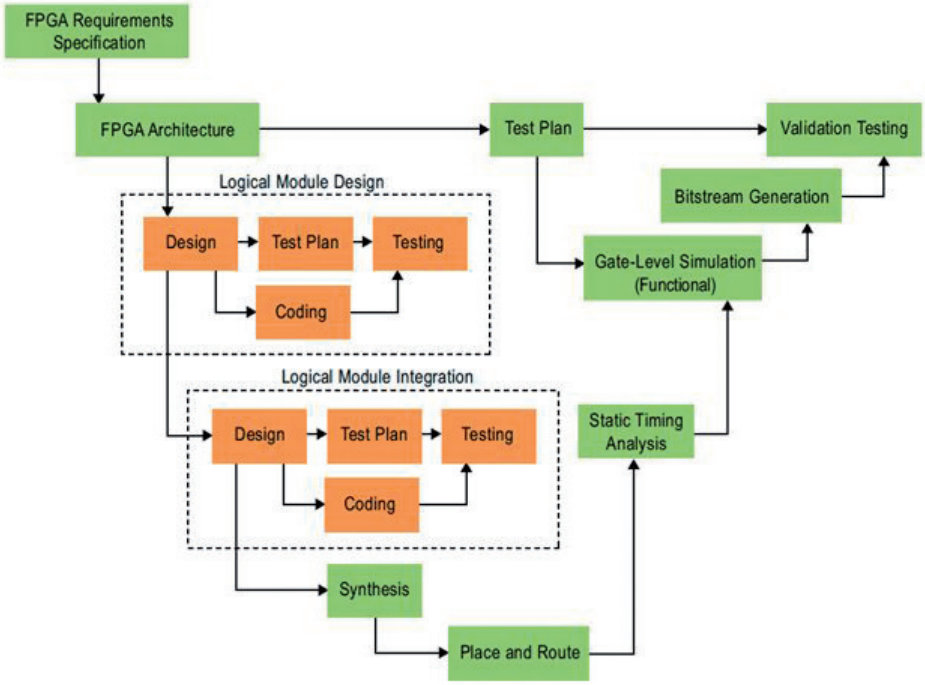
3 MODÈLE DE CONCEPTION EN V SIMPLIFIÉ

Pour appliquer le modèle en V aux conceptions à sûreté de fonctionnement, le processus doit suivre les exigences de cycle de vie CEI 61508:2010 et chaque étape du modèle en V doit être accompagnée de documents définissant une condition préalable (en entrée) et un résultat (en sortie) établissant la réussite de cette étape.



4 FLUX D'OUTILS DE CONCEPTION EN V

Ce modèle en V pour FPGA est approuvé selon la norme CEI 61508:2010 et comprend une description détaillée de la documentation d'entrée et de sortie de chaque étape, les méthodes de vérification à appliquer et les outils à utiliser.



saires au système. Chacune de ces étapes est associée à une étape de vérification.

Pour appliquer le modèle en V aux conceptions à sûreté de fonctionnement, le processus doit suivre les exigences de cycle de vie CEI 61508:2010 et chaque étape du modèle en V doit être accompagnée de documents définissant une condition préalable (en entrée) et un résultat (en sortie) établissant la réussite de cette étape. Le FSDP (Functional Safety Data Package) d'Altera certifié par l'organisme TÜV comprend un document détaillé qui aide les utilisateurs à définir une structure de processus pour appliquer le modèle en V au développement sur FPGA.

Ce modèle en V pour FPGA est approuvé selon la norme CEI 61508:2010 et comprend une description détaillée de la documentation d'entrée et de sortie de chaque étape, les méthodes de vérification à appliquer et les outils à utiliser. Cette approche permet également d'économiser du temps dans l'établissement d'un processus de développement sur FPGA axé sur la sûreté de fonctionnement (figure 4).

Le V-Flow (flux en V) et la documentation associée couvrent toutes les étapes de la conception d'une application à sûreté de fonctionnement sur FPGA, selon la spécification CEI et ses exigences. Il explique quels outils doivent être utilisés pour chaque étape, tandis que les divers chapitres de la spécification CEI guident les utilisateurs à travers les étapes nécessaires pour développer une application sûre.

La suite d'outils de conception Altera Quartus II a ainsi été vérifiée et qualifiée par TÜV Rheinland pour la conception de systèmes à sûreté de fonctionnement.

Altera fournit également des informations détaillées sur la façon de répondre aux exigences de la norme CEI 61508:2010 avec une liste de techniques et de mesures qui évitent l'introduction d'erreurs pendant la conception et le développement. Ces techniques et mesures sont liées aux outils qui les mettent en œuvre, avec le soutien de listes de contrôle qui rappellent aux équipes de développement chacune des étapes qu'ils doivent entreprendre et chaque document qu'ils doivent produire.

- **Données certifiées**

Dans une conception à sûreté de fonctionnement, la rigueur est de mise pour développer ou générer la bonne documentation à chaque étape du processus. Sur ce point, Altera contribue largement en fournissant une analyse statistique approfondie de la fiabilité de ses FPGA, permettant aux utilisateurs de calculer les taux de défaillance dans le temps. Le Safety Data Package contient également un guide d'intégration sur silicium, des données ad hoc sur les caractéristiques intrinsèques du FPGA qui sont primordiales dans les calculs typiques de sûreté de fonctionnement et des informations sur les éléments de conformité spécifiques à la norme CEI 61508.

- **IP de diagnostic**

Les stratégies de conception pour la sûreté de fonctionnement peuvent exiger l'insertion de systèmes de surveillance des signaux de base tels que l'horloge et l'alimentation, et de moniteurs de données complexes pour assurer un fonctionnement correct du système. Il peut également être nécessaire d'inclure des moyens d'identifier automatiquement les défaillances et d'amener le système dans un état sûr.

L'un des avantages de l'utilisation de FPGA réside ici dans le fait que des fonctions de diagnostic peuvent être implémentées au niveau hardware, ce qui évite l'écriture de logiciels supplémentaires et impacte moins les performances du système que les fonctions de diagnostic purement logicielles. Parmi les fonctions typiques pouvant être implémentées dans le silicium, citons les mécanismes de surveillance de la fréquence d'un signal d'horloge par rapport à une référence, une IP de diagnostic qui détecte des perturbations dues à des événements uniques (SEU) et même des processeurs consacrés exclusivement au diagnostic système.

- **Efficacité prouvée et risque réduit d'obsolescence**

L'élaboration de systèmes à sûreté de fonctionnement utilisant des FPGA offre deux avantages supplémentaires. Le premier est qu'il est possible de bâtir les membres à sûreté de fonctionnement d'une famille de produits sur une conception existante qui a déjà fait ses preuves sur le terrain, ce qui augmente d'autant la confiance que l'on peut placer en eux. Le deuxième avantage est que les FPGA standard sont susceptibles d'être proposés avec une durée de disponibilité bien plus longue que celle de composants spécifiques à sûreté fonctionnelle qui n'ont été vendus qu'en faible volume à un nombre limité de clients. ■