Avantages des « éléments de sécurité hors contexte » (SEooC) pour les logiciels sur étagère dans l'automobile

Le développement d'éléments logiciels hors contexte SEooC (Software Elements out of Context) est bien défini par la norme ISO 26262:2018 et constitue une nette avancée par rapport à des spécifications moins strictes que l'on trouve dans d'autres normes de sûreté de fonctionnement. En suivant les méthodes et techniques recommandées par l'éditeur HCC Embedded, il est possible de créer un modèle pour le développement et la maintenance des SEooC pour l'automobile.

Dans l'industrie automobile, la norme ISO 26262 a instauré une définition claire de la manière d'utiliser des composants « prouvés » appelés éléments de sécurité hors contexte (Safety Elements out of Context, SEooC). Si les SEooC sont plus communément considérés comme des composants matériels tels que des microcontrôleurs ou des sous-systèmes, le modèle fournit également une approche idéale pour développer des éléments logiciels de haute qualité hors contexte. Ces éléments logiciels sont conçus pour fournir une fonctionnalité spécifique et répondre à un niveau de sécurité adéquat, même lorsque l'on ne connaît pas la manière dont le logiciel sera utilisé (ou même quelles parties de celui-ci seront utilisées) dans le système cible final.

Exemple d'un SEooC TCP/IP

Examinons les problèmes liés à l'intégration d'une pile TCP/IP à un dispositif au sein d'un véhicule. TCP/IP est un protocole de communication extrêmement utilisé et éprouvé. Il existe sur le marché d'innombrables piles offrant une vaste gamme de fonctionnalités et de variantes. Il ne serait pas très raisonnable de réécrire ce protocole pour chaque dispositif, ce qui en fait donc un candidat idéal pour la réalisation d'un SEooC. Cependant il y a certains défis à relever.

AUTEUR

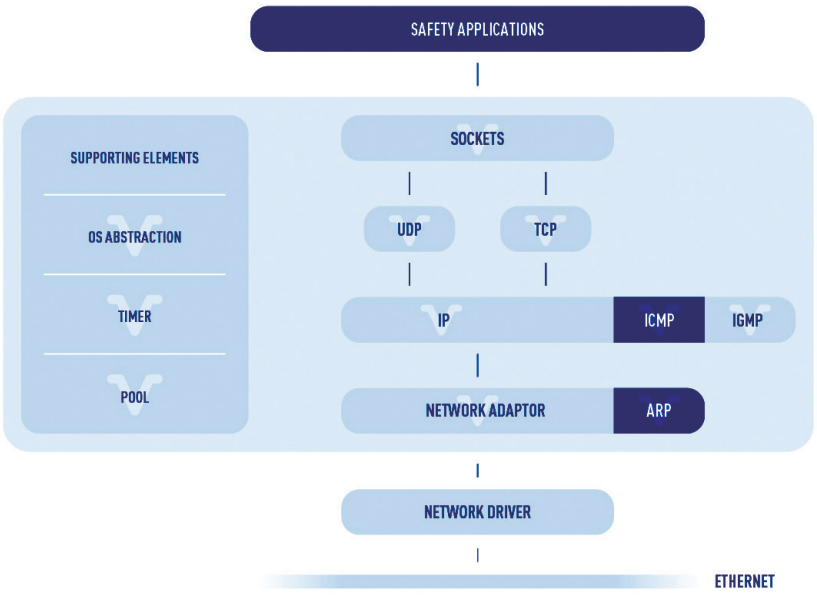
Dave Hughes, CEO et fondateur, HCC Embedded.

Une simple pile TCP/IP conçue pour la sécurité peut inclure des protocoles IP, ARP, ICMP, TCP, UDP, DHCP, ICMP, Sockets et certains modules d'interface réseau permettant d'ajouter un pilote réseau spécifique à la cible (figure 1). Elle peut être développée conformément à la norme ISO 26262-6:2018 avec un processus de développement logiciel suivant un modèle en V, exactement comme vous l'exigeriez pour n'importe quel développement critique pour la sécurité. Ce processus devra néanmoins s'accompagner de certains artefacts importants comme :

- Les hypothèses qui ont été faites au moment de la conception du SEooC. D'un point de vue global, il peut s'agir du type et du boutisme (c'est-à-dire de l'ordre dans lequel les octets sont placés, endianness en anglais) du microcontrôleur cible, ainsi que de la présence ou non d'un système d'exploitation temps réel RTOS, d'un temporisateur, etc.
- Les exigences qui définissent en détail les spécifications de haut

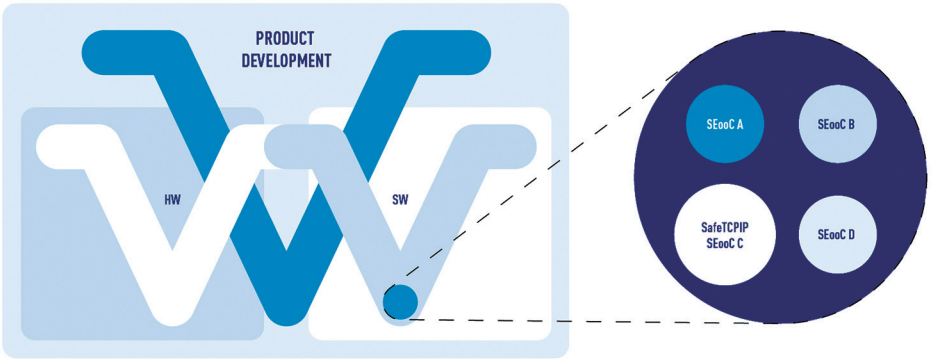
1 ARCHITECTURE D'UNE PILE TCP/IP PRÉSENTÉE EN TANT QUE SEOOC

Une simple pile TCP/IP conçue pour la sécurité peut inclure des protocoles IP, ARP, ICMP, TCP, UDP, DHCP, ICMP, Sockets et certains modules d'interface réseau permettant d'ajouter un pilote réseau spécifique à la cible.



2 ADAPTATION ET INTÉGRATION D'UN SEOOC TCP/IP SELON UN MODÈLE EN V

Un SEooC doit être conçu pour pouvoir être réutilisé au sein d'un dispositif spécifique. Le processus de personnalisation d'un SEooC est décrit dans la section 9.2.4 de la norme ISO 26262-10:2018.



niveau ainsi que les spécifications fonctionnelles du SEooC. Elles commenceront par les items de plus haut niveau, y compris les protocoles et les fonctionnalités qui seront fournies, et s'affineront au fur et à mesure de manière à spécifier le système complet.

- Une suite de tests de validation qui vérifie de manière exhaustive que l'élément logiciel se comporte de la même manière après l'intégration que dans le processus de développement du SEooC.

Tout cela doit être couvert par une traçabilité complète entre les exigences et les scénarios de test, et entre les exigences et les résultats de conception et d'implémentation.

Pour utiliser ce SEooC, l'intégrateur doit s'assurer de compléter plusieurs étapes :

- Valider que les hypothèses formulées lors du développement du SEooC correspondent à celles fournies par le système cible.
- Valider la conformité des exigences (spécifications) du SEooC face à celles requises par le dispositif.
- Vérifier que l'élément fonctionne correctement sur la cible.
- Effectuer des tests d'intégration spécifiques du SEooC dans le contexte du système cible.

Tout ceci peut, jusqu'ici, paraître assez simple – mais il reste cependant des problèmes pratiques à résoudre.

Premièrement, pour un dispositif particulier, il se peut que certaines parties de la pile ne soient pas nécessaires. Par exemple, dans un cas simple, un dispositif peut n'utiliser que TCP pour la communication, rendant donc le composant UDP redondant. Les composants inutiles doivent être retirés pour éliminer les tests d'intégration associés.

Dans un autre cas de figure, il se pourrait que le dispositif ait toujours une adresse réseau préconfigurée en raison de son rôle fixe au sein du véhicule, la reconfiguration dynamique n'ayant pas lieu d'être dans les véhicules routiers ; dans le pire des cas, elle ne se produirait que durant la maintenance. Dans ce cas, DHCP n'est donc plus requis.

En dehors de la fonctionnalité, il peut être nécessaire de modifier la configuration ; par exemple, le nombre de ports réseau ou de sockets disponibles devra naturellement être modifié pour s'adapter à la cible.

Tous ces problèmes signifient que le SEooC doit être conçu pour pouvoir être réutilisé au sein d'un dispositif spécifique. Le processus de personnalisation d'un SEooC est décrit dans la section 9.2.4 de la norme ISO 26262-10:2018 (figure 2).

C'est pourquoi HCC a conçu le SEooC SafeTCPIP comme un ensemble de SEooC – chaque module (IP, TCP, UDP, etc.) possédant son propre modèle en V complet, conformément à la norme ISO 26262-6:2018 – de sorte que ces modules puissent être assemblés en fonction des exigences (figure 3).

Une fois qu'un set de modules est défini, le problème suivant consiste en la personnalisation de ces modules. Il en résultera une nouvelle série de tests entièrement adaptés aux nouvelles exigences et hypothèses.

Options pour le développement de SEooC

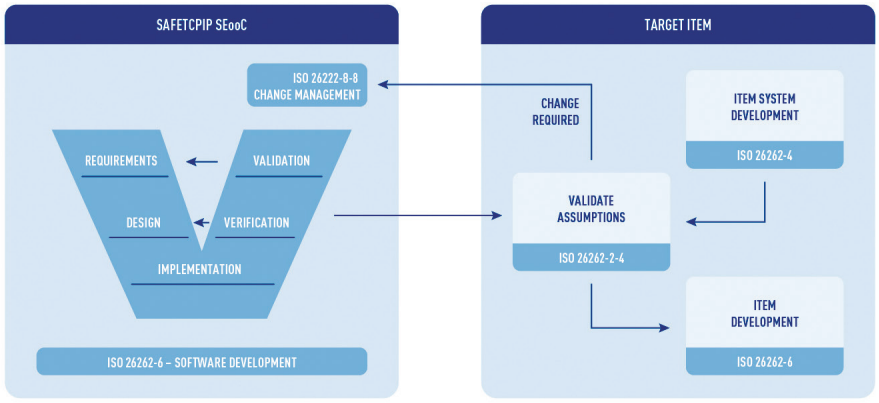
La section 9 de la norme ISO 26262-10:2018 décrit comment concevoir des SEooC logiciels. Ce document spécifie quatre options pour créer des SEooC :

- Prouvé par l'usage.
- Qualification d'un composant logiciel.
- Élément logiciel ISO 26262-6 dans le contexte d'un certain dispositif.
- Élément logiciel ISO 26262-6 hors contexte.

Parmi ces différent cas, seul le dernier – développer l'élément logiciel hors contexte spécifiquement pour sa réutilisation – répond à toutes les exigences décrites plus haut, à savoir la nécessité de développer un élément proprement, de le réutiliser et de le modifier. Le nœud du problème

3 PRINCIPE DE L'ASSEMBLAGE D'UN SEOOC TCP/IP SELON HCC

HCC a conçu le SEooC SafeTCPIP comme un ensemble de SEooC – chaque module (IP, TCP, UDP, etc.) possédant son propre modèle en V complet, conformément à la norme ISO 26262-6:2018 – de sorte que ces modules puissent être assemblés en fonction des exigences.



COMPARAISON DES DEUX APPROCHES POUR LA MAINTENANCE DES SEOOC

Maintenance effectuée par le fournisseur du SEooC	Avantages	L'expertise des concepteurs du SEooC peut être utilisée pour apporter des modifications L'expérience acquise dans d'autres instances du SEooC peut être utilisée pour en maintenir la qualité. Vérification externe que les concepts proposés lors de la personnalisation sont adéquats dans le contexte du SEooC
	Inconvénients	Les modifications doivent correspondre au même niveau ASIL
Maintenance effectuée par le fabricant du dispositif	Avantages	Permet le contrôle du processus de modification qui ne dépend pas d'une partie externe Des modifications peuvent être apportées à un niveau ASIL inférieur à celui du SEooC fourni.
	Inconvénients	L'intégration des outils de travail du fournisseur du SEooC au système de développement pour la sûreté du fabricant peut poser des problèmes. Le fabricant doit devenir un expert des moindres détails du SEooC.

Deux approches sont possibles pour résoudre le problème de l'intégration d'un nouvel élément SEooC au système de développement pour la sécurité fonctionnelle du dispositif cible. On peut intégrer tous les artefacts développés pour le SEooC au système de développement pour la sûreté de la cible, ou dissocier les responsabilités et utiliser les processus de personnalisation et de test d'intégration comme mécanismes de contrôle de l'intégration.

est qu'à moins qu'un élément ne soit développé avec une traçabilité totale et avec tous ses artefacts, il n'est pas possible de faire une analyse d'impact complète permettant d'effectuer un ensemble de modifications de l'élément et de garantir le même niveau de validation.

Comment choisir un niveau ASIL

Une étape fondamentale du développement d'un quelconque élément selon la norme ISO 26262 consiste à déterminer les risques potentiels que cet élément pourrait créer et à lui attribuer un niveau d'intégrité pour la sécurité automobile (Automotive Safety Integrity Level, ASIL). Ces niveaux vont de la valeur ASIL/A, correspondant à un faible risque, à ASIL/D pour un risque élevé mettant la vie en danger. Bien sûr, si vous développez un élément hors contexte, vous n'avez aucun moyen de savoir quel niveau ASIL peut être requis.

Une solution simple serait de développer les SEooC au plus haut des niveaux ASIL, soit ASIL/D, afin qu'ils puissent être utilisés n'importe où, mais cela présenterait quand même certains inconvénients. Le principal problème est le coût. L'utilisation d'un composant ASIL/D dans un dispositif développé en ASIL/A peut s'avérer onéreux en termes de développement, ainsi que de personnalisation et de maintenance.

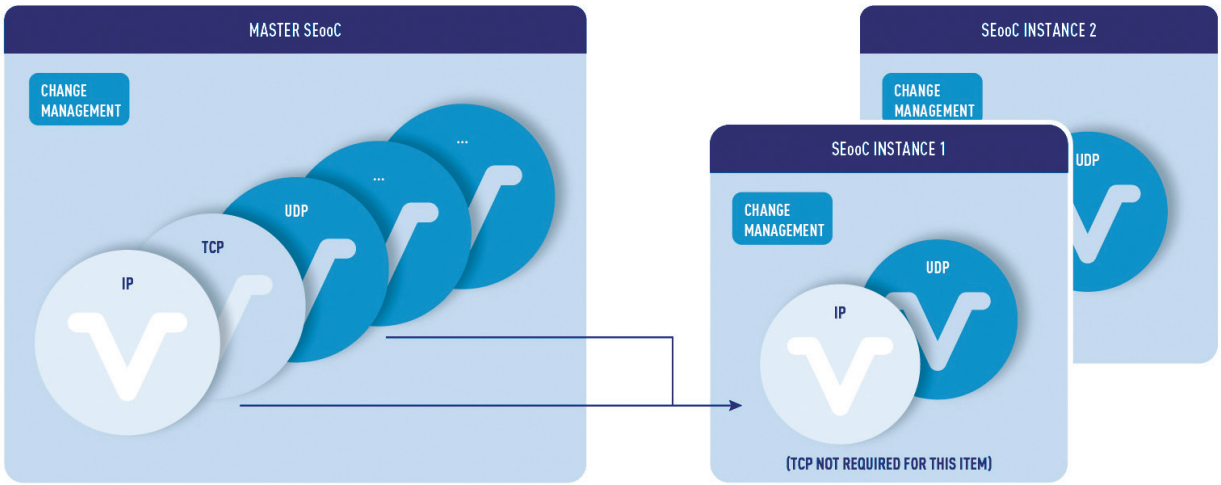
Une fois que vous avez créé une instance cible d'un SEooC, vous aurez probablement la possibilité de personnaliser les processus de maintenance spécifiques pour cette instance, mais c'est une tâche non triviale que d'analyser tous les processus et d'avoir éventuellement à les dégrader en niveau. Des étapes spécifiques peuvent facilement être supprimées, mais il s'avère difficile de dégrader la traçabilité (qui est souvent la tâche la plus lourde dans un développement pour la sécurité).

Comment s'intégrer au système de développement de la sûreté

Une autre considération importante est de savoir comment intégrer ce nouvel élément au système de développement pour la sécurité fonctionnelle du dispositif cible – un dispositif probablement développé par une société différente du fournisseur du SEooC avec son propre système de développement pour la sûreté éprouvé et structuré. En principe, il y aura des similitudes évidentes entre les deux systèmes de développement, mais même de petits détails, tels que l'outil utilisé pour la saisie

4 PRINCIPE DE LA CRÉATION D'UNE INSTANCE DE SEOOC

HCC a adopté une approche dans laquelle, pour chaque dispositif en cours de développement, une instance indépendante du Master-SEooC est créée pour cet item.



des exigences, pourraient ne pas être identiques.
Deux approches sont possibles pour résoudre ce problème :
- Intégrer tous les artefacts développés pour le SEooC au système de développement pour la sûreté de la cible, ou
- Dissocier les responsabilités et utiliser les processus de personnalisation et de test d'intégration comme mécanismes de contrôle de l'intégration.
Les deux approches ont leurs avantages et leurs inconvénients (tableau). HCC, pour sa part, adopte une approche dans laquelle, pour chaque dispositif en cours de développement, une instance indépendante du Master-SEooC est créée pour cet item : SEooC-item-instance-x (figure 4). Une instance inclut tout ce qui la concerne depuis le développement du SEooC, y compris tous les documents de processus, de sorte que, à tout moment, l'instance SEooC-item-instance puisse être modifiée indépendamment de toute autre instance. L'utilisation d'un SEooC de cette façon évite de créer une interdépendance entre les dispositifs.
En adoptant cette approche, nous pouvons utiliser notre expertise des fonctionnalités de base du SEooC pour en maintenir des instances indépendantes, de manière à ce que toute personnalisation ou gestion des défauts ne s'applique qu'à cette instance du SEooC.
Cela crée certes une charge supplémentaire, car chaque fois qu'une modification doit être apportée, elle doit être implémentée indépendamment pour chaque instance. L'avantage est cependant que chaque modification peut être approuvée par le fabricant du dispositif.

En résumé

Le développement d'éléments logiciels hors contexte est bien défini par la norme ISO 26262:2018 et constitue une nette avancée par rapport aux normes moins strictes COTS ou SOUP que l'on trouve dans d'autres normes de sécurité fonctionnelle. En suivant les méthodes et techniques recommandées ici, il est possible de créer un modèle pour le développement et la maintenance des SEooC, et de gérer des intégrations individuelles pour des dispositifs cibles.
L'unique voie à suivre consiste à développer le SEooC selon les méthodes établies par la norme ISO 26262-6:2018 et à utiliser le processus défini à la section 9 de la norme ISO 26262-10:2018 pour effectuer des intégrations aux dispositifs cibles.
Une condition importante d'une utilisation réussie de SEooC réside dans une compréhension mutuelle totale entre le fournisseur de SEooC et le fabricant du dispositif cible. Les processus de développement et de maintenance doivent être précisés dans le cadre de la phase initiale de l'élaboration du projet. En utilisant cette approche, HCC Embedded a développé la pile SafeTCPIP qui permet l'intégration en toute sécurité d'une gamme de cœurs TCP/IP au sein des systèmes automobiles. ■