Always reliable. Always ahead.

Accélérer le développement de solutions ferroviaires intelligentes et sécurisées avec des composants COTS de niveau SIL

Les chemins de fer intelligents nécessitent des systèmes de contrôle et de gestion intelligents qui doivent souvent répondre aux exigences de sécurité les plus élevées jusqu'au niveau SIL 4. Avec des plates-formes modulaires COTS (Commercial Off-The-Shelf ; Composants sur-étagère) pré-certifiées SIL, de tels systèmes peuvent être développés plus rapidement et de façon plus rentable que jamais. Le système menTCS (TCS pour Train Control System) de MEN Mikro Elektronik, est le premier kit de développement modulaire au monde à répondre aux spécifications de sécurité ferroviaire.

Table des matières

Plus d'intelligence dans les trains et sur les voies

Dans les années à venir, le passage au numérique pour l'industrie ferroviaire sera la tâche dominante attribuée aux opérateurs de trains et de voies, ainsi qu'aux équipementiers et aux fournisseurs d'automatisation qui les approvisionnent. L'objectif est de rendre le transport ferroviaire plus sûr, plus efficace et plus convivial. Le mot à la mode en est «*smart railways*» (chemins de fer intelligents): des trains et des infrastructures de plus en plus intelligents permettent une surveillance plus étroite, plus précise et donc permettre des horaires de trains plus serrés. Cela améliore l'utilisation des voies tout en augmentant la fiabilité des horaires. Dans les systèmes ferroviaires intelligents, des cycles d'entretien rigides peuvent également être changés en des services plus efficaces, à la demande. Cela permet d'économiser non seulement sur les coûts, mais augmente aussi la fiabilité, car le besoin de maintenance est détecté avant qu'une panne ne se produise. Dans le transport de passagers, la billetterie électronique contribue à améliorer la satisfaction des passagers. Avec des données plus complètes sur le nombre de passagers, l'utilisation peut être prédite avec plus de précision et la capacité planifiée en temps réel sur la base de ces données de *Big Data*. Dans le domaine du transport de marchandises, les systèmes ferroviaires intelligents peuvent, par exemple, offrir des programmes horaires basés sur le Web pour les emplacements de chaque wagon. Cela fait des trains une véritable alternative au transport routier, puisque les clients peuvent désormais planifier et suivre de plus petits lots avec plus de précision.

Une forte demande

La transformation numérique du marché des transports ferroviaires conduit à d'immenses investissements: au cours des 10 prochaines années, le marché des technologies des transports ferroviaires devrait croître de plus de 22% CAGR (Compound Annual Growth Rate) dans le monde entier. Si vous regardez l'Europe, l'un des projets spécifiques prévu est d'équiper l'ensemble des 4000 (voire plus) passages à niveau non gardés en Italie avec des systèmes sécuritaires pour minimiser les risques d'accidents. En Suède, la logique au sein des boîtiers de signalisation devrait être remplacée dans presque tous les systèmes, car ils fonctionnent encore avec des relais vulnérables qui sont coûteux à entretenir. Et en Allemagne, le transport de marchandises doit être intégré dans l'European Train Control System (ETCS). En outre, la compagnie ferroviaire allemande Deutsche Bahn prévoit de basculer encore plus de son transport régional vers des trains de voyageurs autonomes.

Les nouvelles technologies à la hausse

Les chemins de fer intelligents ont besoin de nouvelles technologies intelligentes. Les systèmes intelligents le long des voies et à bord des trains doivent intégrer de nombreuses nouvelles fonctionnalités et être capables de gérer des forts volumes de données, par exemple pour analyser en temps réel les lectures provenant de capteurs intelligents pour la vitesse des roues, l'accélération, les vibrations et la température. Le suivi de localisation précis nécessite également des informations provenant de systèmes de navigation par satellite mondiaux tels que GPS, GLONASS ou Galileo. Une opération semi ou même entièrement autonome exige un contrôle automatique des trains beaucoup plus précis, à la fois le long des voies et dans les trains eux-mêmes. En outre, des systèmes radar, à ultrasons ou basés sur la vision doivent être intégrés. Presque toute l'électronique ferroviaire de sécurité critique, à la fois en ce qui concerne les voies et les trains, sera mise à l'épreuve et souvent deviendra obsolète, car elle ne permet pas l'intégration de nouvelles fonctions ferroviaires intelligentes.

Les normes ferroviaires sont un must

Ce qui est nécessaire est une nouvelle génération de systèmes de gestion et de contrôle de sécurité critique. Tout comme les systèmes déjà installés, ils doivent être très robustes pour être en mesure de fonctionner de manière fiable pendant des années dans les conditions difficiles typiques du secteur ferroviaire. Comment concevoir de tels systèmes est spécifié, par exemple, par la norme EN 50155. Elle stipule la résistance requise aux températures extrêmes, aux changements rapides de température, aux vibrations, aux chocs ainsi qu'aux interférences électromagnétiques. Mais cela seul ne suffit pas.

Il en va de même des normes SIL

Les systèmes où une erreur ou une panne peuvent présenter un risque pour la vie humaine ou l'environnement ou causer de grandes pertes financières doivent répondre à des exigences élevées de sécurité fonctionnelle. Par conséquent, la technologie ferroviaire intelligente est généralement soumise aux nombreuses exigences de sécurité internationales de la norme EN 50128 / IEC 62279 pour les logiciels, et EN 50129 / IEC 62425 pour le matériel. Et fournir une preuve de conformité à ces exigences n'est pas une tâche facile ni rapide.

La documentation de certification – un travail porteur

Dans une nouvelle conception, mettre en place la documentation nécessaire pour démontrer la conformité avec les normes de sécurité peut doubler, voire tripler, les coûts du projet ainsi que sa durée. Les spécifications pertinentes pour la sécurité fonctionnelle sur le marché ferroviaire comprennent les critères RAMS (Reliability, Availability, Manageability, Safety) de la norme EN 50126 / EN 50128 pour les logiciels et EN 50129 pour le matériel. Ils impliquent tous une augmentation du travail de documentation, que les fournisseurs de solutions préfèrent garder à un minimum.

Du matériel pré-certifié réduit l'effort de documentation

Le levier stratégique pour une réduction significative de l'effort de documentation est l'utilisation de matériel pré-certifié, car celui-ci est en grande partie basé sur une technologie standardisée. Donc, en supposant qu'il y a un fournisseur de solution ayant une connaissance spécifique des exigences de conformité de type 501xx, il devrait être possible de déléguer cette partie de la documentation à ce fournisseur. Deux avantages vont en découler: tout d'abord, cela permettra d'économiser sur les coûts de la documentation interne. Deuxièmement, cela permettra d'économiser un temps précieux, qui, dans la compétition pour les solutions les plus innovantes est l'un des facteurs les plus importants. Celui qui est le premier sur le marché bénéficie des plus grandes opportunités, jouit d'une exclusivité sur le marché et est en mesure de définir des normes clés. Mais à quoi un tel matériel pré-certifié devrait-il ressembler?

Les recommandations de l'UIC pour la mise en œuvre matérielle

Dans son rapport «Global Vision for Railway Development Report», l'UIC fait trois recommandations claires:

- Au lieu des systèmes existants souvent fermés, de nouvelles configurations doivent être construites comme des conceptions modulaires. Il est ainsi plus facile d'adapter des systèmes pour des applications différentes et favorise la réutilisation efficace des conceptions déjà existantes. Par exemple, les systèmes modulaires peuvent être déployés dans différentes configurations aussi bien dans les systèmes de gestion des trains que dans les installations en bord de voie qui contrôlent les aiguillages ou les signaux. Les systèmes modulaires permettent également une maintenance plus rapide et plus rentable puisque les modules individuels peuvent être remplacés directement sur le

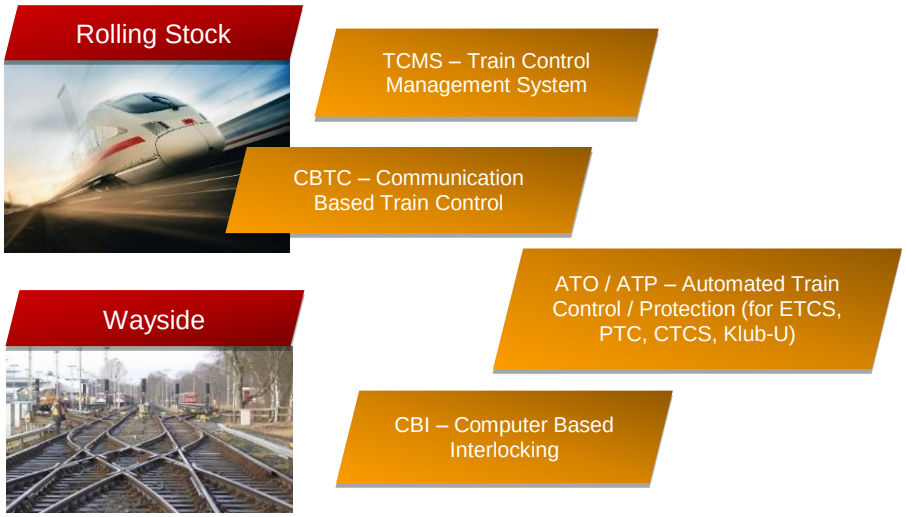
terrain. Enfin, et ce n'est pas le moins important, ils sont protégés contre l'obsolescence car des extensions sont faciles à mettre en œuvre en ajoutant des modules supplémentaires ou en les remplaçant par des modules plus puissants.

- En outre, les systèmes doivent être basés sur des standards ouverts. Ceci permet d'assurer que la conception du système a un long cycle de vie et qu'il ne deviendra pas obsolète si un fournisseur se retire du marché. Cela améliore également la rentabilité, car lorsque les composants peuvent être achetés auprès de fabricants différents, la concurrence joue pour obtenir des coûts plus compétitifs.
- Des conceptions dénommées « boîte blanche » sont également recommandées. Contrairement aux conceptions propriétaires de type « boîte noire » qui prévalent actuellement, dans lesquelles les composants matériels et logiciels sont inséparables et ne fournissent pas d'option pour faire des ajustements, les conceptions « boîte blanche » visent à fournir une structure de système transparente. Une souplesse qui assure des adaptations faciles du système pour satisfaire différentes tâches, normes d'interface et protocoles de communication, garantissant ainsi leur interopérabilité. Il s'agit là d'une condition importante pour assurer la sécurité et les communications transfrontalières dans le transport ferroviaire à moyen et à long terme.

Les plates-formes modulaires de type COTS basées sur la norme CompactPCI édictée par le PCI Industrial Manufacturing Group (PICMG), qui est maintenue depuis 1997 et est spécialement conçue pour les conceptions modulaires très robustes avec des fonds de panier passifs, répondent à ces exigences en général. Cependant, ces spécifications ne décrivent que la technologie de base et n'incluent pas à elles seules la certification et la documentation nécessaire pour les normes EN 50155 et EN 50126, EN 50128 et EN 50129. Pour que les fournisseurs de solutions retirent le maximum d'avantages de l'utilisation de telles plates-formes COTS modulaires, il est donc impératif d'étendre cette norme à la technologie ferroviaire.

La plate-forme menTCS

MEN Mikro Elektronik est la première entreprise au monde à avoir reconnu ce besoin et élargi son portefeuille complet de produits CompactPCI conformes EN 50155 avec un système qui est spécialement conçu pour les applications ferroviaires de sécurité critique, et pré-certifié pour EN 50126, EN 50128 et EN 50129. Le nouveau système menTCS (MEN Train Control System) avec des composants pré-certifiés SIL 4 raccourcit le processus de certification pour les fournisseurs de solutions. Grâce à sa conception modulaire, il peut être adapté à tous types d'applications différentes. Par exemple, dans le matériel roulant, le système menTCS est une solution idéale pour l'Automatic Train Operation (ATO), l'Automatic Train Protection (ATP), le Positive Train Control (PTC) et l'Enhanced Train Control (ETC). Dans les applications en bord de voie, il peut être utilisé pour contrôler les signaux et les aiguillages jusqu'au niveau de sécurité SIL 4.

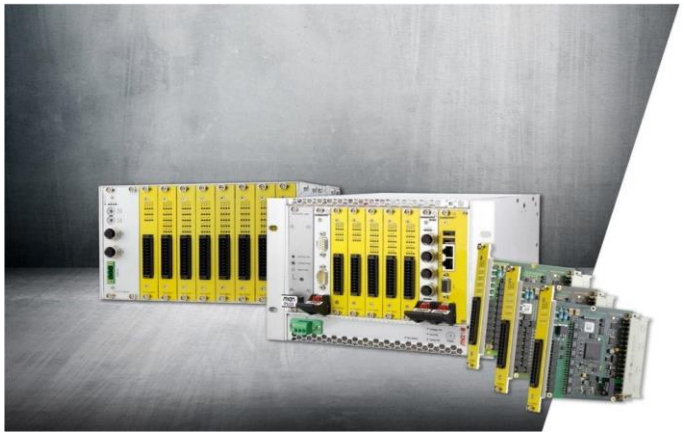


Non limité à une application spécifique: le MEN Train Control System (menTCS) avec des composants pré-certifiés SIL 4 est déployé dans une variété de matériel roulant ou en bordure de voie pour des applications de sécurité critique.

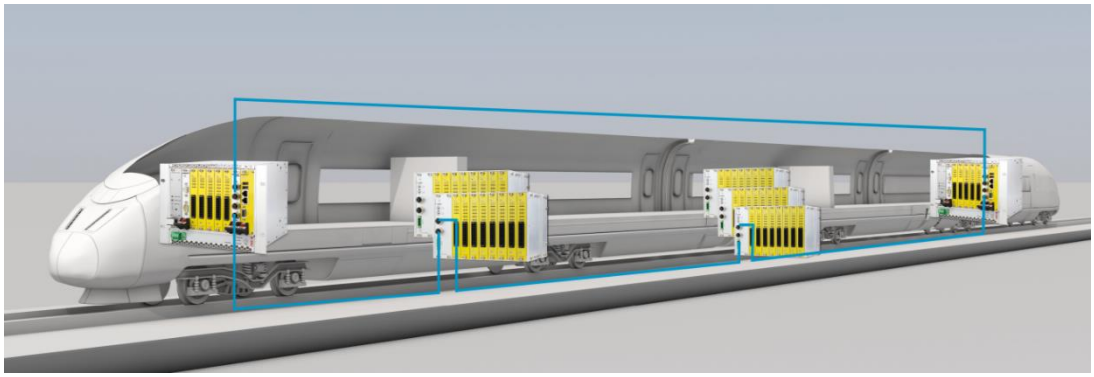
Architecture du système

Le cœur du MEN Train Control System (menTCS) est le contrôleur central MH50C. Il abrite la logique de contrôle central sous la forme d'une carte multiprocesseur CompactPCI qui est pré-certifiée pour les normes EN 50155 et EN 50126, EN 50128 et EN 50129 et peut être personnalisée avec un maximum de 6 cartes d'extension en fonction des exigences de l'application. En outre, jusqu'à 63 boîtiers d'E/S modulaires menTCS sont disponibles pour connecter au contrôleur menTCS central des E/S distantes. Une caractéristique très intéressante pour les installations dans les trains à grande vitesse où chaque voiture a besoin de son propre boîtier d'E/S pour connecter les capteurs et les actionneurs. Le concept d'extension modulaire fait également ses preuves dans les installations en bordure de voie telles que les systèmes de signalisation, où des boîtiers d'E/S modulaires menTCS peuvent être utilisés pour contrôler certains tronçons de voie en fonction des besoins. Dans ce cas, les boîtiers d'E/S menTCS sont connectés via une topologie en anneau à base d'Ethernet. Cela permet non seulement de simplifier le câblage, mais aussi augmente considérablement la fiabilité, car deux canaux de communication redondants peuvent être utilisés.

Les composantes de ce concept de famille modulaire, certifiables individuellement, peuvent également simplifier le développement de systèmes 19 pouces entièrement personnalisables si cela est nécessaire.



Standard ouvert: Le MEN Train Control System pré-certifié SIL 4 est basé sur le standard ouvert et modulaire CompactPCI pour des systèmes en rack avec fonds de panier passifs



Flexible: Le contrôleur MH50C du menTCS permet une expansion flexible avec jusqu'à 63 boîtiers d'E/S modulaires menTCS distants qui sont connectés via une topologie en anneau temps réel redondante.

Des extensions et interfaces flexibles

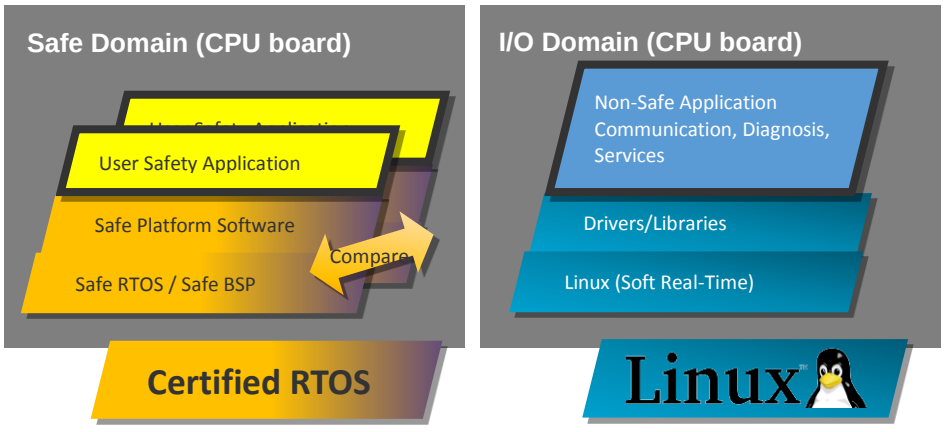
Le concept d'E/S modulaire de l'architecture standardisée de menTCS procure aux développeurs une grande flexibilité et il est très facile pour eux d'équiper le contrôleur et les boîtiers E/S déportés avec des interfaces de communication via des cartes CompactPCI. Pour la connexion avec un réseau TCN, des cartes d'interface MVB peuvent être utilisées. Des éléments embarqués ou unités de contrôle supplémentaires peuvent être connectés via RS485, CAN, ProfiNet et autres bus de terrain, communiquer via WLAN, GSM-R, GPS, GLONASS ou Galileo pour la connectivité IoT, ou encore être utilisés comme des routeurs et des switches standards via Ethernet.

Une sécurité évolutive

Comme tous les modules menTCS de sécurité critique sont pré-certifiés au niveau le plus élevé SIL 4 selon la norme EN 50128 et EN 50129, ils remplissent toutes les exigences qui peuvent survenir dans les applications ferroviaires de sécurité critique – de SIL 2 pour les systèmes ATO à SIL 4 pour les applications de signalisation. Cela permet aux développeurs de se concentrer exclusivement sur le logiciel, sans tenir compte du matériel. En fonction de l'application finale, le niveau de sécurité du matériel peut être déterminé à tout moment et sans autre effort d'ingénierie.

Des domaines sécurisés réduisent l'effort de développement logiciel

La plate-forme matérielle menTCS est conçue de telle sorte que le logiciel de contrôle relatif à la sécurité est clairement isolé de tout logiciel périphérique non utilisé pour la certification. La plate-forme menTCS réalise ceci en exécutant les fonctions individuelles de contrôle de sécurité critique dans des domaines sécurisés distincts, en les gardant ainsi en dehors des fonctions générales d'E/S non-critiques. Cet isolement est effectué à la fois au niveau matériel et logiciel. Grâce à cette séparation stricte, la programmation de sécurité critique plus complexe se limite exclusivement aux domaines sécurisés, ce qui simplifie le développement logiciel et permet également une certification SIL plus facile et plus rapide. Après l'effort réduit de documentation pour le matériel, c'est le deuxième levier majeur pour des économies de coûts significatives par rapport à un développement en interne.



La plate-forme menTCS est le premier système au monde à être indépendant de l'application finale, car elle sépare les fonctions de contrôle de sécurité critique des fonctions communication d'E/S non critiques.

Une carte processeur haute sécurité SIL 4

Au cœur du contrôleur MH50C des menTCS se trouve la carte processeur F75P CompactPCI PlusIO certifiée SIL 4. Cette carte embarque trois processeurs Intel Atom E680T. Deux processeurs redondants assurent les fonctions de contrôle de sécurité critique. Ils sont liés à PCIe via un FPGA, qui gère la synchronisation des points de contrôle de l'application SIL 4 pour la redondance 2oo2 nécessaire. Le troisième processeur est responsable de la communication globale des E/S. Grâce à l'expérience à long terme de l'ensemble du marché avec ces processeurs, toutes les erreurs de sécurité critique trouvées jusqu'à présent sont connues et documentées. Tant que les directives disponibles pour ces cartes sont respectées, aucune erreur systématique pouvant influer le comportement de sécurité ne peut se produire. Pour plus d'informations, veuillez consulter https://www.men.de/products/f75p/

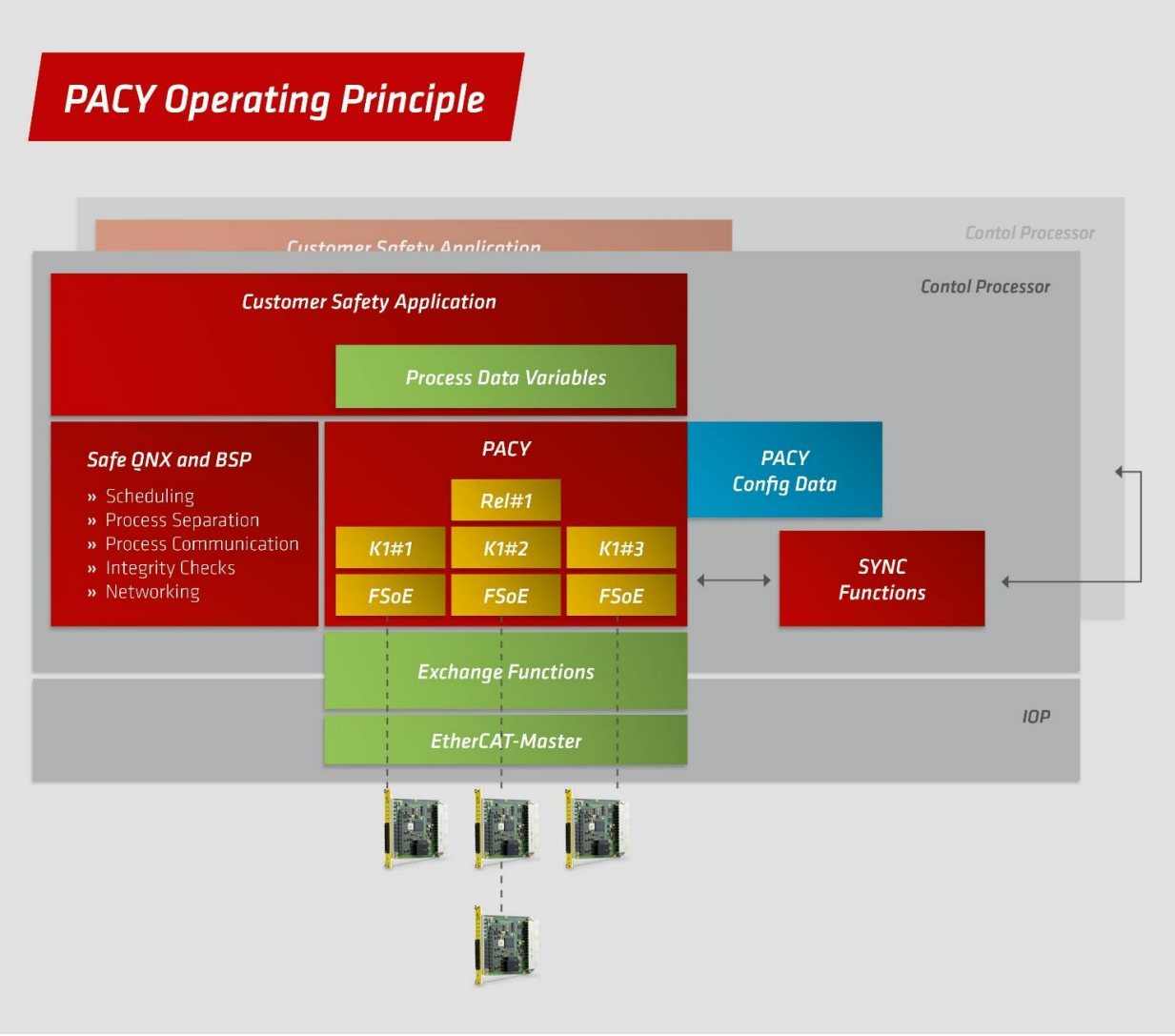
Des domaines sécurisés avec QNX Neutrino

Pour les applications de sécurité critique, le contrôleur MH50C de menTCS intègre le système d'exploitation temps réel QNX Neutrino, qui est spécifiquement adapté au matériel embarqué. Par rapport aux systèmes d'exploitation propriétaires, cette intégration seule permet aux développeurs et aux OEM d'économiser autour de deux millions d'euros sur les coûts du projet et leur permet d'éviter tous les risques associés à la certification. Le BSP (Board Support Package) de la carte pour la mise en œuvre de QNX Neutrino est pré-certifié SIL 4 sur la plate-forme menTCS et offre donc dès le départ le plus haut degré de fiabilité.

QNX Neutrino utilise une architecture de micronoyau qui isole strictement les processus logiciels les uns des autres, ce qui empêche que la performance et le comportement des autres processus ne soient affectés. Ceci garantit à son tour que le système reste dans un état sécurisé à tout moment, puisque même des logiciels malveillants ne peuvent avoir d'influence sur les processus de sécurité critique. En outre, QNX Neutrino® supporte la séparation et l'utilisation souple de la bande passante du processeur. Les applications critiques de sécurité peuvent être programmées en C ou en Ada, ainsi que sur la base de modèles – par exemple dans des environnements de programmation SCADE ou Soft PLC. Les développeurs peuvent souvent rester dans leur environnement de développement familier, ce qui minimise les re-certifications coûteuses. D'autres systèmes d'exploitation, tels qu'INTEGRITY de Green Hills, PikeOS de Sysgo ou VxWorks de Wind River, peuvent être implémentés sur demande.

Un cadre de travail pour des communications d'E/S unifiées

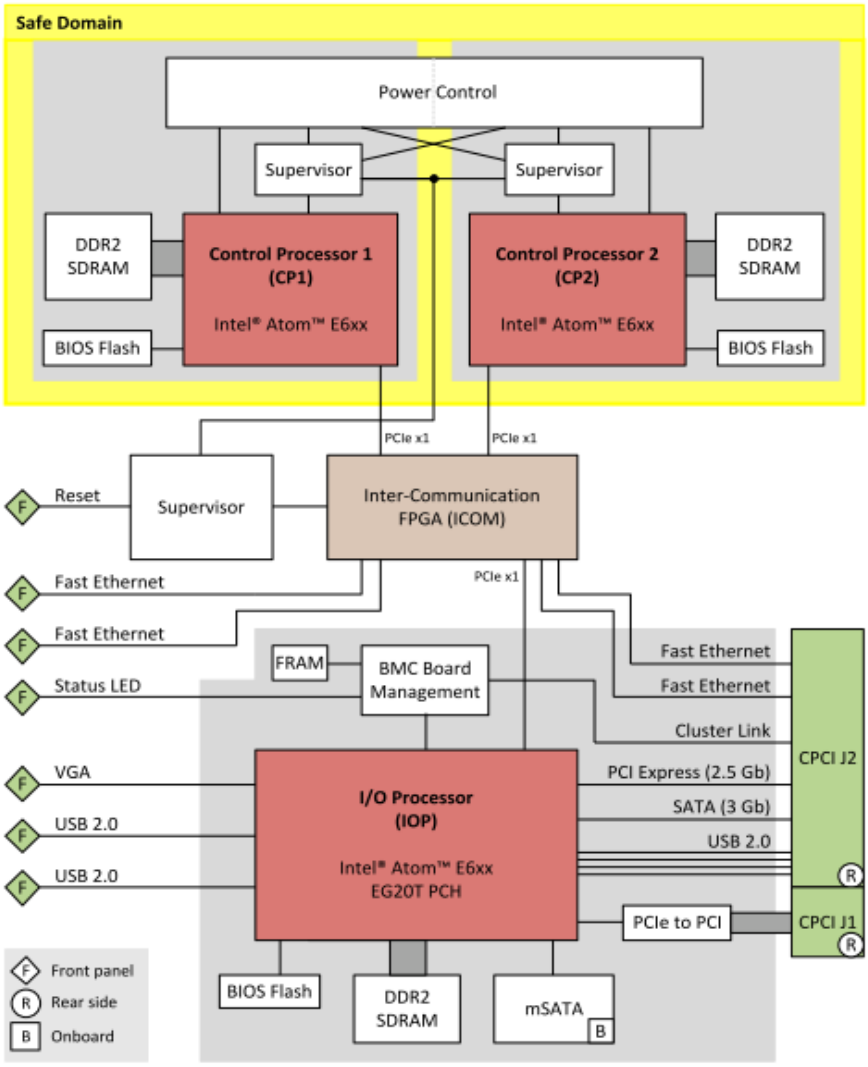
Pour simplifier la gestion des E/S dans un domaine sécurisé, MEN Mikro Elektronik a intégré l'infrastructure d'E/S PACY dans le domaine sécurisé, qui introduit une couche d'abstraction transparente entre le domaine sécurisé et le domaine des E/S. Cela signifie que des fonctions identiques sont toujours traitées de la même manière dans le même domaine, et deviennent indépendantes de l'exécution effective des entrées et des sorties. Avec PACY, qu'une commande porte sur un relais ou une E/S numérique n'a plus aucune influence. Cela rend l'intégration de menTCS beaucoup plus simple et plus souple. Les systèmes de train et de voie avec différents capteurs et actionneurs pour les mêmes fonctions peuvent désormais être équipés de systèmes de contrôle identiques, ce qui non seulement simplifie immensément les rénovations, mais aussi le déploiement de nouvelles technologies.



L'infrastructure d'E/S PACY unifie la communication entre le domaine sécurisé avec des logiciels applicatifs de sécurité spécifiques et le domaine des E/S

PACY est implémenté en tant qu'infrastructure souple sur une base modulaire, ce qui facilite toute extension avec des modules individuels, spécifiques au client, ainsi que la communication avec toute application en C. A l'avenir, les développeurs seront également en mesure de définir des blocs fonctionnels PACY qui combineront plusieurs tâches en une seule macro-commande. De cette manière, des procédés fréquemment utilisés, tels que la fonction de freinage d'urgence, peuvent être activés simplement sans qu'il ne soit nécessaire de les reprogrammer selon chacun des cas. La communication entre la commande de sécurité et le frein de sécurité est fait dans le domaine des E/S.

Le domaine des E/S avec Linux



F75P CPU board block diagram

La carte contrôleur F75P de menTCS est certifiée SIL 4 et est composée de trois processeurs Intel Atom E680T : deux en redondance pour les éléments de sécurité, et un pour les communications d'E/S

Puisque le troisième processeur Intel Atom gère la connexion aux E/S de manière totalement séparée du domaine sécurisé, il est garanti que le domaine des E/S ne pourra jamais influencer la logique de commande de sécurité. MEN Mikro Elektronik utilise à cette fin un système d'exploitation Linux pré-intégré et pré-certifié. Cela donne aux clients l'accès à un écosystème entièrement développé et éprouvé avec des outils sur-étagère et des pilotes qu'ils peuvent utiliser immédiatement. Des OS supplémentaires sont disponibles sur demande.

La communication entre le système sécurisé et les cartes d'E/S du contrôleur menTCS et des boîtiers d'E/S est basée sur le protocole EtherCAT. EtherCAT est un standard Ethernet temps réel, avec des cycles de moins de 5 millisecondes, qui répond à toutes les exigences pour une communication sécurisée avec les composants menTCS. EtherCAT ne requiert aucun commutateur car il supporte une topologie en anneau avec canaux de communication redondants. EtherCAT utilise le protocole de sécurité Fail Safe over EtherCAT (FSoE) pour détecter de manière fiable des paquets de données modifiés, dupliqués ou perdus. L'ensemble de la liaison de communication des E/S fonctionne par conséquent comme un Black Channel, qui assure la sécurité de fonctionnement requise pendant la communication.

Conclusion: menTCS est une plate-forme unique pour les applications ferroviaires de sécurité critique

La plate-forme « prête à l'emploi » menTCS de MEN Mikro Elektronik est parfaitement adaptée pour toutes les applications ferroviaires intelligentes de sécurité critique. Elle propose aux opérateurs de trains et de voies ainsi qu'aux fournisseurs d'automatisation et aux sociétés tierces de nombreux avantages qui sont à ce jour unique sur le marché des applications ferroviaires intelligentes. Les grands équipementiers, qui dominent actuellement le marché des applications certifiées SIL, gagneront tout autant à partir de ces plates-formes innovantes que les jeunes start-ups et les décideurs professionnels, qui peuvent avoir moins d'intérêt pour les exigences techniques mais qui veulent mettre en œuvre des solutions ferroviaires intelligentes innovantes ouvertes à l'IoT. Il est même possible de réduire la taille des plates-formes menTCS pour les rendre compatibles avec des applications ferroviaires simples telles que l'info-divertissement ou la surveillance vidéo des portes et des compartiments de passagers. De cette façon, des solutions fortement multifonctionnelles peuvent être mises en œuvre à tout moment avec une plate-forme technologique unique. Toute personne qui développe des plates-formes ferroviaires intelligentes devrait certainement envisager la plate-forme menTCS dans le cadre de son processus d'évaluation et d'approvisionnement, la tester rigoureusement et calculer le retour sur investissement attendu parce que les plates-formes modulaires SIL prêtes à l'emploi pour une industrie spécifique seront déterminantes pour l'avenir. Ceux qui ne monteront pas à bord de cette nouvelle technologie au moment opportun risquent littéralement de manquer le train !