

La haute fiabilité des technologies SNCC de Yokogawa

Les systèmes CENTUM CS et CENTUM CS3000 sont sur le marché depuis plus de 10 ans et sont utilisés avec succès sur de nombreuses applications stratégiques et critiques.

Le contrôleur du CENTUM CS3000 utilise l'architecture unique « Pair and Spare ». Elle est basée sur l'utilisation d'une paire de processeurs au sein même des unités centrales « Pair ». Associée à une seconde unité centrale (elle-même « Pair ») pour assurer une redondance, l'ensemble qui comprend 4 processeurs est alors en structure « Pair and Spare ».

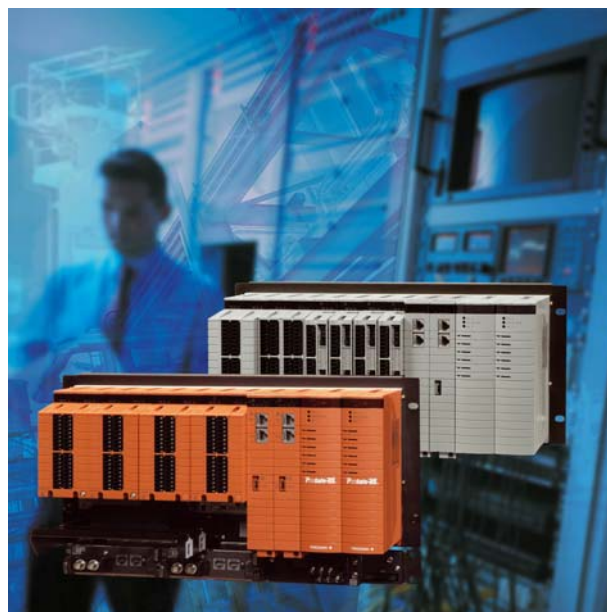
Par ailleurs, le CENTUM CS3000 dispose d'autres possibilités de redondance pour les E/S, les différents bus de communication, les alimentations électriques, ...

Ce concept mis au point par Yokogawa assure ainsi des niveaux de fiabilité et disponibilité inégalés.

Comme résultat de cette unique technologie, les statistiques issues du terrain montrent que la disponibilité opérationnelle du système comprend sept 9 ou en réalité 99.9999953%.

En d'autres termes, cela représente une minute d'arrêt sur 40 années d'exploitation.

Aussi Yokogawa a réutilisé les mécanismes largement éprouvés du CS3000, tant matériels que logiciels, comme base de développement du contrôleur de sécurité qui se nomme *ProSafe-RS*.



ProSafe-RS (orange) et CS3000 (gris), une ressemblance frappante !

Nota :

ProSafe-RS prend l'appellation de contrôleur de sécurité lorsqu'il est associé au CENTUM CS3000, par analogie au contrôleur standard.

Utilisé seul, on utilisera plutôt le terme d'automate de sécurité.

SIL3 de base

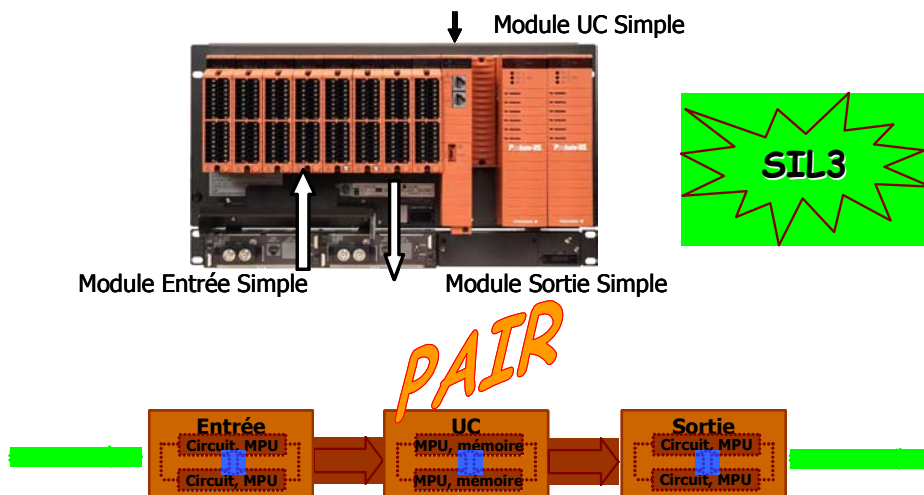
Le contrôleur de sécurité *ProSafe-RS* embarque les mêmes architectures et les mêmes technologies que celles des contrôleurs du *CS3000*. Chacun des modules Entrées, Unités Centrales, Sorties dispose d'une architecture interne redondante pour garantir le plus haut degré de sécurité, pour toutes les applications de niveau SIL3 (ou inférieur).

L'unité centrale de *ProSafe-RS*, ne contient pas seulement des processeurs redondants mais dispose aussi de mémoires redondantes, de circuits additionnels et de logiciels spécialisés pour les diagnostics.

Selon le même principe, les modules d'entrées et de sorties sont équipés de circuits redondants pour des contrôles infaillibles de l'intégrité des informations.

Cette architecture, fait de *ProSafe-RS*, un contrôleur de sécurité très simple et facile à comprendre, à mettre en œuvre et à maintenir dans le respect du niveau d'intégrité requis.

Les fonctions de sécurité de niveau SIL3 sont assurées par une unité centrale simple et des modules d'E/S simples qui remplissent pleinement les prescriptions de la norme CEI61508, comme les PFD (Probabilité de défaillance à la sollicitation), SFF (taux de défaillances non dangereuses) et tolérance aux défaillances du niveau d'intégrité SIL3.



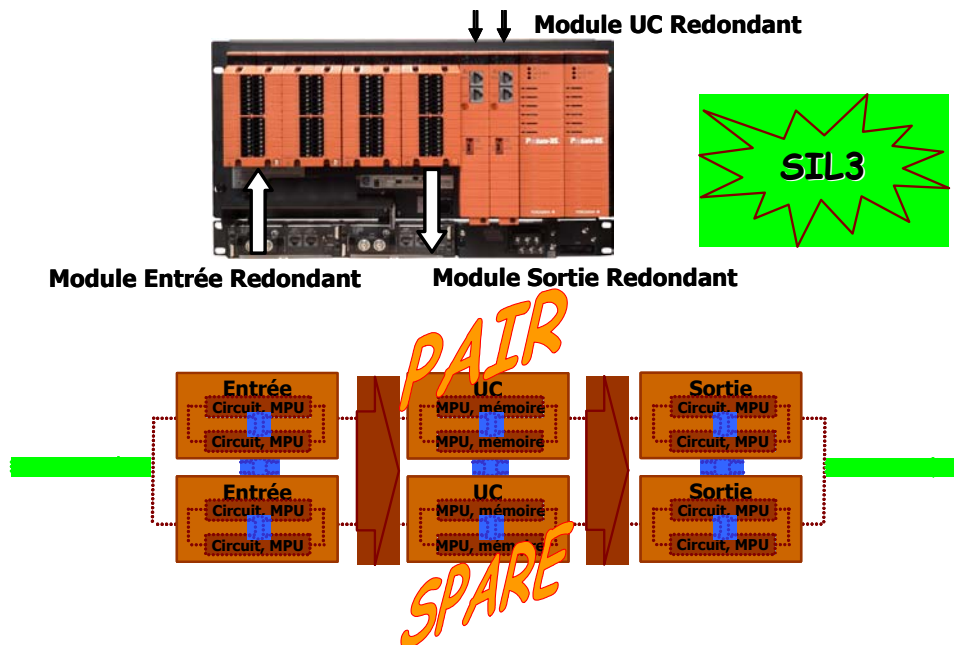
Redondance « à la carte » pour la meilleure disponibilité

Lorsque les plus hautes disponibilités sont requises, *ProSafe-RS*, peut être constitué d'unités centrales redondantes et de modules d'E/S redondants, de la même façon que pour le CENTUM CS3000.

La redondance n'est utilisée que là où elle se justifie. Elle est donc disponible « à la carte ». Toutes les combinaisons de redondance sont possibles : unité centrale et tout ou partie des modules d'E/S.

Par exemple, entrée redondante (car un seul capteur) avec sorties simples (car plusieurs actionneurs), entrées simples (car plusieurs capteurs) avec sortie redondante (car un seul actionneur) et enfin entrées redondantes avec sorties redondantes. La mixité la plus totale est possible permettant ainsi de ne redonder que les voies des fonctions les plus critiques en matière de disponibilité.

En outre, les diagnostics ayant un taux de couverture de plus de 99%, *ProSafe-RS* offre des temps de détection de panne et par conséquent de dépannage les plus courts avec un impact minimal sur le procédé.



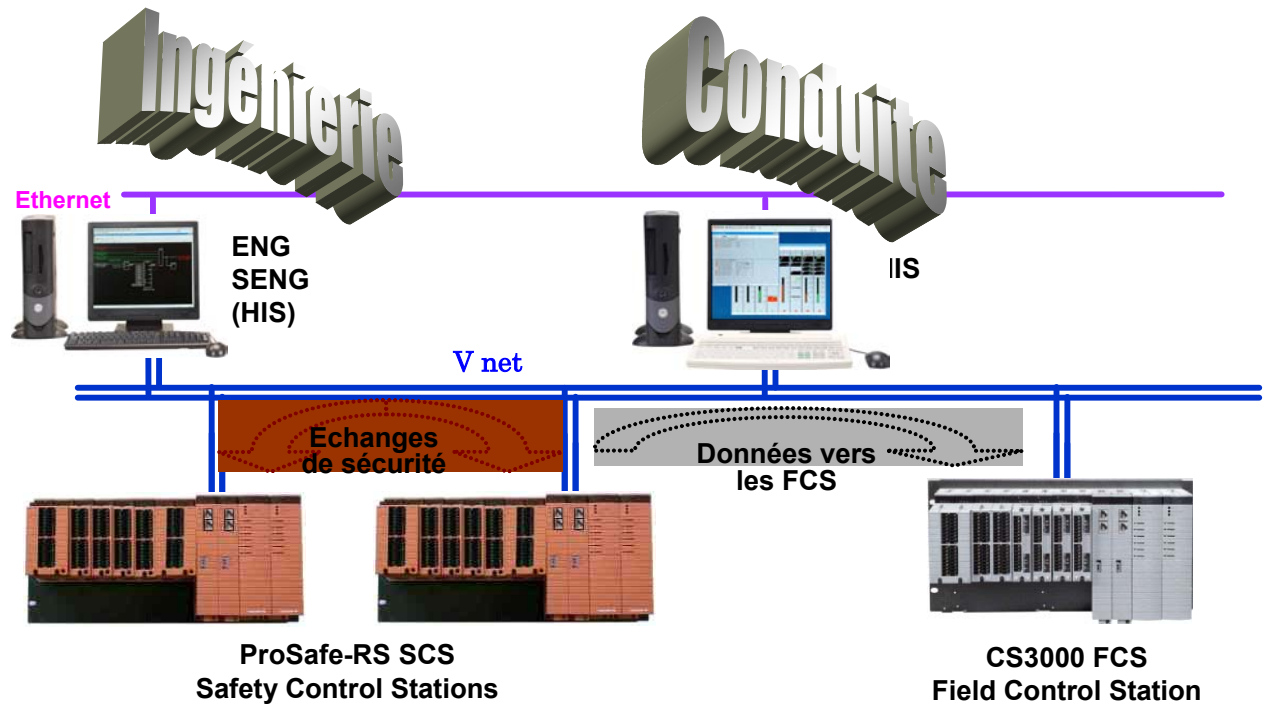
Par ailleurs, cette architecture permet les pannes croisées. Les deux chaînes qui pourraient être vues comme fonctionnant en parallèle acceptent en fait toutes les permutations de module à module.

Ainsi, l'entrée représentée en « haut » peut être gérée par l'unité centrale du « bas » qui elle-même piloterait la sortie du « haut ».

Un seul réseau, une seule fenêtre !

En plus de son très haut degré de sécurité et sa très haute disponibilité, *ProSafe-RS* s'intègre parfaitement avec le CENTUM CS3000. Il peut être connecté directement sur son réseau. Pas de passerelle de communication ni d'interface matérielle n'est nécessaire pour l'échange de données entre SNCC et SIS.

Par ailleurs, la communication (pour des fonctions de sécurité) entre contrôleurs de sécurité est possible. Elle est certifiée dans une architecture globale mixte qui comprend aussi une partie contrôle commande classique.



ENG : outils d'ingénierie de CS3000
SENG : outils d'ingénierie de *ProSafe-RS*
HIS : poste de conduite

Cette intégration permet aux opérateurs d'avoir accès à toutes les informations issues du procédé via une « seule fenêtre » de conduite du CENTUM CS3000.

Les opérateurs ont ainsi une meilleure vue d'ensemble. Ils peuvent agir plus rapidement et plus efficacement lors de dérives du procédé, ils peuvent anticiper.

Une gestion globale du procédé n'est pas uniquement intéressante en termes de conduite mais elle permet aussi d'éviter des erreurs de jugement et de mauvaises décisions.

Enfin en termes de diagnostics, les mêmes vues permettent de disposer nativement d'informations sur la santé du système tant coté contrôle que coté sécurité. La aussi, les avantages en termes d'analyse et d'efficacité d'intervention sont évidents.

La partie ingénierie, quand à elle, garanti une séparation du contrôle et de la sécurité. En effet, un contrôle des accès et des habilitations est assuré. Les logiciels ENG ne « voient » que les contrôleurs CS3000 alors que les logiciels SENG ne « voient » que les contrôleurs de sécurité *ProSafe-RS*.

La mémoire des contrôleurs de sécurité est protégée contre toute action externe pendant la phase de marche industrielle du procédé. Seules les personnes habilitées pourront intervenir.

Certification TÜV



Les certifications du TÜV sont mondialement reconnues comme étant indépendantes et crédibles sur le fait qu'un produit remplisse les conditions indispensables pour assurer des fonctions de sécurité, et ce en regard de la normalisation.

Depuis la phase de conception de *ProSafe-RS*, le TÜV (Rheinland) a été impliqué. Il a vérifié sa conformité au regard de la CEI61508 qui définit les spécifications générales à appliquer aux systèmes de sécurité.

Par ailleurs, *ProSafe-RS* est également certifié selon la CEI61511 qui concerne la sécurité du secteur des industries de procédé.

C'est le premier automate au monde à disposer de la double certification 61508 et 61511 !

Ses langages de programmation ont été certifié selon le CEI611131-2 (2003).

ProSafe-RS est également certifié pour des applications BMS, feu & gaz, four, ... selon les EN298(2004), EN 50156 (2004), NFPA85 (2001), EN54-2 (2004) et NFPA72 (2002).

TÜV : « Technischer Überwachungs Verein », organisme de certification allemand qui fait foi en matière de sécurité.

Philippe PRIMARD

Responsable de l'activité Systèmes de Sécurité