

Design d'un système de sécurité des personnels PSS d'accélérateur

Utilisation d'un système d'automatisme de sécurité

Harold BZYL, CNRS/INP-iRSD (UAR3364), Orsay, France

Topologie matérielle & implantation

Sur cet exemple, le PSS est basé sur un automate Simatic S7-1516F [1] relié par une communication sécurisée annulaire (protocole Media Redundancy Protocol [2]) (fig.1). Le MRP est un protocole standardisé utilisé pour éviter des pannes en un seul point et d'assurer des délais de récupération égaux ou inférieurs à 10 ms.

Les unités périphériques sont :

- Écran pour la supervision de l'ensemble du PSS en salle de contrôle
- Écrans pour le service, l'exploitation et les alarmes
- Périphériques décentralisés (ET200), cartes E/S standards, sécurisées & analogiques
- Routeurs managés
- Alimentations secours

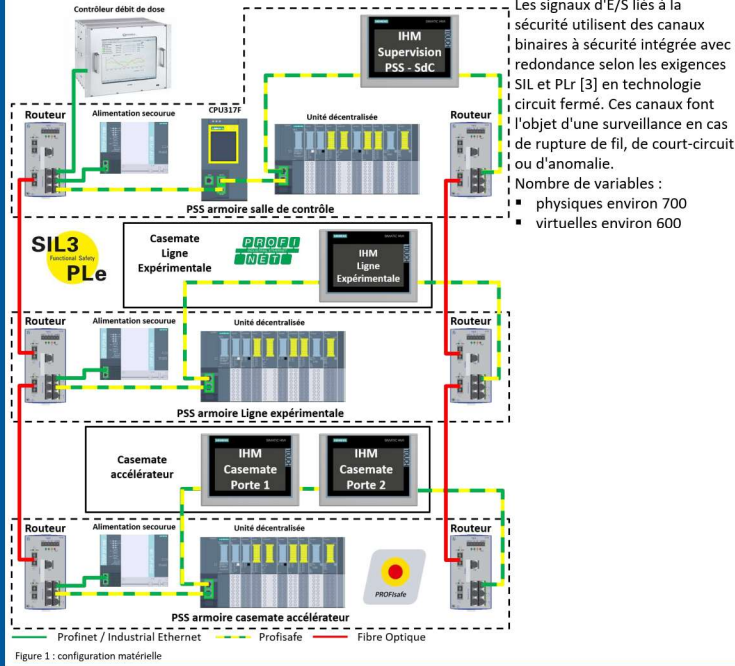


Figure 1 : configuration matérielle

Les signaux d'E/S liés à la sécurité utilisent des canaux binaires à sécurité intégrée avec redondance selon les exigences SIL et PLr [3] en technologie circuit fermé. Ces canaux font l'objet d'une surveillance en cas de rupture de fil, de court-circuit ou d'anomalie.

- Nombre de variables :
- physiques environ 700
 - virtuelles environ 600

IHM

L'interface homme-machine (IHM) est le maillon entre l'opérateur, l'utilisateur et un processus automatisé du PSS. L'IHM permet aux opérateurs et aux utilisateurs de visualiser les données et de gérer les processus comprenant environ 700 variables physiques et 600 variables virtuelles.

Les avantages dans notre cas sont :

- ✓ L'intégration des IHM dans la topologie matérielle est dans l'anneau MRP
- ✓ Le développement des IHM se fait directement dans TIA Portal V17© [1]
- ✓ Visualisation
- ✓ Maintenance

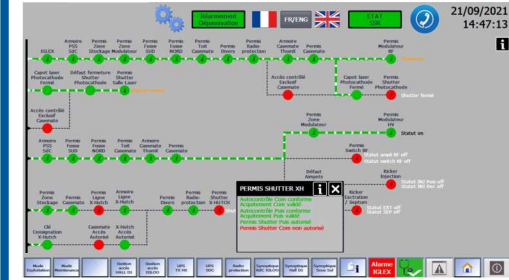


Figure 2 : écran salle de contrôle

L'écran de la salle de contrôle (fig.2) permet de superviser en temps réel l'ensemble du PSS de l'accélérateur. Il permet de visualiser :

- Les modes d'exploitation et de maintenances
- La gestion des accès
- La visualisation des alarmes (incendie, anoxie, ventilation)
- Les états du système de surveillance radiologique (alarme et seuil des balises)
- Les synoptiques de l'installation
- Les diagnostics et alarmes de l'automate
- Les notices d'aide

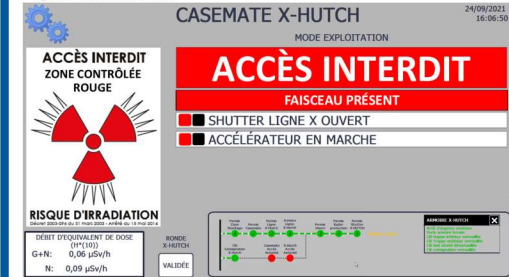


Figure 3 : écran ligne expérimentale

L'écran de la ligne expérimentale (fig.3) permet aux utilisateurs de connaître en temps réel l'état du PSS de la ligne expérimentale. Il permet de visualiser :

- Les états de l'accès à la ligne
- L'état du bloqueur de ligne et de l'accélérateur
- Le niveau de la dosimétrie de la ligne

Capteurs et interverrouillage à technologie RFID

La technologie RFID est de plus en plus utilisée sur les capteurs (fig.5) et interverrouillages (fig.6) de sécurité, car elle présente de nombreux avantages.

Capteur RFID :

- ✓ Pas de contact mécanique;
- ✓ Niveau de codification élevé;
- ✓ SIL 3 / PLe;
- ✓ Plus de discordance entre les 2 voies.



Figure 5 : capteur RFID

Interverrouillage intégrant des hauts niveaux de sécurité :

- ✓ SIL3 / PLe avec un seul dispositif;
- ✓ Force de retenue 9750 N;
- ✓ Niveau de codification élevé;
- ✓ Déverrouillage d'urgence.

Figure 6 : interverrouillage RFID

Mise en œuvre du logiciel PSS

Les automates de sécurité sont configurés et programmés à l'aide de TIA Portal V17© [1]. Les programmes de sécurité et standard sont séparés par des tableaux de codes différents. Le code de sécurité est exécuté dans un cycle fixe (100 ms) et est contrôlé contre la falsification des données pendant l'exécution. Il comprend toutes les fonctions de sécurité (voir tab.1). Les modifications non autorisées du logiciel ou de la configuration provoquent un changement de CRC (contrôle de redondance cyclique) et entraînent la perte de l'autorisation de fonctionnement.

Programme de sécurité	Programme Standard
Modes (exploitation, maintenance) de fonctionnement PSS	Communication standard
Ronde et statut des casemates	Gestion des alarmes
Permettre l'ouverture des portes	Supervision
Délivre les autorisations de l'accélérateur et les lasers interlocks detection	Gestion des signalisations (non sécurisés)
Surveillance radiologique, ventilation, incendie et anoxie	
Communication de sécurité	
Surveillance des équipements	

Tableau 1 : Tâches principales du logiciel PSS

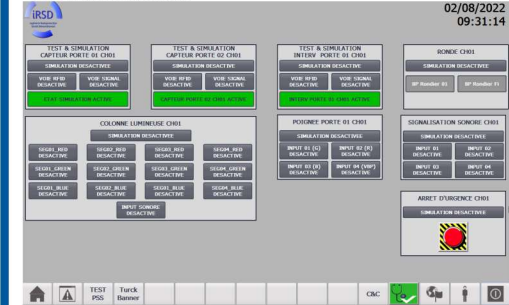


Figure 4 : écran des vérifications périodiques

Écran des vérifications périodiques (fig.4)

Afin simplifier les procédures de vérification périodique, l'iRSD développe une IHM portable pour réaliser les vérifications. Ce protocole est asservi à une clé test, le simple retrait de la clé inhibe le protocole de test, désactive toutes les fonctions de test, et réinitialise le programme (état initial).

Banc de développement, de test et de simulation

L'iRSD a développé 2 châssis mobiles lui permettant sur 1m² de disposer de tous les équipements constituant un PSS de dernière génération (automate de sécurité, Routeur managable, HMI, rondier, arrêt d'urgence, capteur de porte, système de verrouillage, système de signalisation sonore et lumineux...) dans le but de :

- ✓ Développer, tester et simuler les fonctionnalités d'un PSS
- ✓ Faire de la veille technologique
- ✓ Former des stagiaires, apprentis...
- ✓ Former les personnels travaillant sur les accélérateurs à l'utilisation de tel système.



Figure 7 : châssis banc

Normes et évaluations des risques

Une évaluation détaillée des risques doit être réalisée conformément à la norme CEI 61508 [4]. Les fonctions de sécurité doivent être formulées et leur niveau de mise en œuvre (SIL) doit être déterminé en tenant compte des mesures organisationnelles et techniques.

Les fonctions de sécurité de l'accélérateur de particules exigent un niveau SIL3 conforme à la nouvelle version de la norme NF M 62-105 de juin 2021 [5]

[1] <https://new.siemens.com/fr/fr/products/automatisation-entrainements.html>

[2] CEI, réseaux de communication industriels - Réseaux d'automatisme à haute disponibilité - Partie 2: Protocole de redondance du support (MRP), IEC 62439-2, 2016

[3] ISO, sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1: Principes généraux de conception, 13849-1, 2015

[4] CEI, Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Partie 1: Prescriptions générales, 61508-1, 1998

[5] AFNOR, Énergie nucléaire - Accélérateurs utilisés dans les domaines industriels et de la recherche : installations. [Normes], Paris : AFNOR, 2021. M62-105