Sécurité - Marronniers

Des normes qui évoluent, des choix à faire, des retours d'expériences qui refroidissent, des mises à niveau devenues impossibles… les difficultés s'amoncellent dans le domaine de la sécurité, et les mises en place deviennent encore plus complexes avec l'arrivée des fonctions programmées.

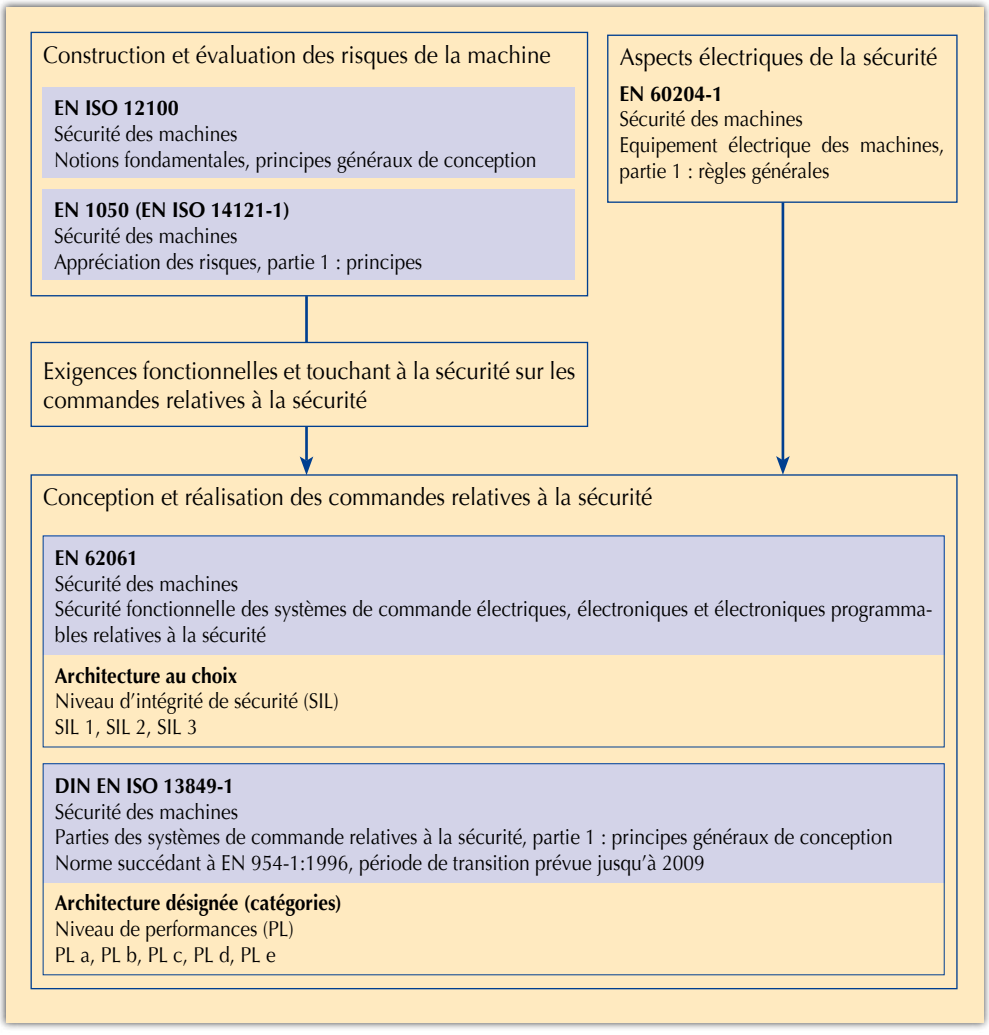
Dans le langage journalistique il y a ce que l'on nomme « les marronniers ». Ce sont les sujets qui reviennent sans cesse sous les feux de la rampe. Comment maigrir dans les numéros du mois de mai, ou comment rentrer dans son maillot pour le mois de juin, bref dans nos domaines techniques, il en est un qui revient souvent c'est celui sur la Sécurité. Et le Club Automation ressent le même phénomène, lui qui, tout juste un an après une journée consacrée à la sécurité, vient d'en clôturer une nouvelle, avec succès d'après l'accueil réservé par les participants.

ELLES SONT INCONTOURNABLES

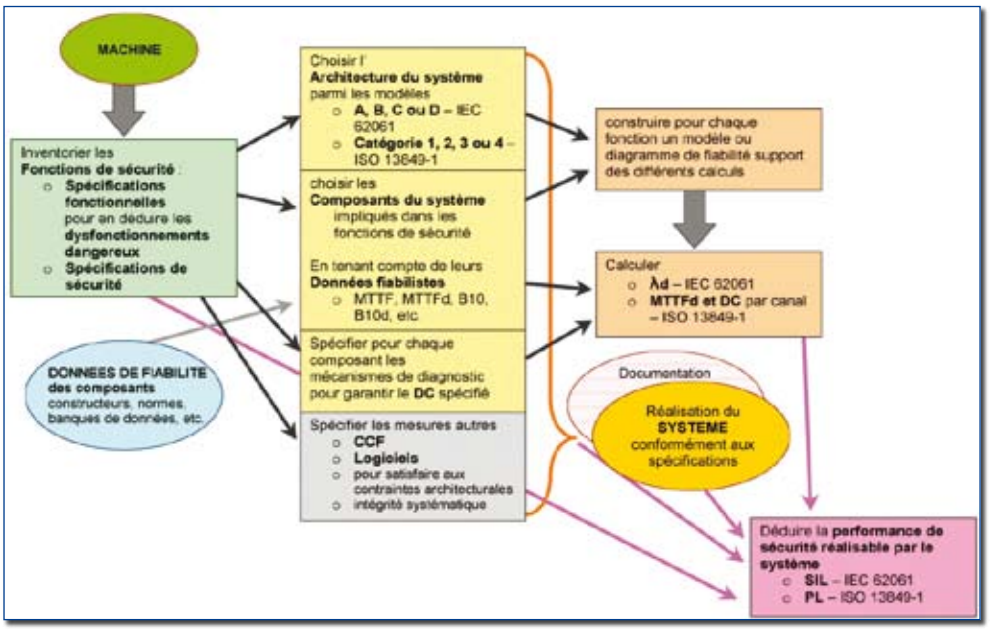
Alors que vous soyez spécialistes ou non des normes de sécurité, le dilemme entre l'IEC/EN 62061 et l'IEC/EN 13849-1 se posera tout ou tard. Des normes différentes, concurrentes, complémentaires ? Difficile d'y voir clair, et ce ne sont les propos de Jean-Pierre Buchweiller, analyste de sûreté de fonctionnement de systèmes électroniques, de l'INRS qui nous ont rassurés.

En effet, les choses ne devraient pas aller en s'arrangeant, car « *l'offre de composants d'automatismes se multiplie et se complexifie* » note Jean-Pierre Buchweiller. Ce sont ces composants qui vont intégrer une machine, et les concepteurs devront résoudre la problématique de la sécurité. Même l'INRS annonce qu'il ne tentera pas de convaincre l'assistance que l'utilisation de ces textes sera aisée, mais que malgré leurs complexités, leurs lacunes, leurs imprécisions, ils sont incontournables.

Par rapport à l'ancienne EN 954-1, ces nouvelles normes apportent des réponses impossibles auparavant. Jusqu'ici si dans une machine le concepteur mettait en place un capteur de catégorie 1, une unité de traitement de catégorie 4



Normes fondamentales de la conception des fonctions de commande. (doc. Festo)



IEC/EN 62061 vs. ISO/EN 13849-1. Démarche de conception préconisée par les deux textes.

et une interface de sortie de catégorie 3, personne n'était capable de donner le niveau de sécurité de la machine, et pourtant c'est bien la seule chose importante. Impossible de faire une formule mathématique résultant des catégories pour obtenir le chiffre final. Il fallait de nouveaux référentiels, et c'est ce qu'apportent ces nouvelles normes.

L'EN 954-1 aura répondu aux problèmes simples lorsque les modes de défaillance étaient correctement appréhendés, mais dès que le nombre de composants augmentait elle s'est vite avérée dépassée. Les nouvelles normes proposent cette démarche globale de conception en incluant des méthodes simplifiées et surtout en prenant en compte la fiabilité des composants.

Des normes écrites pour corriger les lacunes de l'EN 954-1, mais elles montrent déjà leurs limites. En dehors de la complexité de compréhension propre aux normes, elles restent des normes de conception d'installation, et non de machines existantes. Et cette limitation vaut également pour les machines conçues et validées avec cette norme et qui seront upgradées, que ce soit mécaniquement ou informatiquement, difficile de faire évoluer l'ensemble. A l'heure de la flexibilité, le frein est évident.

Pour bien démarrer dans sa réflexion, il ne faudra pas négliger les spécifications des fonctions de sécurité, souvent passées trop rapidement. Plusieurs choix se présentent au concepteur, la solution de facilité consistant à mettre de la sécurité niveau 4 partout mais avec le risque de se trouver devant une machine ingérable avec des impasses techniques et des surcoûts très importants comme une redondance de l'ensemble de l'installation.

De même, il faudra mettre dans la boucle de travail les concepteurs du circuit de commande dès l'origine afin de spécifier correctement les fonctions à réaliser, les limites de ces fonctions et les dysfonctionnements dangereux. Sans ce travail de groupe, le circuit réalisé ne pourra pas répondre aux attentes, entraînant des reprises *a posteriori*, pouvant être dommageables pour la sécurité des personnes.

62061 OU 13849-1 ?

Quelle que soit la méthode employée, il faut savoir que les performances de sécurité obtenues au terme du développement seront équivalentes mêmes si les réponses techniques sont différentes, comme l'indique Jean-Pierre Buchweiller *« Mettez 4 experts et vous obtiendrez 4 réponses différentes et les 4 auront raison »*. Chacun aura une vue fiabiliste différente, aboutissant à un diagramme différent.

Sachant qu'il est impossible de « décalquer » un développement issu de l'EN954-1 en EN 62061 ou 13849-1, que faire des systèmes développés avec l'EN 954-1 ? Pour les systèmes à courte espérance de vie, la conformité pourra être justifiée par l'application d'une norme harmonisée et ne sera pas forcément remise en cause tant que le système n'est pas modifié. Pour les autres cas, et notamment en cas de modifications, il

	Technologie mettant en oeuvre la(les) fonction(s) de commande relative(s) à la sécurité	ISO 13849-1	CEI 62061
A	Non électrique, par exemple hydraulique	X	Non couvert
B	Electromécanique, par exemple relais, et/ou électronique non complexe	Limité aux architectures désignées[a] et jusqu'à PL = e	Toutes architectures et jusqu'à SIL 3
C	Electronique complexe, par exemple programmable	Limité aux architectures désignées[a] et jusqu'à PL = d	Toutes architectures et jusqu'à SIL 3
D	A combiné avec B	Limité aux architectures désignées[a] et jusqu'à PL = e	X[c]
E	C combiné avec B	Limité aux architectures désignées[a] et jusqu'à PL = d	Toutes architectures et jusqu'à SIL 3
F	C combiné avec A, ou C combiné avec A et B	X[b]	X

X indique que ce cas est traité par la Norme internationale indiquée en tête de colonne.

[a] Les architectures désignées sont définies en 6.2 afin de fournir une approche simplifiée de la quantification du niveau de performance.
[b] Pour l'électronique complexe : utilisation des architectures désignées conformes à la présente partie de l'ISO 13849 jusqu'à PL = d ou toute architecture conforme à la CEI 62061.
[c] Pour la technologie non électrique, utilisation des parties en tant que sous-systèmes conformes à la présente partie de l'ISO 13849.

Utilisation recommandée de la CEI 62061 et de la présente partie de l'ISO 13849.

faudra soit valider le processus de conception qui a conduit au système, soit « redesigner » le circuit dans ce nouveau cadre, avec le risque de modifications importantes.

Quelle que soit la nouvelle norme choisie, sachez qu'il existe des logiciels disponibles qui vous aideront, mais il ne faudra pas incriminer les normes des inconvénients dus aux logiciels.

Alors quelle norme choisir ? Vous trouverez un tableau qui montre les spécificités de chacune, dans les faits pour les technologies autres qu'électriques, la seule norme qui s'applique est la 13849-1.

La difficulté vient du fait que les textes sont concurrents, voire contradictoires. C'est le point noir, des tests ont montré que les résultats d'analyses convergeaient dans la moitié des cas, mais divergeaient de plus ou moins un niveau de SIL dans une moitié des cas, et allaient même jusqu'à diverger de deux niveaux de SIL dans certains cas particuliers. Ce qui incite Jean-Pierre Buchweiller à conclure : « *les résultats de l'estimation du risque selon qu'elle aura été conduite avec l'une ou l'autre norme, peuvent diverger notoirement et, au final, entraîner des conséquences dommageables sur la sécurité des personnes… il nous semble que la méthode présentée par l'ISO/EN 13849-1 puisse être préférée* ». Une réponse qui a le mérite d'être claire.

IEC/EN 62061		ISO/EN 13849-1	
Description	*Désignation*	*Description*	*Désignation*
Simple canal, sans fonction de diagnostic	Type A	**Simple canal**, couverture du diagnostic nulle	Catégorie 1
Double canal, sans fonction de diagnostic	Type B	**Double canal**, couverture du diagnostic faible ou moyenne	Catégorie 3
Simple canal, avec fonction de diagnostic	Type C	**Simple canal**, couverture du diagnostic faible ou moyenne	Catégorie 2
Double canal, avec fonction de diagnostic	Type D	**Double canal**, couverture du diagnostic élevée	Catégorie 4

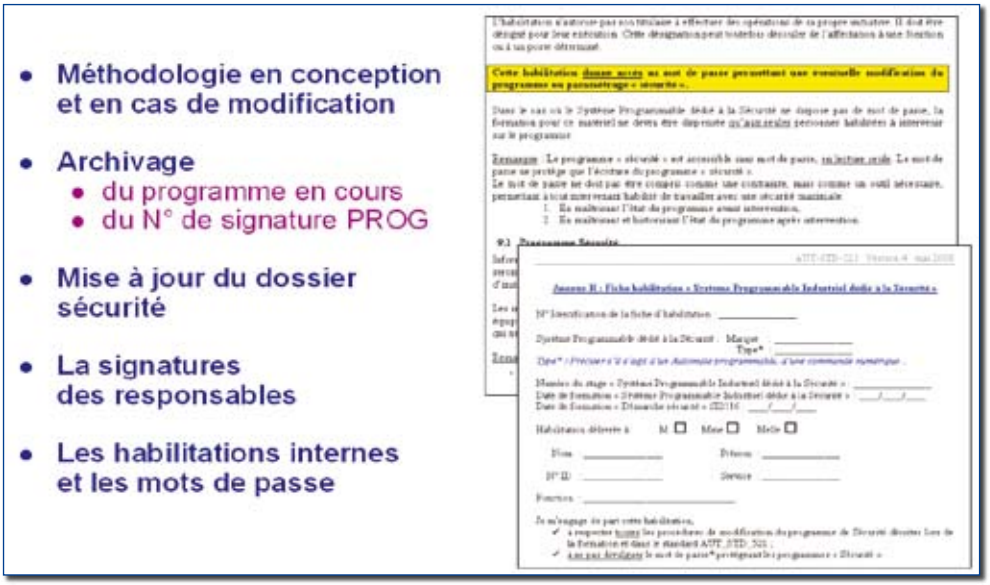
Normes concurrentes ? complémentaires ? Les architectures définies pour les circuits de commande sont très voisines, voire équivalentes.

Et demain, comme hier, sans référentiel normatif, les concepteurs de circuits de commande relatifs à la sécurité auront de très grandes difficultés à justifier la conformité de leurs machines aux exigences de la directive. Le concepteur doit impérativement se positionner, car l'EN 954-1 est fini, il doit s'approprier une nouvelle norme, sans attendre la norme idéale et le texte parfait.

LA « VIE SÉRIE » AU CŒUR DE LA PROBLÉMATIQUE PSA

Laurent Mauguy, Responsable des activités transversales automatismes et homologation du groupe PSA, tient à préciser dès le début de sa présentation, lors de cette journée du Club Automation, que malgré un contexte difficile dans l'automobile, la sécurité reste un invariant et une préoccupation majeure. *« Aucune économie ne sera faite sur ce sujet »*.

Depuis longtemps, PSA a mis en place une méthodologie de maîtrise de la sécurité des biens d'équipements qui se résume à l'application de normes et standards de sécurité pour le câblage, les portillons, les règles de programmation… mais effectue également une analyse de risques en commun avec les intégrateurs. Mais au-delà de l'évolution des normes, la préoccupation majeure reste l'intégration et la mise en œuvre concrète des composants ainsi que leur gestion en « vie série ». Le mot est lâché, « vie série », un terme qui montre que l'arrivée de fonctions programmées, de sujets de plus en plus complexes emmènent des difficultés lors de la vie d'une installation, est-elle toujours conforme au fil du temps ?



Procédure mise en place chez PSA.

Car sans nul doute les APIdS (Automate Programmables Industriels de Sécurité) apportent des simplifications de mise en œuvre avec la réduction des armoires, des câblages en diminution et une simplification des programmes de sécurité. Tout semble positif dans le choix des APIdS, reste à régler le problème de la vie série, *« aujourd'hui le groupe PSA est plutôt dans une stratégie d'industrialisation avec une grande majorité de modifications de ses installations »* précise Laurent Mauguy.

Et en matière de fonctions de sécurité, le groupe PSA a parfois l'impression d'avoir essuyé les plâtres. Ce fut le cas avec les premières CN Safety. Leurs mi-

ses en place ont mis en exergue un manque de rigueur des fournisseurs et de maîtrise de cette technologie de la part des organismes de contrôle. Le groupe a même relevé des incohérences entre les paramètres CN et les Checksum montrant des différences entre le virtuel et le réel sur le terrain. Il a fallu limiter l'utilisation des certaines fonctions comme les accès de zone, car face à l'offre catalogues, le manque d'outils de diagnostic, de dimensionnement… s'est vite fait sentir.

LES RETOURS D'EXPÉRIENCE

Comme le précise Laurent Mauguy, *« ce retour d'expérience CN Safety nous a incité à la prudence avec les APIdS »*. Du coup, les premiers automates de sécurité ont passé des phases de tests dès 2002 et un îlot robotisé en 2004 à Poissy. Le retour d'expérience fut plus positif avec une simplification des blocs Sécurité validés et l'utilisation de blocs standardisés, ce qui n'était pas le cas avec les CN Safety dont les fonctions Safety n'étaient pas standards.

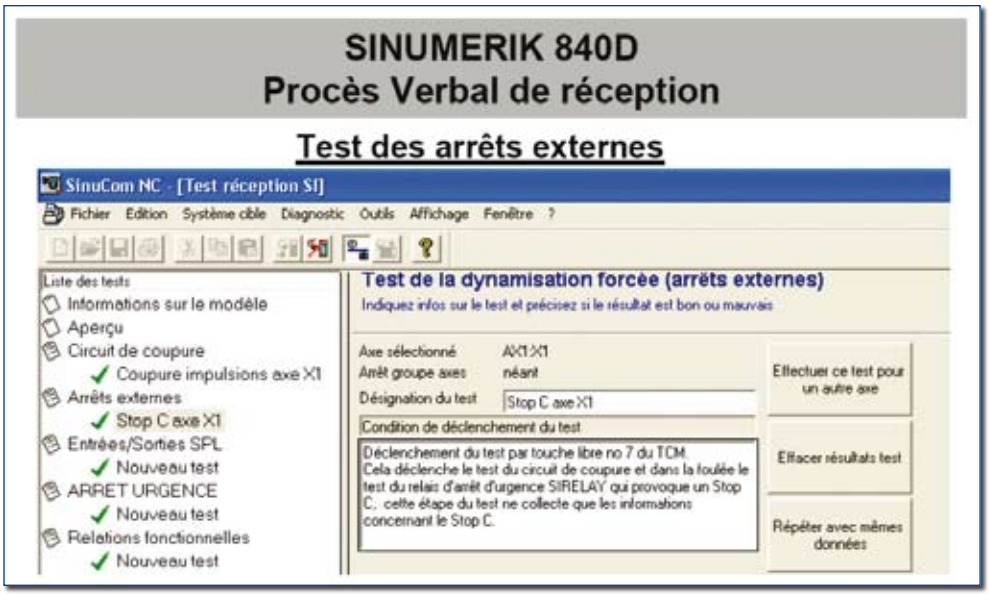
Seulement les fournisseurs ont encore une connaissance limitée de la réglementation, des normes… et les dossiers sécurité s'en trouvent incomplets avec des absences de validation. *« On a parfois l'impression que les offreurs, et les organismes, découvrent la technologie en même temps que nous, ce qui rend le travail difficile »*. Aujourd'hui, ce sont une centaine d'automates de sécurité qui sont implantés dans le groupe français, dont trois lignes de presses d'emboutissage mises en œuvre en 2006 et 2007, auxquelles se sont rajoutés trois projets de ferrage en 2007 et 2008, et plusieurs projets sont en cours pour 2009.

Encore aujourd'hui, le groupe PSA utilise une méthodologie stricte, et doit encore accompagner ses fournisseurs, d'ailleurs il en vérifie la compétence en termes techniques et de programmation, de réglementation en vigueur, de rédaction du dossier de sécurité. Pour réussir, il faut mettre en place un chef de projet, un programmeur ayant une culture

réglementation, un contrôleur pour la validation des diverses phases. Un moyen de suivre ensuite l'installation au cours de sa « vie série » avec dans ce dernier cas, l'intervention sur des programmes sécurité uniquement par des personnes habilitées, avec validation par tierce personne, et mise à jour des divers dossiers.

Reste maintenant à intégrer la nouvelle tendance, les fonctions Safety pour les robots. Si les avantages paraissent évidents, PSA ne tient à pas à revivre les difficultés connues avec les CN Safety, surtout que la robotique a une place importante sur les lignes, et qu'aucun risque ne doit être pris. Laurent Mauguy raconte même l'anecdote avec un capteur de sécurité testé hors production utilisant la vision et destiné à la sécurité d'un îlot robotisé : *« Pendant un mois, l'installation a fonctionné sans problème en plein hiver, seulement un jour le soleil s'est mis à briller différemment et le robot s'est arrêté. Imaginez l'impact sur une ligne de production avec 2 ou 300 robots »*.

Les premiers tests portent sur les cames électroniques qui sur l'axe 1 ont tendance à vouloir remplacer les cames mécaniques. Une simplification qui prendra toute son importance lorsque tous les axes pourront fonctionner sur un modèle similaire uniquement avec des cames électroniques. Seulement pour y parvenir, il faudra développer des outils de vérification qui n'existent pas encore, et que donnera l'ensemble d'une installation lors de déplacements de l'installation, en « vie série » ? Pour l'instant aucun outil pour contrôler l'enveloppe robot n'existe ? Comment fixer les limites ? Et dans le cas de la robotique, restera une dernière donnée, non technique, c'est l'acceptation du personnel à ces solutions sans barrière.



Exemple PV de réception CN Safety. Ils doivent être fournis par les constructeurs, adaptés à chaque évolution des fonctions Safety.

Dans l'avenir, une autre question se pose, celle des compatibilités des versions logicielles et leurs impacts sur les fonctions de sécurité. Par exemple, sur l'une de ses installations PSA a dû recharger le programme robot après deux ans de service, le système lui a alors demandé un mot de passe, impossible à trouver immédiatement, car édité nulle part et qui n'avait pas été correctement archivé. Des constats qui poussent le groupe à prévoir dès le départ des marches dégradées dans l'analyse des risques afin de ne pas être totalement bloqué sur une ligne en raison de la défaillance d'une fonction Safety programmée. *« Pour nos automaticiens, c'est une évolution importante, comparable à celle où nous sommes passés du relayage aux automates, les fonctions de sécurité programmées vont se généraliser et nous amener à développer, puis à maintenir, une nouvelle culture technique « Safety » sur les différents sites »* conclut Laurent Manguy.

STATION DE GAZ

Le sujet est explosif, pensez c'est le site de Gaz de Laneuvelotte qui a demandé à Clemessy d'étendre la puissance de compression du gaz de 24 MW à 48 MW, avec en parallèle une extension et une mise à niveau du système de contrôle de commande et des automates de sécurité existants.

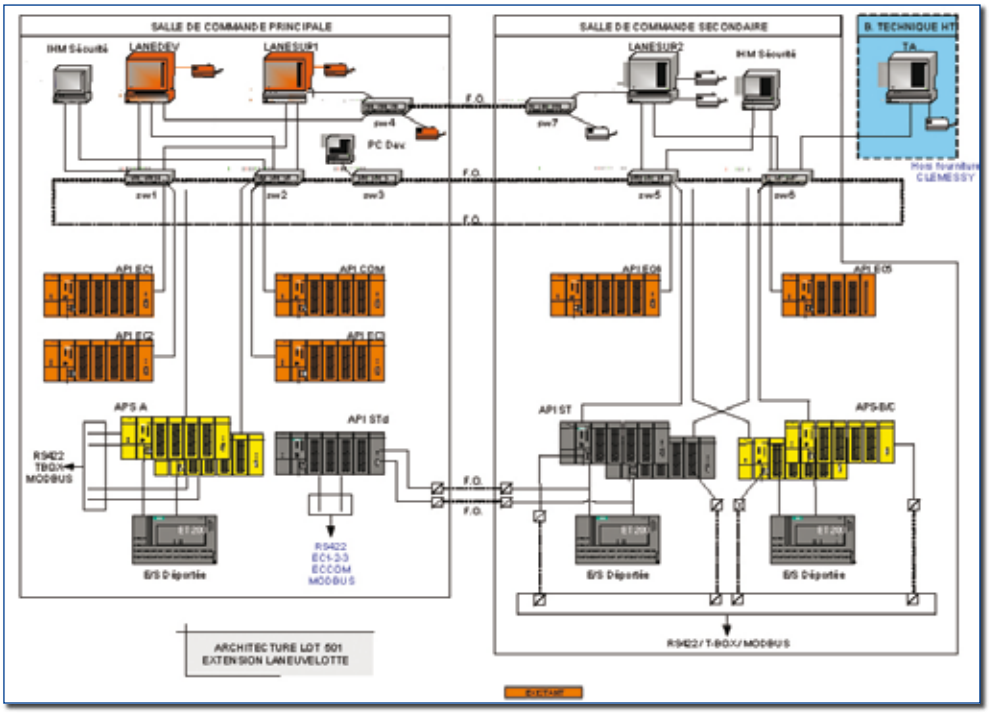
Le client réclamait à Clemessy un niveau de sécurité SIL 2 pour toutes les fonctions, avec un impératif de réaliser une simulation en plate-forme des automatismes pour valider toutes les fonctions de sécurité.

L'intégrateur/concepteur s'est retrouvé à la tête d'automates redondants à installer, mais également à intégrer des automates existants déjà sur le site. Et si les choix de l'architecture et des automates n'a pas posé en soi de problèmes, il en a été autrement pour les paramètres de sécurité, les actionneurs (principalement les vannes gaz) ou certains capteurs qui ne faisaient pas partie de la zone d'influence de Clemessy. Pourtant, ce dernier devait remplir l'objectif initial d'un SIL2 pour toutes les fonctions de sécurité de l'installation.

Pour le choix des automates de sécurité, c'est la simplicité pour le programmeur qui a prévalu avec la volonté d'avoir à écrire le minimum de lignes de codes. Les difficultés sont intervenues par la suite pour déterminer les niveaux SIL des équipements, si pour les automates ou les transmetteurs ces informations ont été rapidement disponibles, il n'en fut pas de même pour les vannes et encore moins pour les boutons-poussoirs ou les relais d'urgence. Même si dans ce dernier cas, il existe bien des relais dénommés « Safety Relays » mais sans rapport avec la certification SIL.

Le plus difficile, fut le manque de compétences en interne pour réaliser les calculs PFD. *« Nous avons des informaticiens, des automaticiens… mais pour interpréter les normes c'est une autre histoire »* confie Carlos da Silva, responsable BE Automatismes, chez Clemessy. C'est en contactant la société ISO Ingénierie que Clemessy a trouvé l'aide réclamée.

Cette application fut une première pour Clemessy, suivie par trois autres ayant le même objectif de recherche de sécurité. Un début d'expérience encore trop rare dans le monde industriel, d'ailleurs les participants à la journée du Club Automation se demandaient bien comment les organismes de vérification pouvaient faire pour valider les solutions, leurs compétences en la matière étant également neuves. Les retours d'expérience manquent encore, et sans nul doute le « Marronnier » reviendra rapidement avec d'autres journées sur la sécurité.



Station de compression de gaz de Laneuvelotte.