ISA France Section

ISA Flash

Setting the Standard for Automation™

ISA FLASH N°60 – Avril 2016 **Bulletin d'information d'ISA-France**

Au sommaire de ce numéro :

Atelier « Automatisation des transports ferroviaires urbains » du 16 mars 2016

L'atelier du 16 mars 2016 consacré à l'automatisation des transports ferroviaires urbains a connu à un très beau succès. La modernisation des transports est devenue une nécessité dans toutes les grandes agglomérations. L'Atelier du 16 mars 2016 a permis de faire le point sur l'état de l'art en matière d'automatisation et a suscité un débat animé après les trois interventions inscrites au programme :

- Le ferroviaire urbain, quelques concepts essentiels – Patrice Noury (ISA-France)
- Les derniers développements en matière de CBTC – Paul-Edouard Basse – Siemens
- Le concept de véhicules/trains autonome – Jacques Poré - Alstom

Si vous n'avez pas pu participer à ce séminaire, les présentations sont disponibles en accès libre

Une date à retenir : le 18 octobre 2016 à Villeurbanne – « Sûreté et cybersécurité »

A la suite du séminaire de Villeurbanne du 20 octobre 2015 et pour épondre à la demande de nombreux particpants, ISA-France organise avec l'INSA de Lyon (mastère Sécurité informatique) une journée d'études consacrée au thème « Sûreté et cybersécurité ».

Les deux disciplines « cybersécurité industrielle et sûreté de fonctionnement » sont amenées à se côtoyer. La philosophie générale qui les anime est la même : **identifier et analyser les risques et les ramener à un niveau acceptable.**

Mais si les deux concepts partagent un certain nombre de points communs fondamentaux, d'importantes différences existent : origines des dysfonctionnements de nature différente, conséquences identiques ou spécifiques, mesures de protection convergentes ou divergentes. De plus, les méthodes, les référentiels normatifs, les compétences sont aujourd'hui distinctes. **Un rapprochement entre les deux disciplines est nécessaire. Jusqu'où ira-t-il et comment s'y préparer ?**

Le séminaire vise à analyser la problématique des deux approches, de façon à faire comprendre ce qui les unit et ce qui les différencie.

Appel à communication en cours – Ouverture des inscriptions : mai 2016

En partenariat avec

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

ANSYS ESTEREL Technologies

HIMA SAFETY NONSTOP

SOGETI High Tech

Le 8 juin 2016 à 11h00 : Assemblée générale d'ISA-France

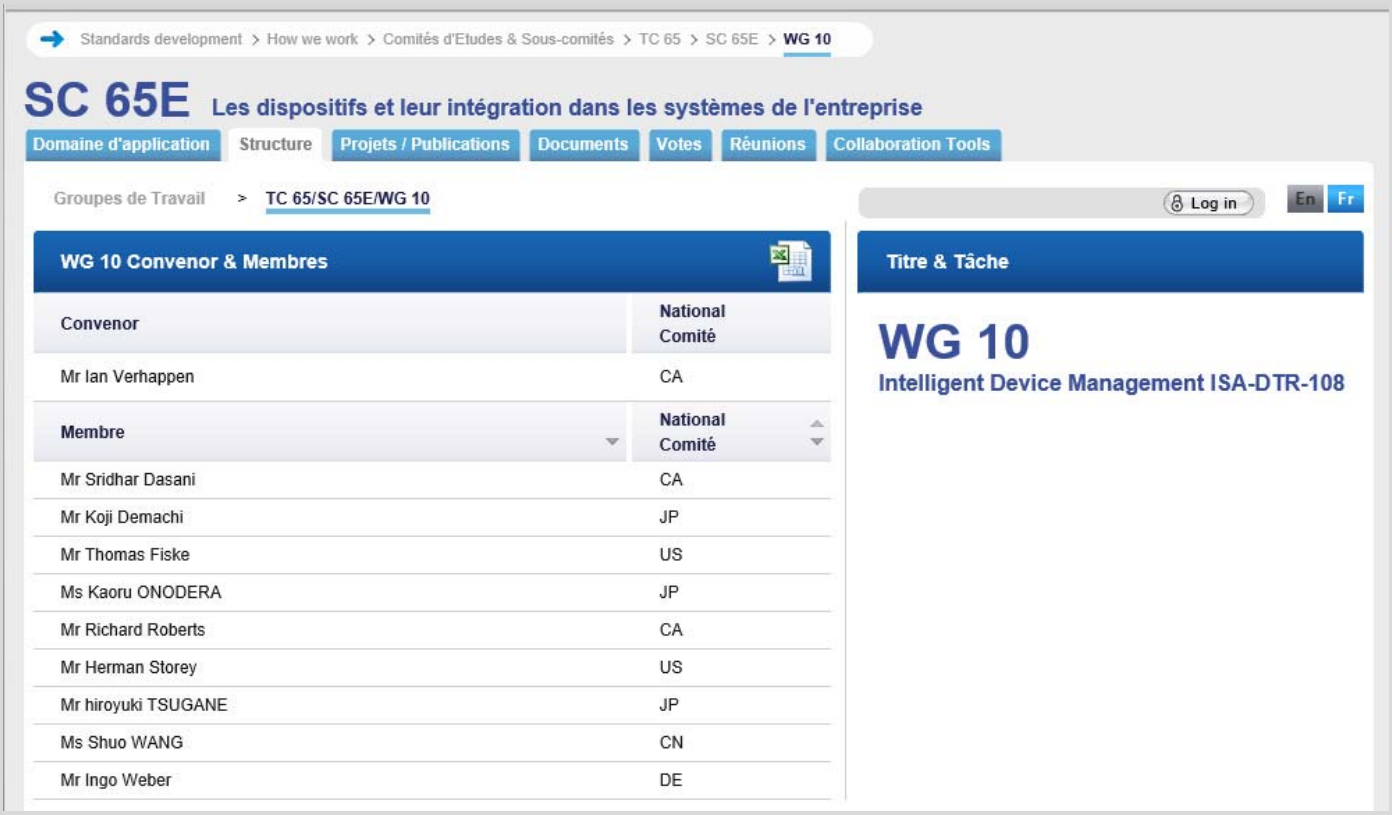
L'Assemblée générale ordinaire d'ISA-France se tiendra le mercredi 8 juin à 11h00 aux Ateliers du Bac – 69 rue du Bac 75007 Paris
Tous les membres d'ISA-France sont invités à y participer. Une occasion de rencontre et d'échanges sur les thèmes d'actualité en rapport avec le mode de l'instrumentation et des automatismes.

ISA-108 (Intelligent Device Management) : la reconnaissance par l'IEC est engagée

Depuis sa création en septembre 2012, le groupe de travail ISA108 s'est montré très actif.
La partie 1 du futur standard ISA108, référencée **ISA-TR108.1-2015 « Concepts and Terminology »,** présente les connaissances générales de base pour mettre en œuvre des systèmes composés de dispositifs intelligents. Les dispositifs intelligents sont des équipements qui disposent en plus de leur fonction de base d'un port de communication numérique pour piloter le périphérique et de fonctions supplémentaires permettant le diagnostic du dispositif lui-même et de l'équipement connexe.

Le document ISA-DTR-108 proposé au comité technique TC65 de la CEI (Mesure, commande et automation dans les processus industriels) a été soumis au vote et accepté par les comités nationaux.

Le groupe de travail WG10 (Intelligent Device Management ISA-DTR-108) a été formé dans le comité SC65E (Les dispositifs et leur intégration dans les systèmes de l'entreprise) et la transformation du standard ISA-108 en un document normatif international est ainsi engagée.



Deux autres parties sont en cours d'élaboration au sein du comité ISA 108, la partie 2 « Spécification des processus de travail » et la partie 3 « Guides d'utilisation » sont en cours d'élaboration au sein du comité ISA108 et seront proposées plus tard à la CEI.

Les dix erreurs du MES à éviter… (deuxième partie)

Le sigle MES (Manufacturing Execution System) s'applique de façon générale à l'informatique de support aux opérations industrielles. La transformation de plus en plus rapide des systèmes industriels nécessite une bonne prise en charge de la dimension informationnelle. Cet article de Jean Vieille, publié en deux parties, expose quelques-unes des difficultés auxquelles sont confrontés les industriels pour appliquer les technologies de l'information aux systèmes physiques dans une perspective d'optimisation systémique.

Nous publions dans cet ISA-Flash la deuxième partie de l'article dont la première partie a été publiée dans l'ISA Flash N°59.

Jean Vieille est expert en contrôle des systèmes industriels. Il est vice-président de l'ISA-France.

5. Implication interne insuffisante

L'industriel délègue souvent la mise en œuvre informatique à des prestataires spécialisés et cherche à minimiser l'intensité de son implication en tant que donneur d'ordres soit en restreignant ses responsabilités et son activité dans la réalisation du projet, soit en s'entourant d'une AMOA (assistance à maîtrise d'ouvrage) externe. Cette approche l'expose au risque d'être dépossédé de son système de transformation qu'il confie à une entité externe non concernée en premier chef par le devenir de l'entreprise.

Or, la transformation (gestion et contrôle de l'évolution de l'entreprise) est précisément l'activité qui assure la survie, le développement de l'intelligence et en filigrane de la performance. L'informatique, en particulier « industrielle » c'est-à-dire liée à l'objet même de l'existence de l'entreprise est un élément essentiel de cette transformation permanente.

L'allocation des moyens internes nécessaires pour un projet informatique représente un défi pour l'entreprise en mettant à contribution des acteurs qui devront partager leur temps avec leur activité opérationnelle.

Le second point (périmètre du projet trop large) n'offre guère d'autre solution que de constituer une équipe interne ad hoc dédiée au projet. Une telle structure éphémère traite la transformation comme une activité exceptionnelle sans lendemain alors qu'elle devrait être un processus structurel.

L'entreprise doit impérativement garder la maîtrise maitrise de la dimension informationnelle de sa transformation et donc

dédier des ressources à cet effet. L'ampleur de ces ressources devra être en rapport avec la dynamique de transformation souhaitée et adaptée à la taille maximale des projets.

6. Approche projet et intégration des prestataires insuffisante

La gestion de projet tend à circonscrire les rôles et les prestations au cadre du projet. Lorsqu'un intégrateur est sollicité pour le contexte exclusif du projet sans espoir de collaboration à long terme, il doit considérer son seul intérêt immédiat dans ce contexte. Il est alors nécessaire d'établir des spécifications très précises, chaque modification/ajout fera l'objet d'avenants pris en compte pour le seul bilan du projet (compromis coût – qualité). Le bon gestionnaire de projet refusera la plupart de ces aménagements pour s'en tenir au cahier des charges initial. Un second projet traitera des problèmes non résolus ou soulevés par le premier. Il en résulte une insatisfaction des utilisateurs, une mauvaise adéquation au besoin et très souvent un échec du projet, que ce soit sur le plan qualitatif (gestion de projet rigoureuse) financière (avenants) ou délais (contractualisation des évolutions).

Cette rigidité affecte directement la performance de transformation. Combinée avec l'erreur précédente elle aggrave la perte de la connaissance et donc de la maitrise même de cette transformation, aux conséquences létales.

Considérant l'importance de la transformation informatique, l'entreprise devra soit installer une cellule informatique industrielle conséquente en charge du pilotage de la stratégie et de la réponse aux besoins, de la conception au déploiement, soit établir un contrat de partenariat à long terme avec un fournisseur/intégrateur qui fera de cette société une entité support de l'entreprise. Cette cellule ou ce partenaire traitera tous les ajustements et développements évolutifs sur la plate-forme technologique en place, et interviendra en supervision des projets plus importants.

7. Incohérence de la conception informatique avec l'organisation

La planification et l'exécution doivent interagir de manière appropriée selon les options organisationnelles qui fixent par

exemple le degré de liberté du domaine opérationnel vis-à-vis des directives de la planification. Il en est de même pour le partage des tâches et responsabilités des activités de conception produit/industrialisation, maintenance, logistiques et qualité. La conception informatique doit les respecter en ajustant les accès et la profondeur de visibilité aux utilisateurs que ce soit à travers l'urbanisation des applications calquée sur les domaines de responsabilité ou de manière plus fine et flexible par une approche SOA (Service Oriented Architecture) d'abstraction applicative des fonctions.

La réflexion systémique, l'optimisation organisationnelle, l'ajustement informationnel correspondant et la coordination générale des développements informatiques sont souvent absents de la cartographie des applications dont l'empreinte fonctionnelle découle davantage de leur potentialité et de la précédence des projets, que d'une programmation consciente. Par exemple :

- la gestion des stocks ricoche entre ERP et MES, sa consolidation est laborieuse ;
- les ordres et réponses de fabrication portent nombre d'informations redondantes ou inutiles en s'attachant à une granularité et un niveau de détail inadaptés ;
- l'évolution et l'introduction de nouveaux produits sont difficiles en imposant une élaboration et propagation complexes des données techniques ;
- la gestion de la performance est entraînée dans des dérives dommageables, comme le suivi dans l'ERP des temps d'arrêt des machines perçu comme « flicage » inutile au lieu de l'efficience des équipements justifié pour la planification capacitaire.

Les projets sont finalement plus difficiles à réaliser, avec des options de mise en œuvre réduites tandis que les utilisateurs souffrent d'une situation détériorée et de contraintes résultant de la distorsion de l'informatique avec l'organisation.

8. Négliger l'interopérabilité

Les logiciels intégrés d'entreprise comme les ERPs facilitent le développement des applications autour d'une base de données unique. Les logiciels MES créent un espace linguistique à part tout en restant lié de manière très étroite aux autres applications (ERPs, maintenance, qualité, ingénierie, développement) par les ressources et les flux d'activités.

Les interfaces des applications d'un projet avec les applications existantes sont souvent laissées à l'appréciation et à l'expertise de l'intégrateur. La relégation des interfaces au rang de trivialités à traiter de manière ad hoc par les informaticiens n'est pas toujours une cause immédiate de l'échec, mais inocule les germes d'un cancer. A court terme, le maintien de la cohérence des référentiels (produits, matières, équipements) devient vite un cauchemar. Plus tard, l'évolution applicative et handicapée par le codage purement technique des canaux de communication.

Ce point découle du précédent. L'interopérabilité est liée directement au couplage systémique dans l'organisation industrielle et à la cartographie applicative. Il est indispensable d'encadrer la notion technique d'interface par celle linguistique d'interopérabilité prenant en compte le sens de l'information sur la base d'un langage d'entreprise cohérent avec le modèle d'architecture qui guide la transformation industrielle. Elle implique la gestion d'une taxonomie des concepts et des données de référence.

9. Ouvrir un champ de bataille IT/ingénierie

Le domaine fonctionnel MES empiète sur celui de l'ERP ; il est normal que l'ERP ou le MES soit en compétition sur la réalisation de certaines fonctions. La justification du MES réside moins dans la couverture fonctionnelle que dans la fourniture d'un outil plus adapté à l'exploitant qu'au gestionnaire, apte à gérer un niveau de détail indispensable dans l'atelier, inutile voire nuisible pour les acheteurs, vendeurs et stratégistes de l'entreprise, à absorber la complexité opérationnelle pour rendre possible son pilotage et son contrôle au sein de l'entreprise.

La nécessité de maitriser la complexité de l'entreprise aboutit à des schémas d'organisation où l'informatique industrielle s'insère de différentes manières, aboutissant souvent à l'attribution du domaine MES à une entité différente de celui de l'ERP, aboutissant à un positionnement concurrentiel sur les projets lorsque les responsabilités ou les règles d'allocation ne sont pas clairement établies.

Auxiliaire du système de production, service autonome à l'échelle de l'entreprise, extension de l'informatique d'entreprise, de l'ingénierie ou structure mixte, il peut être nécessaire de repenser le modèle organisationnel de l'informatique industrielle pour prévenir des conflits inutiles. On peut chercher à optimiser le service informationnel en découplant l'aspect plateforme centralisée (offrir des services de développement et de déploiement) et l'aspect service et réalisation localisé sous la responsabilité de l'unité de fabrication s'appuyant sur les ressources offertes jugées sur le contrat de service et l'adéquation fonctionnelle sans exclure le prototypage Excel...

10. Budget inadapté

On entend parfois que le retour sur investissement d'un projet MES n'est pas plus chiffrable que celui d'un ERP, il faut donc convaincre la direction qu'il est indispensable. D'autres prétendent chiffrer des économies de main d'œuvre alors que personne ne sera licencié à l'issue du projet – au contraire ! D'autres décomptent les bouts de chandelles liés à une amélioration présumée de la productivité, alors que l'usine est sur-capacitaire. Dans la plupart des cas, le business case est fragile. A moins de parvenir à susciter l'enthousiasme, le projet ne se décide qu'à la condition d'une dépense minimale faute d'une valorisation crédible du potentiel économique. Un budget insuffisant aboutissant à une solution insatisfaisante, la preuve est faite du bien-fondé de la méfiance managériale. Cette difficulté budgétaire entraine donc deux types d'échec : abandon du projet et projet raté.

Le soin apporté à l'évaluation de l'impact économique est déterminant pour définir le budget et les livrables du projet soutenant une projection crédible pour la direction. Une telle évaluation devrait porter sur différents horizons temporels, sur le plan purement économique ainsi que sous l'angle de la survie et du développement moyen-long terme, et ceci en impliquant de manière contradictoire les acteurs concernés. Cette évaluation peut être conduite pour un projet, mais elle est plus facilement et utilement déterminée globalement pour l'activité permanente de transformation informatique : un budget multi-annuel (afin de pouvoir absorber les pics de transformation) calibré en conséquence serait utilisable aussi bien pour les ajustements continus que pour les projets plus importants à la discrétion du responsable de l'informatique industrielle. Le contrôle est simplifié, permettant une plus grande réactivité de la transformation qui n'aurait pas à justifier par exemple de ses décisions technologiques incompréhensibles par la direction.

En conclusion

L'informatique industrielle apparait comme un domaine sensible pour trois raisons principales :

- elle croise des domaines fonctionnels de l'entreprise dont les interactions ne sont pas toujours bien formalisées, sans sponsor naturel capable de diriger l'alignement technologique et fonctionnel sur une organisation systémique cohérente ;
- la rencontre des processus de gestion triviaux et stables avec des processus physiques très technique en développement permanent représente un défi pour la mise en œuvre qui doit rationaliser une connaissance propre à l'industriel difficilement décrite dans des cahiers des charges ;
- la dynamique de transformation informatique doit accompagner celle du système industriel au cœur de la raison d'être de l'entreprise. Elle nécessite d'encadrer les projets dans un processus structurel doté des moyens nécessaires.

Cet inventaire est loin d'être exhaustif. Les difficultés humaines (résistance au changement) et programmatiques (changement de stratégie et de contexte en cours de projet) n'ont pas été citées en entrées parce qu'elles ne sont que la conséquence des points mentionnés.

Le plus important est sans doute la prise de conscience de l'importance et du couplage intime de la dimension informationnelle dans le système industriel. Cet état d'esprit guidera naturellement l'industriel vers des choix pragmatiques et cohérents faces aux modes et argumentaires commerciaux pour tirer profit d'une technologie disponible sans perdre de vue son caractère utilitaire au service de la transformation industrielle.

Jean-Vieille - j.vieille@syntropicfactory.com

L'industrie du futur

Mis en place en 2015, le plan gouvernemental initialement appelé Usines du Futur puis rebaptisé **Industrie du futur** a pour ambition d'améliorer la performance globale du système industriel des entreprises françaises en transformant les usines pour les rendre plus "intelligentes et flexibles".

Ce projet vise à amener chaque entreprise à franchir un pas sur la voie de la modernisation de l'outil de production et à réussir sa transition numérique. Il couvre l'ensemble des activités de l'entreprise, de la conception du produit jusqu'au service après-vente, en passant par la production et la logistique. il s'agit d'accompagner les entreprises, dans un monde où les outils numériques font tomber la cloison entre industrie et services.

Christian Verney *fait ici le point sur cette initiative.*

1. Les cinq axes de la feuille de route de l' « Usine du Futur »

- **une usine intelligente,** avec des modes de production sophistiqués qui repensent l'interface et la collaboration homme-machine, et replace les femmes et les hommes au cœur de l'activité.
- **une usine connectée plus intégrée et pilotée**, connectée au cœur des territoires et proche de ses parties prenantes (clients, sous-traitants et fournisseurs); l'usine de demain contribuera à dynamiser un réseau et une économie locale.
- **une usine numérique plus moderne et plus flexible** pour faire face et pour rester compétitive. Au sein de l'usine, la connexion des machines est une révolution en route pour optimiser les paramètres de production. Ces outils numériques permettent à l'usine d'être de plus en plus flexible.
- **une usine plus humaine** qui doit remettre l'humain au cœur de la relation homme-machine. « Il faut remettre l'industrie au cœur de notre économie, et l'Homme au cœur de l'industrie. » telles sont les paroles d'Emmanuel Macron. L'homme est donc au centre du débat.
- **une usine verte,** plus respectueuse de son environnement, grâce à des modes de production moins consommateurs de ressources et moins générateurs de rejets.

Pour assurer la pérennité du plan Industrie du futur, une association loi de 1901 a été créée « L'alliance pour l'industrie du futur" qui capitalise sur les acquis du plan Usine du Futur, pour sa mise en œuvre opérationnelle.

Afin de toucher toutes les entreprises, l'Alliance, coprésidée par Fives, et Dassault systèmes, implique les fédérations professionnelles de l'industrie et du numérique, et des partenaires technologiques et académiques.

En juillet 2016, Philippe Darmayan, président d'ArcelorMittal en France, du Groupe des fédérations industrielles et membre du bureau du Conseil national de l'industrie, a été nommé président opérationnel du comité de pilotage.

2. Le projet « Industrie du futur » repose sur cinq piliers

Pour atteindre ces objectifs et accompagner cet effort sans précédent le projet « Industrie du futur » repose sur cinq piliers :

- **développer l'offre technologique** : cela passe par le renforcement de la recherche dans des domaines clefs. Des projets structurants de R&D financés par l'État sont retenus, ils concernent l'impression 3D, le contrôle non-destructif, la plateforme robotique Industrielle, la virtualisation de l'usine et l'Internet des objets, les matériaux composites et la place de l'homme dans l'usine.
- **accompagner les entreprises dans cette transformation :** pour accompagner les PME et ETI, des diagnostics industriels sont proposés ainsi que des mesures exceptionnelles de soutien financier aux entreprises qui investiront dans la modernisation de leurs capacités de production.
- **former les salariés :** la formation axée sur la présence accrue du numérique et de la robotisation dans l'usine, sont proposées aux jeunes générations. Il convient également de s'assurer que les cursus de formation initiale prennent bien en compte l'évolution des technologies. Les travaux sur la formation et la place de l'homme seront suivis par l'UIMM accompagné par les grandes écoles. La montée en compétence des salariés de l'industrie et la formation de nos jeunes constituent en effet un enjeu crucial et central.
- **renforcer la coopération internationale sur les normes :** un groupe de travail porte la voix des industriels français dans les plus hautes instances de normalisation internationale. Il s'agit de ne plus subir les décisions d'un système dans lesquels les Allemands sont très actifs (la normalisation était au cœur du programme Industry 4.0 lancé Outre-Rhin en 2010).

  Sur le plan européen, l'Alliance pour l'Industrie du Futur représente les intérêts français au sein des initiatives européennes dans le domaine du « smart manufacturing » et de la numérisation de l'industrie. Elle offre un appui aux entreprises françaises pour leurs candidatures aux appels à projets européens « Horizon 2020 » et permet de mieux peser dans le domaine des normes européennes qui faciliteront le déploiement de l'offre technologique Industrie du futur.

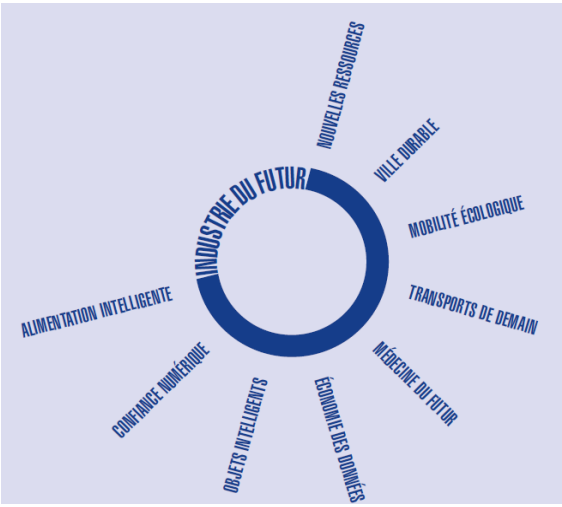
Les travaux de normalisation sont suivis principalement par la FIM et le Gimélec. Une publication de la stratégie française de normalisation pour l'Industrie du futur est prévue pour 2016.

Le projet Industrie du futur a vocation à nouer des partenariats stratégiques au niveau international que ce soit avec le Smart-Manufacturing aux Etats-Unis, mais surtout au niveau européen et en particulier avec l'Allemagne et sa plateforme « Industrie 4.0 ». Cette coopération s'incarne dans des projets communs, des projets pilotes ou de développements technologiques, qui seront présentés dans le cadre du plan d'investissement européen.

- **Promouvoir l'Industrie du futur française :** en créant d'ici la fin de l'année 2016 une quinzaine de vitrines technologiques de visibilité nationale voire européenne, (des projets emblématiques réalisés dans les grands groupes et pouvant faire office de démonstrateurs). Avec les opportunités offertes par le numérique, il ne s'agit plus seulement d'avoir le meilleur produit ou le meilleur service pour gagner des parts de marché. Il faut désormais proposer des solutions qui regroupent les produits et les services et apportent ainsi des réponses concrètes et cohérentes aux grands défis d'avenir. Un grand salon de l'Industrie du futur aura lieu à Paris fin 2016.

3. Développer des solutions industrielles françaises pour neuf marchés prioritaires

Un appel à projets est lancé et s'adresse à des consortiums de plusieurs partenaires. Les projets doivent avoir des retombées industrielles à court-moyen terme. La durée d'un projet est typiquement de 24 à 36 mois, pour un investissement total de l'ordre de 5 à 10 M€. Afin d'adresser plus directement les besoins et les marchés et piloter plus efficacement le dispositif des solutions industrielles seront développées pour neuf marchés prioritaires.



1. **Nouvelles ressources :** de nouveaux matériaux biosourcés et recyclés pour toutes les industries

Il s'agit de produire autrement en utilisant nos ressources de façon plus optimale, en misant sur le recyclage des produits et des matières, ainsi que sur l'efficacité des modes de production.

Pour cela, il faut permettre l'éclosion de nouvelles solutions pour de nouveaux modes de production plus propres, plus économes en matière et moins consommateurs d'énergie. Parmi les idées retenues :

- l'utilisation des ressources végétales, en lieu et place des énergies fossiles, et le développement de la chimie verte et la production de biocarburants avancés ;
- le déploiement des installations industrielles capables de collecter, trier et recycler de nouveaux matériaux.

2. **Ville durable :** la ville économe de ses ressources, du producteur au consommateur.

Il faut relever le défi et proposer des solutions pour développer des produits et des services qui rendront nos villes plus durables par exemple :

- développer une gestion plus intelligente des réseaux d'eau et d'énergie (smart grids) ;
- améliorer la performance énergétique des bâtiments et l'implication des consommateurs finaux ;
- augmenter la productivité, la qualité et la durabilité du secteur de la construction, notamment en privilégiant les matériaux biosourcés.

3. **Mobilité écologique :** une mobilité moins chère, plus libre, plus respectueuse de l'environnement et plus sûre au quotidien**.**

Il faut changer nos manières de nous déplacer, pour les rendre plus écologiques, moins coûteuses et moins subies. Pour répondre à ce besoin, nos véhicules doivent devenir plus économes, plus connectés et plus autonomes.

La solution passe par :

- le véhicule électrique ;
- le développement des transports collectifs ;
- une sécurité renforcée.

4. **Transports de demain :** Un transport des personnes et des marchandises plus écologique et plus compétitif.

Les industries des transports sont un domaine d'excellence industrielle historique de la France. Il est nécessaire de :

- réinventer les modes de transports et proposer des solutions innovantes alliant efficacité écologique et compétitivité économique ;
- répondre aux enjeux d'efficacité énergétique (-50 % de consommation pour le TGV du futur et pour le navire de demain).

- proposer des solutions pour une plus grande électrification des technologies et un stockage plus performant de l'énergie.

5. **Alimentation intelligente:** une alimentation sûre, saine, durable et exportable.

Les modes de consommation sont chaque jour plus sophistiqués ; l'exigence de sécurité sanitaire est de plus en plus forte; la volatilité du cours des matières premières impose une meilleure productivité de la filière agroalimentaire.

Pour innover et atteindre ces objectifs il est impératif de :

- proposer des solutions industrielles pour reconquérir la compétitivité des métiers de la viande, ouvrir le marché de l'alimentation fonctionnelle, s'imposer dans les emballages du futur, prendre le leadership du froid durable, et garantir la qualité et la sécurité des aliments et des boissons ;
- permettre à la filière de se saisir des opportunités offertes par l'intégration des outils numériques ;
- développer une industrie de référence au niveau mondial dans les domaines d'avenir où la France dispose d'une recherche d'excellence, tels que les ferments et les protéines

6. **Économie des données :** une meilleure gestion et valorisation des données dans les entreprises et dans les services publics.

Bien qualifiées, ordonnées, sécurisées, les données de l'entreprise révèlent de nouveaux gisements de valeur ajoutée. Il est nécessaire pour cela de :

- soutenir et accompagner la maîtrise des technologies de base pour permettre aux acteurs publics et privés de s'approprier le calcul intensif, le cloud et le Big Data ;
- développer une offre innovante dans le domaine du Big Data ;
- mettre en place un environnement adapté : création ou renforcement des formations, mise en place d'un label sur la sécurité des données stockées ;
- adapter le cadre réglementaire pour faciliter l'accès et l'exploitation des données dans le respect des libertés individuelles.

7. **Objets intelligents :** L'internet des objets pour améliorer le quotidien.

Un objet connecté apporte un service à valeur ajoutée allant au-delà de sa fonction il peut prendre une décision ou alerter l'utilisateur. Son intérêt réside notamment dans la manière dont sont exploitées les données. Pour répondre au challenge, il faut:

- créer de nouveaux objets qui améliorent notre quotidien dans des champs divers, comme la santé, les transports, les paiements ou la culture ;
- accélérer les cycles d'innovation pour faciliter la conception et la production d'objets innovants, par la mise en place de moyens mutualisés ;
- déployer des services innovants par de grands acteurs et par les collectivités : des services sans contact pour le paiement, les transports et autres services du quotidien ;
- valoriser l'offre française au travers d'événements mondiaux.

8. **Confiance numérique :** un environnement numérique de confiance protecteur des entreprises et des individus**.**

Le développement du numérique est un formidable relais de croissance pour notre économie mais ce développement suppose un degré élevé de sécurité des infrastructures et des services numériques. Cela implique de :

- intervenir à toutes les étapes de la chaîne numérique ;
- préserver notre souveraineté technologique pour des filières stratégiques (composants électroniques, satellites) ;
- développer des technologies qui se différencient par leurs performances (puces multi-cœurs, réseaux 5G), leur efficacité énergétique, leur sûreté de fonctionnement ;
- soutenir les PME et les startups ;
- sensibiliser les acteurs économiques aux problématiques de sécurité et de sûreté.

9. **Médecine du futur :** un parcours de soins plus performant grâce à l'innovation médicale et digitale.

Il faut soigner mieux et à moindre coût pour relever les grands enjeux, celui du vieillissement de la population, celui de l'accroissement des maladies chroniques, celui de l'innovation au service de la qualité de la prise en charge. Pour cela il convient de :

- concentrer les efforts d'investissement pour accélérer le développement d'une offre de niveau international de dispositifs médicaux, de thérapies innovantes et de séquençage haut-débit pour le diagnostic et la thérapie.
- accompagner au travers du CSF Santé la mise sur le marché des nouvelles biotechnologies médicales et des dispositifs médicaux innovants.

4. Industrie du futur : La normalisation est un élément essentiel

Une nouvelle guerre des standards est à éviter

Le consortium allemand Industry 4.0 a choisi le standard **OPC UA** comme norme de communication entre équipements dans son modèle d'usine du futur mais les industriels français lui préfèrent largement le protocole **Modbus TCP** (développé

par Schneider Electric). Cependant ce dernier ne peut gérer des modèles de données comme le fait OPC UA.

OPC UA (IEC 62541 série) est un protocole de communication universel et sécurisé, particulièrement adapté à la communication entre machines. Il peut être appliqué à tout type de support physique, de système d'exploitation et il peut être installé aussi bien sur une machine à forte capacité de calcul qu'à un petit objet connecté.

Les membres de l'Alliance devront décider s'ils souhaitent pousser à tout prix des technologies franco-françaises ou s'il est préférable de se conformer à ce qui est désormais considéré comme un standard dans plusieurs régions du globe. Le groupe Afnor pilote une enquête qui devrait déboucher, mi-février, sur un programme de normalisation pour bâtir une stratégie normative sur les "industries du futur"

D'autres standards internationaux s'imposeront plus naturellement

- les spécifications ISA88 - IEC 61512 Batch control (system model, process model) pour le batch control ;
- les spécifications Prolist - IEC 61987 Industrial-process measurement and control - Data structures and elements in process ;
- IEC 62264, "Enterprise-control system integration" (enterprise model, system model, function model) ;
- Les spécifications ISA 99 – IEC 62443 (Security in Automation) ;
- IEC 62714 Automation ML.

Christian Verney – verney.christian@orange.fr

Actualité : la cyberattaque contre les réseaux électriques ukrainiens du 23 décembre 2015

Le 23 décembre 2015, à partir de 15h30 environ, les opérateurs des centres de contrôle de trois distributeurs d'électricité de l'Ouest de l'Ukraine (dans l'oblast d'Ivano-Frankivsk notamment) perdent le contrôle du système électrique dont ils ont la charge. Sur leurs écrans de contrôle, une main invisible s'est emparée du curseur et ouvre un à un les disjoncteurs qui commandent le réseau. Les opérateurs essaient de reprendre le contrôle mais rien ne répond et la machine leur refuse l'accès. Ils tentent de se connecter à nouveau mais leurs mots de passe sont devenus inopérants.

En l'espace d'une demi-heure, une trentaine de sous-stations sont mises hors service et 225 000 foyers de l'Ouest ukrainien sont privés d'électricité. Les centres de contrôle eux-mêmes sont plongés dans le noir car les alimentations de secours (UPS) ne fonctionnent pas. Impossible de faire le point de la situation au téléphone car le réseau est saturé. Quatre-vingt-dix minutes après l'attaque une bombe logique active un logiciel malveillant qui détruit les logiciels implantés sur les stations de contrôle. Des agents sont envoyés sur le terrain et l'alimentation est rétablie manuellement en quelques heures mais deux mois après les évènements l'exploitation n'était pas encore redevenue normale.

Le scénario probable de l'attaque

Dès 17h37, la principale utilité touchée, Prykarpattya Oblenergo (http://www.oe.if.ua/), évoquait sur son site Internet l'hypothèse d'une ingérence extérieure et présentait ses excuses à ses clients. Par la suite les autorités ukrainiennes ont fait appel au FBI et au Department of Homeland Security américains pour analyser le déroulement de la cyberattaque.

Cette attaque semble avoir été conduite par deux équipes d'intervenants successifs :

- elle aurait été préparée par une équipe internationale de mercenaires du cybercrime, comme il en existe en Chine, aux Etats-Unis et en Russie, qui aurait conçu le scénario et mené à bien la phase préliminaire ;
- elle a été conduite le jour J par une équipe de professionnels des réseaux électriques capables d'opérer à distance un système de contrôle.

La phase préliminaire a consisté en une attaque banale en *spear-phishing* (harponnage) qui remonterait à mai 2015 et s'est traduite par l'envoi d'un grand nombre de courriels non sollicités vers les utilités ukrainiennes et d'ailleurs également vers d'autres infrastructures du pays. A ces courriels était joint un document Word contenant des macros qu'à l'ouverture le destinataire était invité à activer. Des informations disponibles publiquement sur Internet ont peut-être facilité l'attaque, un intégrateur ayant par exemple documenté (à des fins commerciales) la prestation pour l'un des opérateurs, avec la liste détaillée des matériels et versions mis en place, dont les passerelles Ethernet-série.

L'attaque a été fructueuse sur trois compagnies régionales d'électricité permettant à l'agresseur de pénétrer dans le système de gestion des entreprises. Il leur fallait alors descendre au niveau des SCADA (Supervisory Control and Data Acquisition) qui étaient tous différents et protégés par des pare-feu. Le passage ne s'est pas fait en force, en exploitant des failles éventuelles des équipements, mais après quelques mois en utilisant des accès légitimes : après reconnaissance approfondie des lieux et compromission des contrôleurs de domaine Windows, les attaquants ont eu accès aux clés et mots de passe protégeant les passerelles et les réseaux de commande à distance (VPN) vers les SCADA. Les logiciels de contrôle et les UPS ont été reconfigurés pour préparer l'attaque.

Le jour J, les attaquants ont eu accès aux SCADA via les VPN et les UPS ont été neutralisées. Les disjoncteurs ont été actionnés les uns après les autres sans que les opérateurs puissent s'y opposer. Puis le firmware des passerelles Ethernet-Série a été écrasé, les rendant non seulement inopérantes mais irrécupérables et contribuant à empêcher la reprise de contrôle. Les centres de contrôle ont été plongés dans l'obscurité du fait de la défaillance des UPS. Dans le même temps, une attaque en déni de service, sous forme d'une vague d'appels massifs provenant d'un pays voisin, a neutralisé le réseau téléphonique. Seul, le réseau Internet est resté en service permettant aux compagnies d'informer leurs usagers via leurs sites.

A la fin de l'attaque, le logiciel malveillant KillDisk, activé par une bombe logique, est venu effacer les logiciels installés dans les stations opérateurs, ainsi que des systèmes d'entrées-sorties déportées (RTU), ce qui a rendu plus difficile la restauration des réseaux.

Il est à noter que le logiciel malveillant Blackenergy3 utilisé à plusieurs reprises dans des campagnes précédentes touchant notamment l'Ukraine[1], semble avoir été utilisé comme trojan pour pénétrer par harponnage les systèmes et permettre l'installation d'une porte dérobée. La figure 1 reproduit un message utilisant Blackenergy qui semble provenir du Conseil suprême d'Ukraine, le Rada.

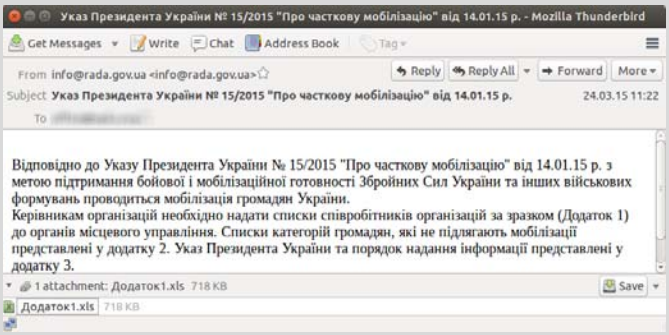


Figure 1 : Courriel semblant provenir du rada ukrainien et utilisé dans des attaques de spear-phishing fondées sur black energy – Source : CyS Centrum LLC.

Les enseignements à en tirer

Cette attaque très sophistiquée est la troisième connue conduisant à une défaillance majeure sur une installation industrielle, après l'attaque Stuxnet (juillet 2010) et celle dirigée en 2014 contre une usine métallurgique allemande. De nombreux enseignements seront à en tirer et le débriefing ne fait que commencer.

En premier lieu, une sensibilisation de tous les personnels aurait permis d'éviter de tomber dans le piège du harponnage. En second lieu il faut renforcer la protection des communications entre système de gestion et système de contrôle. L'IEC 62443 impose un contrôle d'identification basé sur deux facteurs mais d'autres solutions, telles que les data-diodes peuvent s'imposer. La procédure des "listes blanches" permet également d'éviter l'installation d'applications corrompues. Enfin des

1 Blackenergy est un logiciel malveillant dont les premières versions remontent à 2007. Il a été utilisé notamment dans les cyberattaques contre la Géorgie en 2008. Il a été perfectionné depuis et serait couramment utilisé par le gang russe Quedagh. Voir les informations diffusées par F-secure (Finlande) : https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

solutions de détection d'intrusion sur réseau industriel, permettant d'identifier les activités malveillantes, notamment durant les phases de découverte de réseau, pourront à l'avenir réduire le risque, mais sont aujourd'hui à un stade encore peu mature.

Il faut également revoir les sécurités des réseaux de communication à distance (VPN), comprendre pourquoi elles ont été franchies et bien entendu, revoir la sécurité des UPS, notamment leurs accès à distance pour la télémaintenance. L'ICS-CERT du DHS américain fournit une première liste de recommandations accessibles sur https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 .

Jean-Pierre Hauet jean-pierre@hauet.com

Deux nouveaux cours ISA-France en 2016

Dans son programme de formation 2016 (voir ci-dessous), ISA-France propose deux nouveaux cours adaptés aux préoccupations actuelles.

L'Internet industriel des objets - Les futures architectures de systèmes d'automatisme et de contrôle

L'Internet Industriel des objets fait partie du buzz technico-commercial actuel. Mais que signifie-t-il exactement ? Quels changements, voire quels bouleversements, entraînera-t-il dans les architectures d'automatisme et de contrôle ?

Le cours ISAF JPH4 (2 jours) permet de

- Comprendre l'enjeu de l'Internet industriel des objets (IIoT) dans l'usine du futur (Industrie 4.0) pour une meilleure efficacité et une meilleure productivité
- Comprendre les évolutions dans l'architecture des systèmes qu'implique la généralisation de l'approche IP, tant au niveau local qu'au niveau des grandes distances
- Se familiariser avec les principales briques technologiques qui sous-tendent l'IIoT et avec leur impact opérationnel :

Cours sur deux jours (Ref JPH4)

La transformation digitale des systèmes industriels

Industrie 4.0, Smart Manufacturing, Industrie du Futur… ces initiatives marketing ou politiques sont révélatrices du besoin d'évolution des entreprises industrielles et tout particulièrement de la mise à profit des technologies de l'information. Au-delà des modes, l'entreprise doit sans cesse s'adapter, se transformer pour répondre aux exigences de son environnement, rester en vie, améliorer ses performances. L'informatique industrielle (MES) est particulièrement concernée alors que sa complexité et la criticité de son rôle opérationnel rendent les projets de transformation difficiles et risqués.

Le processus de transformation permanente étudié dans ce cours vise à prévenir ces difficultés tout en améliorant l'alignement métier dans une perspective de performance globale incluant la responsabilité des allocations budgétaires.

Cours sur un jour (Ref JV17)

Code	Désignation	Calendrier 2016	
		Lieu	Date
JPH1	L'IEC 62734 (ISA-100) et les applications nouvelles des radiocommunications dans l'industrie - Deux jours	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	16 et 17 mai 2016 3 et 4 octobre 2016 28 et 29 novembre 2016
JPH3	La norme ISA/IEC 62443 (ISA-99) et la cybersécurité des systèmes de contrôle - Un jour	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	8 mai 2016 5 octobre 2016 30 novembre 2016
JPH4	L'Internet industriel des objets - Les futures architectures de systèmes d'automatisme et de contrôle	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	23 et 24 mai 2016 10 et 11 octobre 2016 5 et 6 décembre 2016

JVI1	ISA-88 : Conception fonctionnelle du contrôle des procédés industriels - Deux jours	Fontainebleau	23 et 24 mai 2016 3 et 4 octobre 2016 5 et 6 décembre 2016
JVI2	ISA-95 : Conception fonctionnelle et interopérabilité MES/MOM - Deux jours	Fontainebleau	25 et 26 mai 2016 5 et 6 octobre 2016 7 et 8 décembre 2016
JVI7	Transformation digitale des systèmes industriels – Un jour	Fontainebleau	27 mai 2016 7 octobre 2016 9 décembre 2016
PNO1	ISA-18.2 - Gestion d'alarmes : un outil efficace au service de l'opérateur - Un jour	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	14 juin 2016 20 septembre 2016 13 décembre 2016
BRI1	ISA-84 - Sûreté de fonctionnement avec les normes IEC 61508 et IEC 61511- Deux jours	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	9 et 10 mai 2016 19 et 20 septembre 2016 21 et 22 novembre 2016
BRI2	Modélisations et calculs de fiabilité pour IEC 61508/IEC 61511/S84	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	11 mai 2016 21 septembre 2016 23 novembre 2016
BRI3	Développement d'applications de sécurité IEC 61508 / IEC 61511 / ISA-84	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	2 au 5 mai 2016 12 au 15 septembre 2016 14 au 17 novembre 2016

ISA-France est reconnue comme un organisme indépendant et qualifié de formation des ingénieurs et techniciens du monde de l'automation dans les pays francophones d'Europe ou du Maghreb (Enregistrement auprès de la préfecture d'Ile de France sous le N° 11754084175). Ses programmes, conçus sur la base des standards ISA, couvrent les problèmes d'actualité du secteur de l'automation : wireless, cyber-sécurité, conception et sécurité fonctionnelles, intégration, instrumentation et mesure, normalisation.

Il est également possible d'accéder aux cours dispensés par l'ISA (USA) selon les modalités décrites sur le site www.isa.org ou d'organiser des sessions de formation intra-entreprises (Pendre contact avec ISA-France sur contact@isa-france.org ou au +33 (0)1 41 29 05 09).

Pour tout renseignement sur les stages ISA-France

- Tel : +33 (0)1 41 29 05 09
- Fax : +33 (0)1 46 52 51 93
- contact@isa-france.org
- Télécharger un bulletin d'inscription (à retourner par fax ou par courrier électronique) au format PDF au format Word

Informations et bulletins d'adhésion sur www.isa-france.org et www.isa.org
Pour toute demande de renseignements : Tel +33 1 41 29 05 09 ou contact@isa-france.org
Direction de la publication : Jean-Pierre Hauet – ISA-France – Siège social : 17 rue Hamelin – 75016 Paris
Adresse postale : Chez KB Intelligence - 10 rue Lionel Terray 92500 Rueil-Malmaison
Tel : 33 1 41 29 05 09 – contact@isa-france.org

Rejoignez-nous sur LinkedIn