C&ESAR 2013

Computer & **E**lectronics
Security **A**pplications
Rendez-vous

Sécurité des Systèmes Numériques Industriels

19 – 20 – 21 novembre 2013
Rennes - France

http ://www.cesar-conference.org

C&ESAR 2013 : Sécurité des Systèmes Numériques Industriels

Nous voici arrivés à la 20ème édition de C&ESAR (Computer & Electronics Security Applications), alias Journées SSI de la Défense. Que de chemin parcouru depuis la première édition des journées SSI du CELAR en 1997 ! L'auditoire s'est largement étendu au-delà du ministère de la Défense, et les thèmes couverts ont permis de balayer au fil des années le spectre toujours plus vaste de la cybersécurité. L'évolution des technologies et des usages a profondément transformé le monde qui nous entoure au cours des deux dernières décennies. Si l'ubiquité grandissante des systèmes informatiques a sans doute accru considérablement l'efficacité de ses processus, quels qu'ils soient, le revers de la médaille est la vulnérabilité croissante du monde moderne aux agressions à caractère informatique. La sphère de nos préoccupations déborde maintenant largement des classiques systèmes d'information et de communication, vers des domaines moins connus du grand public comme les systèmes embarqués, les systèmes d'armes, ou encore les systèmes numériques industriels.

La sécurité de ce dernier type de systèmes constitue cette année le thème choisi pour C&ESAR. Souvent désignés - de façon quelque peu réductrice - par l'acronyme anglais SCADA (Supervisory, Control and Data Acquisition), ils regroupent en fait des dispositifs très variés, allant sans être exhaustif des automates programmables autonomes aux systèmes numériques de contrôle-commande intégrés, en passant par l'instrumentation intelligente ou encore les systèmes numériques de supervision. Dénominateur commun : ils jouent un rôle critique dans de nombreuses installations industrielles et constituent un support désormais indispensable des infrastructures vitales de la Nation.

Leur sécurité (au sens protection contre les attaques informatiques dans notre contexte) est longtemps restée un sujet marginal, voire tabou, alors que toutes les attentions se concentraient sur leur fiabilité et leur disponibilité. Historiquement à l'écart des technologies et des évolutions de l'informatique tertiaire, les systèmes industriels ont pourtant ces dernières années employé les technologies numériques toujours plus près du procédé, et connu une standardisation et une interconnexion grandissantes. Si ces évolutions ont permis d'indéniables gains de performance et de productivité, elles ont aussi grandement augmenté l'exposition aux attaques informatiques. Le ver Stuxnet a projeté en 2010 cette réalité sur le devant de la scène. La médiatisation de diverses opérations d'espionnage ou d'attaque (Flame, Gauss, Rocra, Duqu, Shamoon pour n'en citer que quelques unes), bien qu'instructive, ne doit pas faire oublier qu'il ne s'agit que de la partie émergée de l'iceberg. La sécurité des systèmes numériques industriels est aujourd'hui un enjeu majeur et un défi à la fois technique, organisationnel et culturel. Le mythe de leur protection par leur isolation physique et leurs technologies propriétaires a vécu. La prise de conscience de leur vulnérabilité et le besoin crucial d'approches et de solutions adaptées sont autant de dimensions que cette édition se propose de

couvrir, à travers un programme dont nous allons maintenant décrire les grandes lignes.

L'amiral Coustillière, officier général cyber-défense, nous fait cette année l'honneur d'ouvrir la conférence, soulignant l'importance capitale des systèmes numériques industriels pour la sécurité de la Nation. Le programme s'articule par la suite en trois temps. Fidèle à sa vocation didactique, la première après-midi vise à poser la problématique générale. Elle doit permettre à l'audience de mieux comprendre la nature et les particularités des systèmes industriels, des architectures associées et de leurs implications en termes de sécurité. A cet effet, les représentants de secteurs grands utilisateurs de systèmes numériques industriels auront la parole en séance plénière ou en table ronde pour apporter leur éclairage sur la sécurité de leurs infrastructures, et échanger avec l'audience. La seconde journée couvrira un large spectre de thématiques, abordant la problématique sous divers angles : aspects techniques et organisationnels, gouvernance, spécification, normes et référentiels, certification ou encore contractualisation, autant de thèmes et de points de vue qui permettront d'appréhender le sujet de façon transverse, et de nourrir échanges et débats autour des interventions. Le dernier volet de la conférence s'intéresse au futur, proche ou plus éloigné, en traitant des dispositions à prendre pour gérer l' « après-attaque », de l'évolution des activités de l'ENISA à la maille européenne, et de travaux de recherche prometteurs pour le domaine. Enfin l'ANSSI clôturera cette conférence en dégageant pour nous enseignements et orientations.

Nous espérons que les participants à ces journées - et les lecteurs de ses actes - trouveront à ce programme autant d'intérêt que celui que nous avons trouvé à son élaboration. Pour finir, nous tenons à remercier encore une fois chaleureusement tous ceux dont l'engagement rend possible ce rendez-vous annuel de la communauté SSI : les intervenants et conférenciers, les membres du comité de programme, les organisateurs, et tous les partenaires sans qui cette manifestation ne pourrait avoir lieu.

Yves Correc (DGA-MI, ARCSI), Président du comité d'organisation.
Ludovic Pietre-Cambacedes (EDF), Président du comité de programme.
Olivier Heen (Technicolor), Directeur de publication.

Comité d'organisation

Yves CORREC, Chair	(ARCSI, France)
José ARAUJO	(ANSSI, France)
Boris BALACHEFF	(HP Labs, France)
Florent CHABAUD	(DGSIC, MoD, France)
Olivier HEEN	(Technicolor, France)
Benoît MARTIN	(DGA-MI, MoD, France)
Ludovic MÉ	(Supélec, France)
Éric WIATROWSKI	(Orange, France)

Comité de programme

Ludovic PIETRE-CAMBACEDES, Chair	(EDF, France)
Marc ANTONI	(SNCF, France)
Pierre BIEBER	(ONERA, France)
Mathieu BLANC	(CEA, France)
Patrice BOCK	(Areva, France)
Brice COPY	(CERN, Switzerland)
Yves CORREC	(ARCSI, France)
Giovanna DONDOSSOLA	(RSE, Italy)
Donald DUDENHOEFFER	(IAEA, Austria)
Mathias EKSTEDT	(KTH, Sweden)
Yannick FOURASTIER	(EADS, France)
Igor Nai FOVINO	(European Comm. – JRC, Italy)
Frédéric GUYOMARD	(EDF, France)
Patrick HEBRARD	(DCNS, France)
Sébastien HEON	(Cassidian, France)
Robert HOFFMAN	(Idaho National Labs, USA)
Thomas HUTIN	(Thales, France)
Mohammed KAÂNICHE	(CNRS/LAAS, France)
Jean LENEUTRE	(Telecom ParisTech, France)
Stefan LUEDERS	(CERN, Switzerland)
Jean-Christophe MATHIEU	(Siemens, France)
Jean-Pierre MENNELLA	(Alstom, France)
Stéphane MEYNET	(ANSSI, France)
Vitaly PROMYSLOV	(Russian Academy of Sciences, Russia)
Orion RAGOZIN	(Sogeti, France)
Pascal SITBON	(EPRI, Etats-Unis)
Fabrice TEA	(Schneider, France)

Partenaires

ANSSI, ARCSI, DGA, DGSIC, DIRISI, HP, Orange Business Services, Supélec, Technicolor.

Table des matières

Orateurs invités (sans article dans les actes)

Olivier Lesbre (DGA-MI)	Introduction
Yves Correc (ARCSI), Ludovic Pietre-Cambacedes (EDF)	Programme C&ESAR 2013
Arnaud Coustillière (EMA)	Ouverture des Journées
Olivier Chenèble (DGA-MI)	Démo. : Vulnérabilité des automates industriels
Patrick Hébrard (DCNS), Philippe Gaucher (EMM)	Problématiques de sécurité sur un navire de guerre
Yannick Fourastier (EADS) et intervenants	Table ronde : Contraintes et spécificités de la sécurité des systèmes industriels selon les secteurs d'activité
David Sancho (Trend Micro)	Who's really attacking your ICS equipment ?
Jean-Luc Trollé (EDF)	Gouvernance et intégration de la sécurité des différents domaines informatiques
Gerome Billois (CLUSIF)	Référentiels de sécurité pour le domaine industriel
Stéphane Meynet (ANSSI)	Groupe de travail ANSSI sur la sécurité des systèmes numériques industriels
Yannick Fourastier (EADS) et intervenants	Table ronde : Retex organisationnel, référentiels
Sébastien Bombal (Areva)	Cybersécurité : Lorsque le temps vient de faire face...
Guillaume Prigent (Diateam)	Simulation et sécurité des systèmes industriels
Adrian Pauna (ENISA)	ENISA current and future activities on SCADA and and ICS security

Cyber Sécurité des Systèmes de Contrôle Industriel

Les spécificités des SCI, un challenge pour leur sécurité

Jean-Michel Brun –Architecte senior en sécurité informatique - Schneider Electric
Laurent Platel - Architecte en sécurité informatique - Schneider Electric
Fabrice Tea – Développeur offre services Cyber Sécurité Schneider Electric

jean-michel.brun@schneider-electric.com

Résumé : Les systèmes industriels (habituellement appelés OT de l'anglais Operational Technology) et particulièrement les systèmes de Contrôle Industriels (SCI) ont toujours privilégié la robustesse (disponibilité, sécurité fonctionnelle…) et la performance à toute autre considération. Ces choix ont forgé un environnement dans lequel la sécurité informatique des systèmes IT est parfois inadaptée, leur principe de base étant absent des architectures industrielles actuelles.
Ce document expose les spécificités des architectures industrielles pour montrer les incompatibilités avec les solutions de sécurité de l'IT standard.

1 Le contexte des systèmes de contrôle industriel

La sécurité informatique n'est plus une exigence secondaire dans le monde du contrôle industriel contemporain.

Les systèmes de contrôle industriel(SCI), basés sur des technologies informatiques et des réseaux de qualité industrielle, sont en usage depuis des décennies. Les premières architectures de système de contrôle furent développées avec des technologies propriétaires et étaient isolées du monde extérieur. Très souvent, la protection des accès physiques était jugée suffisante et la sécurité informatique n'était pas une préoccupation majeure.

Aujourd'hui, de nombreux systèmes de contrôle utilisent des technologies répandues ou ouvertes et standardisées tels que les systèmes d'exploitation Windows© de Microsoft™, les réseaux de technologie Ethernet TCP/IP et la technologie Web pour réduire les coûts et améliorer les performances. De nombreuses architectures utilisent également la communication directe entre les systèmes de contrôle industriel et les systèmes de gestion d'entreprise pour améliorer l'efficacité opérationnelle et la rentabilité des actifs de production.

Cette évolution technique expose les systèmes de contrôle industriel aux menaces qui ciblent les applications IT et le réseau bureautique de l'entreprise. A ces menaces héritées des technologies du monde IT, Stuxnet et ses dérivés ajoutent une menace spécifique et très avancée (type APT Advanced Persistent Threat) dédiée aux systèmes de contrôle industriel, qui sont désormais vulnérables à des attaques « in-

ternes » (attaques ciblant spécifiquement les technologies de l'OT) et « externes » (les attaques ciblant les technologies de l'IT).

Le succès de la connectivité Ethernet/Internet peut amener aussi à « passer outre » les règles élémentaires de sécurité et privilégier la facilité (de maintenance par exemple) en connectant directement les systèmes SCI sur Internet, là ou il y avait auparavant l'utilisation de liaison spécialisée pour la surveillance et la maintenance à distance et donc comportant des risques de sécurité beaucoup plus faibles.

La sécurisation des systèmes industriels passe donc par une compréhension poussée de leurs spécificités et de leurs contraintes.

Parmi les défis de la sécurité dans le monde du contrôle industriel, citons :

- La multiplicité des frontières logiques et physiques : un système de contrôle industriel est composé d'équipements très différents, sur des réseaux de technologie et de capacités différentes, utilisant des protocoles variés et véhiculant des données variées.
- Des architectures couvrant plusieurs sites sur de larges zones géographiques
- Les effets indésirables de la mise en œuvre de la sécurité sur la disponibilité des processus
- L'ouverture au web des réseaux de communications de l'entreprise (informatique mobile, BYOD, réseaux sociaux) qui augmente l'exposition aux virus et vers, qui peuvent migrer du réseau d'information au réseau de contrôle
- L'exposition croissante aux logiciels malveillants par l'usage accru des lecteurs portables (clef ou disque USB), d'ordinateurs portables (service technique, fournisseur de services) et des réseaux sans-fils.
- L'impact direct des systèmes de contrôle sur les systèmes physiques et mécaniques, qui peut induire des risques sur la sécurité physique des personnes.

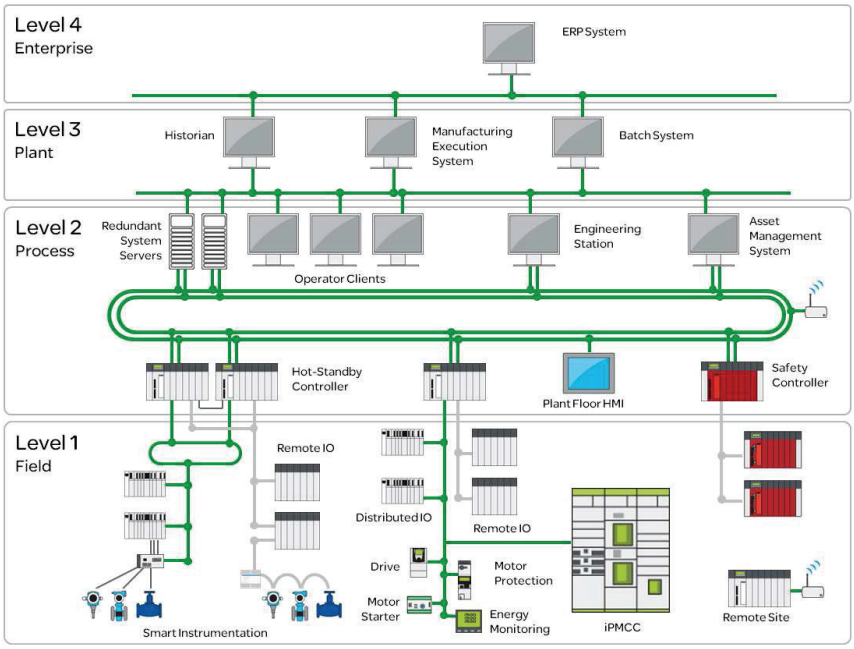
La mise en place d'un firewall n'a jamais été suffisante pour garantir la sécurité des installations industrielles. Par une approche de défense en profondeur, les entreprises doivent être vigilantes dans le choix des mesures à prendre pour sécuriser ces installations: une attaque informatique peut entraîner une perte de production, une atteinte à l'image de l'entreprise, une catastrophe écologique et dans le pire des cas, des pertes humaines. Sur cette approche, le contrôle industriel doit s'inspirer des leçons tirées du monde IT.

Mais, comme nous avons l'intention de le démontrer dans le présent document, les solutions de sécurité informatique qui ont été normalisées pour le monde IT, ne peuvent pas entrer facilement dans le monde OT et particulièrement les systèmes de contrôle industriel.

2 Les principales caractéristiques des équipements industriels

2.1 Description d'un Système de Contrôle Industriel

La norme ISA95 a pour but de fournir un modèle d'entreprise qui contient les fonctions de gestion et de production. Le modèle définit plusieurs niveaux, chaque niveau est dédié à une fonction différente, avec des contraintes différentes.



Niveau 1 (Level 1 Field): le niveau bus de terrain est dédié au contrôle (mesure) et à la commande du Procédé de production.

Niveau 2 (Level 2 Process): le niveau Procédé est dédié à la surveillance et prise de décision du système de production, donc il pilote les équipements du Niveau 1. A l'intérieur de ce niveau Procédé, on peut identifier deux sous-niveaux :

- Le niveau SCADA (Supervisory Control and Data Acquisition) qui affiche l'état du processus à l'aide de représentations graphiques, gère les alarmes, enregistre les données recueillies et assure la conduite du Procédé.
- Le niveau Automate (PLC : Programmable Logic Controller) qui effectue le contrôle automatisé du Procédé. Il prend en entrée les données fournies par les équipements du niveau 1, des IHM (petits terminaux graphiques permettant la saisie de

valeurs par un utilisateur), ou du SCADA et il calcule ces informations pour générer des commandes à travers ses sorties.

Niveau 3 (Level 3 : Plant): le niveau Usine est dédié à la gestion et la répartition de la production en fonction de la charge des ateliers, des recettes de production (généralement via un système MES /Manufacturing Execution System).

Niveau 4 (Level 4 Enterprise) : le niveau Entreprise a pour mission :

- De planifier la production en fonction des commandes des clients
- De gérer les commandes de matériels et matières premières
- De gérer la livraison au client et la logistique en général

Remarque: ISA 95 est une norme internationale pour développer une interface automatisée entre les systèmes de contrôle et l'entreprise. Il est utilisé dans ce document pour illustrer les différentes couches d'applications et de dispositifs de commande industriels. Ainsi, ISA 95 n'est pas pertinente pour décrire d'autres systèmes industriels tels que les systèmes électriques ou le « Smart Grid ».

2.2 Spécificités et contraintes d'un Système de Contrôle Industriel

Ce chapitre a pour objectif de décrire les diverses spécificités et contraintes des Systèmes Industriels (OT) et spécifiquement les Systèmes de Contrôle Industriel, qui sont un challenge pour les solutions de sécurité du monde IT.

Les contraintes de temps.

Le procédé de fabrication est géré en temps réel, c'est-à-dire la réaction à un événement du procédé doit être immédiate (<1ms). Ainsi, les temps de cycles et les temps de réponse sont essentiels pour maintenir le taux de productivité ou la sécurité fonctionnelle (à ne pas confondre avec la sécurité informatique).

Temps de cycle automate:

Le temps de cycle automate correspond à la fréquence de répétition du programme, lié au rythme de la scrutation des entrées/sorties du système. Il correspond au temps d'exécution de l'application, rebouclant sur elle-même à l'infini, avec une durée moyenne comprise entre 5ms et 100ms selon les procédés. Les équipements ICS ont des mécanismes de contrôle de ce temps (chien de garde).

Temps de réponse :

L'équipement doit répondre à une demande dans un temps limité. Le temps de réponse est très critique et peut être extrêmement serré (par exemple, 1 ms pour émettre/recevoir une alerte « Goose » dans la norme IEC 61850 concernant les stations/postes électriques).

Déterminisme:

La durée de l'action / demande doit être prévisible et stable dans le temps.

Action/réaction:

Le volume du trafic réseau augmente fortement lorsque le système se prépare à changer d'état (ou s'adapte à un changement d'état) : maintenance, arrêt d'urgence, redémarrage, étalonnage. Cette évolution ne doit pas dégrader le fonctionnement du système.

Les contraintes de ressources.

Les dispositifs industriels comme les 'Automates Programmables (PLC), les Intelligent Electronic Device (IED), équipements dédiés à la protection et le contrôle-commande des systèmes électriques (les postes ou sous-stations électriques par exemple), sont soumis à des contraintes de ressources (processeur à capacité limité, faible capacité de stockage et mémoire, ...).

Les spécificités des protocoles industriels.

Les protocoles industriels existants (même ceux basés sur TCP/IP) partagent généralement les caractéristiques suivantes :

Trames courtes.

Trames de 200-1000 octets : si le SCI doit échanger une « grande » quantité de données, il génère plusieurs requêtes.

Pas de gestion de transaction.

Le système génère des requêtes indépendantes les unes des autres.

Les réseaux non-TCP/IP

La partie finale du réseau, qui dessert les capteurs et les actionneurs, utilise des bus de terrain basés sur des technologies dédiées : réseau sur bus série, réseau CAN, …

Le manque de sécurité des protocoles industriels

Pour certains des protocoles existants, il manque les fonctions de sécurité élémentaires :

- Pas de gestion de transaction, (ou alors c'est une solution propriétaire)
- Pas d'authentification
- Le SCADA ou tout élément du SCI peut générer des flots de requêtes simultanées (et pour le même équipement)
- Pas de chiffrement pour la confidentialité
- Pas de gestion de l'intégrité (hormis un checksum)

Le cycle de vie des SCI.

Deux contraintes principales régissent ce cycle de vie :

- La durée de vie d'un SCI est comprise en général entre 10 et 20 ans
- Le SCI évolue fréquemment : remplacement d'un équipement/machine, extension/modification de la ligne de fabrication…

Les contraintes d'organisation des SCI.

La plupart des SCI fonctionnent 24h/24, 365 jours par an. Tout arrêt a des répercussions sur la production, donc sur les revenus de l'entreprise. Un arrêt mensuel pour une installation de patch (par exemple le premier mardi du mois) n'est pas acceptable.

Toute panne (matérielle ou logicielle) doit être résolue le plus rapidement possible. La plupart du temps, on répare et on redémarre, il est hors de question de 'profiter' de l'arrêt pour mener des actions de mise à jour.

Pour éviter ces pannes, ou pour limiter le risque de pannes, les modifications d'applications, les mises à jour (antivirus sur un SCADA, système d'exploitation, firmware…) sont rarement acceptées.

Environnement distribué et multi site sur de larges zones géographiques :

Une installation de traitement des eaux avec stations de pompage, usines de traitement,… devra gérer la complexité de la sécurisation d'un environnement distribué et réparti dans une large zone géographique.

Les contraintes d'environnement des SCI.

Les équipements qui fonctionnent dans les SCI font face à divers environnements bien loin des atmosphères contrôlées et tempérées des centres de traitement de données (Datacenter) : température extrême, pression, atmosphères explosives, perturbation électromagnétique (CEM)…

.

3 Sécuriser un Système de Contrôle Industriel : Pourquoi les solutions de sécurités habituelles ont des limites ?

3.1 Les contraintes de temps

Temps de réponse

L'ajout d'une solution de filtrage des échanges (firewall) peut rajouter un temps de latence dans la communication.

Ce délai peut s'avérer incompatible avec les temps de réponse imposés au SCI.

Pour sélectionner un équipement de filtrage (pare-feu par exemple), il est donc indispensable de tenir compte :

- du volume de communication
- du temps de réponse exigé pour chaque équipement
- de la taille des trames de communication
- des spécifications de l'équipement de filtrage.

Déterminisme.

Les irrégularités dans le volume échangé et le filtrage systématique du flot de communication peuvent générer des congestions du réseau (et du firewall). Cela n'est évidemment pas compatible avec la contrainte de déterminisme des actions/réactions propre aux SCI.

Action/Réaction.

Le temps de réponse ne doit pas exploser lorsque le trafic explose (situation de crise ou préparation d'un nouvel état). Il faut donc que le 'temps' dédié à la sécurité ne soit pas proportionnel au trafic. Et il ne faut surtout pas qu'une partie du trafic disparaisse suite à une décision erronée de l'équipement de surveillance (équipement de sécurité de type Détection d'intrusion/ prévention d'intrusion), pouvant mettre en cause les principes d'actions/réactions.

3.2 Les contraintes de ressources

La mémoire et le processeur sont déjà utilisés par le procédé industriel. Il est difficilement envisageable d'ajouter une tâche de sécurité informatique (Système de détection d'intrusion machine ou HIDS/Hosted Intrusion Detection System), système de type Contrôle d'Application ou Whitelisting…) dans les équipements industriels, présentant de plus des contraintes de ressources par conception.

3.3 Les spécificités des protocoles industriels

Trames courtes

Les protocoles industriels se basent sur des échanges très simples, sur des données limitées en taille. Les échanges privilégient des requêtes courtes, mais nombreuses. La raison principale est de faciliter la gestion d'une requête par le PLC, afin de garantir un bon délai de réponse.

Il n'y a pas de requêtes en XML ni de réponses structurées. Par contre, il y a fréquemment 10, 20 ou 100 requêtes émises simultanément.

C'est donc une réelle charge pour tout équipement de sécurité, responsable de filtrer ce trafic.

Pas de transaction/session.

Certains protocoles industriels n'ont pas de gestion de session/transaction. Ce qui les rend particulièrement vulnérables aux attaques par rejeu de paquet. La protection et le filtrage de la communication deviennent difficiles sans schéma transactionnel.

Dans une séquence identifiée, il n'y a pas de moyen de définir un niveau de confiance pour l'ordre de certaines trames. Toutes les trames doivent être inspectées en profondeur (Par contre, un mode stateless du système de filtrage suffit).

Les protocoles non TCP/IP .

En bout de réseaux, les bus de terrain utilisés pour connecter les capteurs/actionneurs aux automates ne sont pas basés sur TCP/IP, et encore moins sur UDP/TCP. Ils peuvent utiliser des adressages spécifiques sur câbles Ethernet, des câbles spécifiques (Modbus+, CanOpen, BacNet,) ou même utiliser des lignes séries (Modbus-RTU, Fip, Profibus, FieldBus) voire des courants porteurs (LonWork). A ces canaux historiques, se rajoutent les solutions radio (Zigbee, 6LoWPAN)

Ces protocoles restent hors de portée d'une surveillance d'outil de sécurité IT, basé sur IP, et c'est pourtant là que Stuxnet « jouait ».

3.4 Le cycle de vie des SCI

Les installations industrielles (sidérurgie, chimie construction automobile,…) ou les infrastructures (réseau routier, ligne électrique, gestion de l'eau,…) ont des durées de vie de plusieurs dizaines d'années. Les systèmes de contrôle de ces installations sont donc installés pour 10 ou 20 ans, avec de très rares et courtes fenêtres d'intervention.

Il faut donc spécifier des outils de cyber-sécurité sur cette durée de 20 ans, ce qui pose un véritable challenge.

En effet, à quoi ressemblait un firewall il y a 20 ans ?

Quels filtrages assurait-il ?

A contrario, que fera-t-il dans 20 ans ?
Quelles règles seront applicables ?
Quel niveau de complexité sera nécessaire pour évaluer ces règles ?
Sur quels protocoles ?

De la même façon, la ligne de production tend à avoir de plus en plus d'action (mesure de qualité, gestion de différentes versions du produit fabriqué, différents emballages) et à avoir de plus en plus d'équipement.

La durée de vie des installations industrielles, combinée à l'évolution de l'appareil de production, rend très difficile de déterminer la puissance nécessaire à des équipements réseaux pour 20 ans.

De plus, un firewall dont l'OS n'a pas reçu de mise à jour pendant 20 ans aura probablement perdu beaucoup de son efficacité.

3.5 Les contraintes d'organisation des SCI : la disponibilité

La disponibilité du système est essentielle, il est synonyme de sécurité des personnes et de revenus pour l'entreprise.

En cas d'événements spéciaux comme un changement d'état de l'automate (PLC) ou une opération spécifique (qui peut être une crise sous contrôle), qui génèrent des augmentations de communication avec des échanges spécifiques (échange de recettes de l'application, fonctionnement normal/secours et sauvegarde...) le système doit rester opérationnel avec différents niveaux de disponibilité et / ou de sécurité.

D'autre part, en cas d'attaque, le trafic de communication peut également augmenter avec des échanges anormaux ou «étranges». Mais, dans cette situation, la communication doit être arrêtée.

Comment détecter et différencier ces deux cas d'utilisation car la réponse à apporter n'est pas du tout la même ?

3.6 Les contraintes d'environnement des SCI.

Les équipements de sécurité dédié IT sont rarement prévus pour des atmosphères sales (poussière, humidité) ou extrêmes (température, pression, atmosphère explosive, perturbation électromagnétique...)

Pour tenir compte de ces contraintes, les équipements de contrôle et les équipements de communication sont généralement installés dans un seul coffret, dont l'accès n'est pas spécifiquement limité.

Il est donc difficile d'appliquer les règles habituelles de la «séparation des tâches» et de «moindre privilège» dans ces installations.

Ces équipements se retrouvent alors à la fois trop accessibles (beaucoup de personnes peuvent accéder et ouvrir ces armoires) et pas assez (les armoires sont réparties sur toute l'installation, il faut réellement parcourir le site industriel pour effectuer une maintenance ou un dépannage).

4 Conclusion

Les solutions de sécurité informatique dans le domaine IT ont constamment progressé depuis les premiers firewalls et la sécurité des années 80. Les développements ont suivi l'évolution des usages, en particulier l'explosion d'Internet et de ses applications.

La sécurité informatique du domaine industriel a beaucoup à apprendre ; mais appliquer directement les produits/solutions conçus pour un autre domaine peut nuire au système de production au lieu d'améliorer la sécurité.

Les solutions techniques de sécurité doivent être repensées et adaptées pour remplir efficacement leur mission de sécurité tout en laissant le SCI remplir ses obligations de performances et de disponibilité.

Ces solutions doivent tenir compte des caractéristiques de l'ICS que nous avons décrites dans ce document. Elles doivent s'appuyer sur ces caractéristiques, qui en même temps, peuvent être de bons piliers en matière de sécurité. Par exemple la grande régularité des échanges, lors de phases de production nominale, peut facilement permettre de détecter des communications indésirables.

5 Glossaire

IT: Technologies de l'information

OT: Operational Technology, désigne les technologies utilisées dans les systèmes industriels

PLC : (Programmable Logic Controller) : Automates programmables

IED: Intelligent Electronic Device, Equipement Electronique Intelligent, terme utilisé dans les systèmes électriques

HMI/IHM: Interface Homme Machine

SCADA: Supervisory Control And Data Acquisition, télésurveillance et acquisition de données ou Superviseur Industriel

IDS : Intrusion Detection System, Système de détection d'intrusion

- NIDS: Network Intrusion Detection System, Système de détection d'intrusion sur réseau
- HIDS: Hosted Intrusion Detection System, Système de détection d'intrusion sur un poste.

IPS: Intrusion Prevention System, , Système de prévention d'intrusion

Whitelisting: Contrôle d'applications qui n'autorise à démarrer et s'exécuter que les process logiciels sûrs (liste blanche), bloquant tous les autres process.

Cyber Security of Industrial Control System

Why ICS specificity lead to Cyber Security Challenge?

Jean-Michel Brun –Cyber Security Senior Architect - Schneider Electric
Laurent Platel - Cyber Security Architect- Schneider Electric
Fabrice Tea –Cyber Security Services Business Developer - Schneider Electric

jean-michel.brun@schneider-electric.com

Abstract : Industrial systems (usually named Operational Technology system) and specially the Industrial Control System (ICS) always focused the robustness (availability, safety…) and performances to any other considerations. These choices have forged an environment where IT security systems are sometimes inadequate and their basic principle missing from the current industrial architecture.
This document outlines the specifics of industrial architecture to show inconsistencies with security solutions of standard IT.

Keywords: determinism, response time, availability, life cycle, industrial protocol,

1 The context of industrial control systems

Cyber security is no longer a secondary requirement in the world of contemporary industrial control.

The industrial control systems (ICS) based on computer technology and industrial grade network are in use for decades. The first control system architectures were developed with proprietary technologies and were isolated from the outside world. Often physical perimeter security was deemed adequate and cyber security was not a primary concern.

Today, many control systems use common or open and standardized technologies such as the Microsoft™ Windows ©, IP network technology Ethernet TCP / IP and Web technology systems to reduce costs and improve performances. Many architectures also use some direct communications between the industrial control systems and the business management systems to improve operational efficiency and profitability of production assets.

This technical evolution exposes the industrial control systems to threats that target IT applications and office corporate network. Upon these threats inherited of the IT world technologies, Stuxnet and its derivatives add a specific threat and very advanced threat like APT (Advanced Persistent Threat) dedicated to industrial control systems. ICS are now vulnerable to "internal" attacks (attacks specifically targeting technology OT) and "external" (attacks propagated by IT technology).

The success of the Ethernet / Internet connectivity can also lead to "override" of the basic safety rules and focus on ease of maintenance (for example) by directly connecting the ICS systems on the Internet. Also they were previously using specialized monitoring and remote maintenance connection and therefore security risks much lower.

The security of industrial systems therefore goes through a thorough understanding of these characteristics and the constraints.

Among the security challenges in the world of industrial control include:

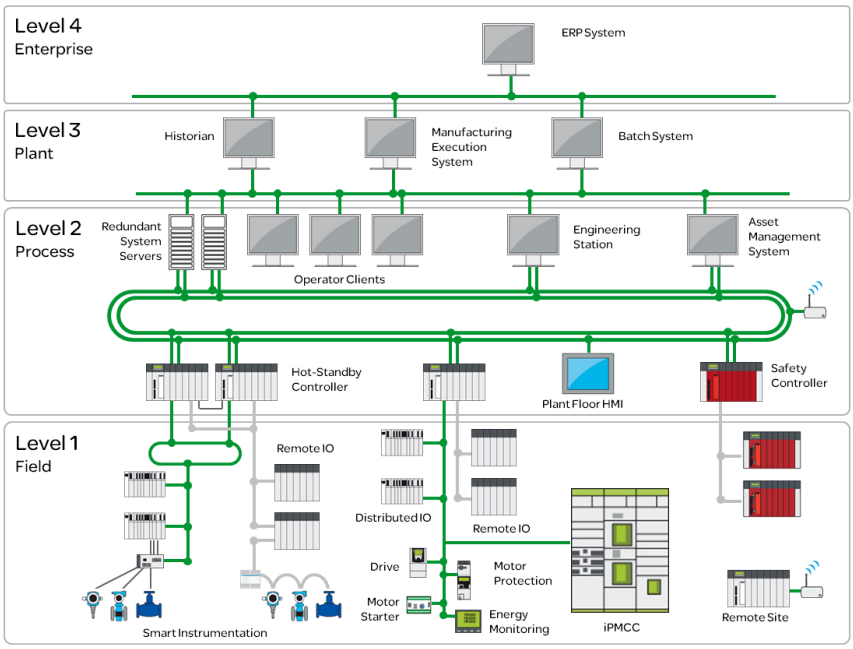
- Multiple logical and physical boundaries: an industrial control system is composed of very different devices on different network technology and different capacities, carrying a variety of protocols.
- Architectures with multiple sites over large geographical areas.
- The adverse effects of the implementation of the security on the process availability.
- The opening to the Web of the company's networks (mobile computing, BYOD, social networks), which increases exposure to viruses and worms which could migrate from information network to monitoring network.
- The increasing exposure to malware by the increased use of portable drives (USB key or disk), laptops (technical service provider) and wireless networks.
- The direct impact of the control systems on the physical and mechanical systems, which can induce risks to safety (injury or death).

The implementation of a firewall has never been sufficient to ensure the safety of industrial installations. With a "defense in depth" approach, companies must be vigilant in choosing the measures to secure these facilities: a cyber attack can cause a loss of production, damage the image of the company, an ecological disaster in the worst case, loss of life. On this approach, industrial control should draw lessons from the IT world. But, as we will intend to demonstrate in this document, cyber security solutions that have been standardized for IT world may not fit into OT world, and specially the Industrial Control Systems.

2 Industrial devices main characteristics

2.1 Industrial Control Systems description

ISA95 intends to provide a model of a company including management and operational functions. The model defines several layers, layers dedicated to different functions and with different constraints.



Level 1 or field level is dedicated to sense and manipulate the production process.

Level 2 or Process level, is dedicated to monitor and control the production process, i.e. these equipments drive the level 1 devices.

Level 2 includes:

- SCADA (Supervisory Control And Data Acquisition) that displays the process status within a graphic interface, manages alerts, log data and allows an operator to drive the process
- HMI (Human Machine Interface) that displays the process status and alerts within a graphic interface, and allows an operator to drive the process
- PLC (Programmable Logic Controller), automated control of the process. It receives input from level 1 devices, from HMI or from SCADA and process the information to drive the outputs

Level 3 or Plant level, is dedicated to manage, optimize and dispatch the production according to workflow, recipes usually using an MES (Manufacturing Execution System).

Level 4 or Enterprise level is dedicated

- to plan the production according to customer's orders
- to manage material orders and delivery
- to manage other logistic issues

Remark: ISA 95 is an international standard for developing an automated interface between enterprise and control systems. It is used in this document to illustrate the different layers of Industrial Control applications& devices. ISA 95 is not relevant to describe other systems like Smart Grid or electrical systems, but there can be some similarities.

2.2 Specificities and constraints of an Industrial Control Systems

This chapter objective is to describe the diverse specificities and constraints of OT and especially of ICS that can be a challenge to standard IT security solutions.

Time constraint.

The industrial process is managed in real time, the reaction to a process event must be immediate (less than 1 millisecond). Thus, the cycle time and response time are essential for maintaining the productivity rate or the functional safety (not to be confused with cyber security).

PLC Cyclic time

The PLC Cyclic time is the repetition frequency of the program, linked to the pace of scan I/O system. It's the execution time of the application, looping back on itself to infinity, with an average value between 5ms and 100ms according the process. The ICS devices have a control mechanism for this timing: the watchdog.

Response Time

The devices have to answer to request in a limited time. The response time is highly critical and can be extremely tight (e.g 1ms to send/receive a "Goose" alert in the IEC61850 standard for electric sub-station).

Determinism

The duration of the action / application must be predictable and stable over time.

Action/reaction

The network traffic volume increases sharply when the system is preparing to change state (maintenance, emergency stop, restart, calibration). This modification should not degrade the performance of the system.

Resource constraints.

Industrial devices, such as the controller (PLC) or Intelligent Electronic Device (IED) for protection and control command of electrical systems (stations or electrical substations, etc.), are subject to resource constraints (CPU limited capacity, low storage capacity and memory, UPS ...).

Industrial protocol specificities.

The existing Industrial protocols (even based on TCP/IP) generally have the followings characteristics:

Short Frames

Frames size is between 200 and 1000 bytes. If the ICS need to exchange a "big" quantity of data, the system will generate several requests.

No transaction management

The system will generate several independent requests.

Non-TCP/IP network

The final part of the network that serves the sensors and actuators is using fieldbus based on dedicated technologies: network serial bus, CAN network...

The lack of security of Industrial Protocols

For some existing industrial protocol, there is a lack of security features:

- No Session management or proprietary solution
- No Authentication
- The SCADA or any ICS client(HMI, etc) can generate a lot of request in parallel (and for the same device)

ICS life cycle.

Two main constraints that govern life cycle:

- The life cycle of an ICS is usually between 10 to 20 years
- The ICS is evolving frequently : replacement of device, extension/modification of manufacturing lines, etc

ICS organizational constraints

Most part of ICS runs 24h/day, 365 days / year. Any ‘STOP’ has implications for the production, so the income of the company. A monthly stop for a patch installation (e.g. on the first Tuesday of the month) is not acceptable.

Any failure (hardware or software) must be solved in a short time. Most of the time, it’s “repair and restart”, it is out of question to 'benefit' of the stop to update anything.

To avoid such failures, or to minimize the risk of failures, unplanned application changes, updates (antivirus, operating system ...) are rarely accepted.

Distributed environment and multi-site over large geographical areas

Water distribution architecture with pumping, water treatment, waste water treatment will manage different installation spread all over a city area, or over a complete county in case of metropolitan.

ICS environment constraints

Devices running in industries face different environments far from controlled and regulated atmosphere of a IT data center: extreme temperatures, pressure, explosive atmospheres, ElectroMagnetic Compatibility…

3 To Secure an Industrial Control System: Why the standard security solutions show their limitations?

3.1 Time constraints

Response time

Integrating of a communication filter solution such as firewall may add latency in the communication traffic.

This delay may be incompatible with required tight response time of the ICS.

Thus, to select a filtering device and to define its location within the ICS architecture, it is critical to consider:

- Communication traffic flows
- Required response time of each device
- Frame sizes of communication
- Specifications of filtering device.

Determinism

Irregularities in the trading volume and the systematic filtering of the flow (eg firewall) can generate network congestion (and firewall overload). This is not compatible with the requirement of determinism in actions / reactions.

Action/Reaction

The response time should not increase during traffic bursts (crisis or preparing a new state). This requires that the 'time' dedicated to safety is not proportional to the traffic. And no part of the traffic could disappear after a decision of the monitoring equipment (cyber-security equipment like Intrusion Detection / Prevention System).

3.2 Resources constraints

The memory and the processor are already used by the industrial process. It is difficult to envisage adding a task computer for security (detection system or intrusion Machine HIDS / Hosted Intrusion Detection System), type system Application Control and Whitelisting ...) in these devices, because resources are not available.

3.3 Industrial protocol specificities

Short Frames

Industrial protocols are based on very simple exchanges on limited data size. The exchanges prefer short queries, but several requests. The first idea is to facilitate the management of a request by the PLC to ensure a good response time.

There are no queries in XML or structured responses. By cons there are often 10, 20 or 100 queries issued simultaneously.

It is a real burden for any safety equipment, responsible for filtering the traffic.

No transaction/session

Some industrial protocols do not have session management / transaction. This makes them particularly vulnerable to replay the attacks.

So there is no way to define a trust for some frames over their place in an identified transaction. All frames must be inspected in depth (but a stateless mode filtering system is enough).

Non-TCP/IP protocols

At the bottom part of the networks, field buses used to connect sensors / actuators to PLCs are not based on TCP / IP, or even UDP / TCP. They can use specific mappings of Ethernet cables, special cables (+ Modbus, CANopen, BACnet,), the serial lines (Modbus-RTU, FIP, Profibus, Fieldbus) or even use powerline (LonWorks). And now we can also find some radio solutions (Zigbee, 6LoWPAN).

These protocols are out of range of a monitoring tool based on IP, and yet it is here that Stuxnet was playing.

3.4 ICS life-cycle

Industrial facilities (steel, chemicals, automotive) and infrastructure (roads, power lines and water management) have lifetimes of several decades. Control systems of these facilities are installed for 10 or 20 years, with very few and short windows of maintenance.

The cyber security tools must be usable on this for 20 years, and this is a big problem.

What was a firewall 20 years ago?
What did it check?

Conversely, what will it do in 20 years?
What rules will apply?
What level of complexity is necessary to evaluate these rules?
Which protocols?

Similarly, the production line tends to have more action (quality measurement, management of different versions of the manufactured product, different packaging) and have more and more equipments.

The lifetime of industrial facilities combined with the evolution of the production system makes it very difficult to determine the capacity required for network equipment in the next 20 years.

In addition, a firewall, whose OS has not been updated for 20 years, is probably much less effective.

3.5 ICS organizational constraints: Availability

System availability is essential; it is synonymous with safety (for people) and cash-flow for the company.

In case of special events such as a PLC status change (PLC) or a specific operation (which may be a crisis under control) that generate increases communication with specific exchanges (exchange revenue of the application, Hot standby / backup ...) the system must remain operational with different levels of availability and / or safety.

On the other hand, in case of attack, the communication traffic may also increase with abnormal or "strange" trade. But in this situation, this communication must be stopped.

How to detect and differentiate these two use cases as the response to is not at all the same?

3.6 ICS Environnement constraints.

The devices dedicated to “IT Cyber-security” are rarely provided for dirty environments (dust, humidity) or extreme environments (low/high temperature, pressure, explosive atmosphere, electromagnetic interference ...)

To address these constraints, control equipment and communication equipment are installed in a single cabinet, to which access is not specifically limited.

It is therefore difficult to apply the usual rules of "separation of duties" and "least privilege" in these facilities.

These devices are then found both too accessible (too many people can open these cabinets) and not enough accessible (cabinets are distributed throughout the installation, you must actually travel through the site to perform industrial maintenance or troubleshooting).

4 Conclusion

The security solutions in the IT field have grown steadily since the early '80s firewalls. The developments followed the evolution of uses, especially the explosion of the Internet and these applications.

Cyber-security in industrial area has a lot to learn, but apply the products / solutions designed for another area can directly affect the production system instead of improving security.

Technical security solutions need to be re-design and adapted to effectively fulfill their mission of safety while leaving the ICS to do its obligations of performance and availability.

These solutions must take into account the characteristics of the ICS that we mentioned above. They should be based on these characteristics, which can be good pillars of security, for example the great regularity of exchanges during periods of nominal output, can easily afford to detect unwanted communications.

5 Glossary

IT: Information Technology
OT: Operational Technology
PLC : Programmable Logic Controller
IED: Intelligent Electronic Device
HMI: Human Machine Interface
SCADA: Supervisory Control And Data Acquisition,
UPS : Uninterruptible Power Supply
IDS : Intrusion Detection System,
NIDS: Network Intrusion Detection System
HIDS: Hosted Intrusion Detection System
IPS: Intrusion Prevention System
Whitelisting software: Software application that allows to start and run the authentified process (white list), blocking all other processes.

Retour d'expérience RTE suite à Stuxnet

Patrick Assailly (RTE –DSIT)

Jean Marie Boisset (RTE-CNER)

Philippe Jeannin (RTE-DSIT)

Abstract. RTE est le gestionnaire du réseau de transport d'électricité français. Pour assurer sa mission, RTE dispose d'un réseau électrique composé de postes électriques conduits à partir de dispatchings et de groupements de postes. Les équipements qui composent cet outil industriel se sont progressivement numérisés à partir des années 2000. Un risque nouveau lié à la sécurité informatique a été dès l'origine pris compte mais il s'est avéré plus crucial qu'escompté lorsqu'est survenu en 2010 le virus Stuxnet. En effet, la connaissance de l'existence de Stuxnet a incité RTE à lancer une campagne nationale de recherche virale dans ses postes électriques dotés d'un contrôle commande numérique. Le virus incriminé ne s'y trouvait pas mais d'autres virus – inoffensifs – ont été détectés. RTE a entrepris depuis une analyse de risque globale de la sécurité du SI. RTE dispose d'une feuille de route de sécurisation de son SI déclinée en actions de sécurisation internes et externes en partenariat avec ses fournisseurs industriels.

Keywords: Outil industriel, numérique, stuxnet, virus, risque, sécurité informatique, SCADA, contrôle-commande, vulnérabilité

1 Présentation de RTE, de sa mission et de ses enjeux

RTE, société anonyme du groupe EDF, est le gestionnaire du réseau français de transport d'électricité à haute et très haute tension. Entreprise de service public et Opérateur d'Importance Vitale, il a pour mission l'exploitation, la maintenance et le développement du réseau haute et très haute tension. Il est garant du bon fonctionnement et de la sûreté du système électrique.

RTE veille à la qualité de ses infrastructures et à une gestion optimale des flux d'électricité sur le réseau et contribue, par sa mission même, à la mise en œuvre de la transition énergétique.

RTE achemine l'électricité entre les fournisseurs (français et européens) et ses clients, qui peuvent être des distributeurs ou des industriels directement raccordés au réseau de transport.

Avec 100 000 km de lignes de tensions comprises entre 63 000 et 400 000 volts et 46 lignes transfrontalières (appelées "interconnexions"), le réseau géré par RTE est le plus important d'Europe.

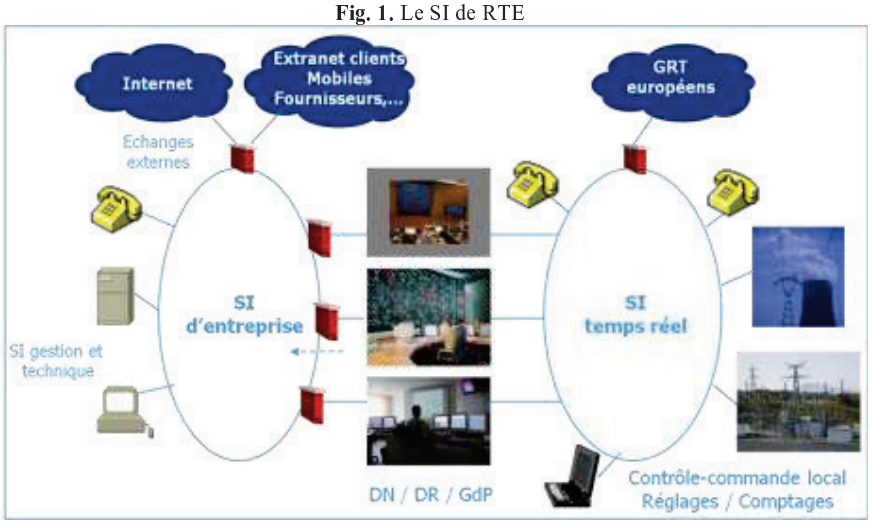
RTE a réalisé un chiffre d'affaires de 4 529 M€ en 2012 et emploie 8 400 salariés.

2 Présentation du Système d'Information de RTE

L'architecture du Système d'Information (SI) de RTE est organisée en 2 zones :

- Le SI d'entreprise est un intranet auquel sont connectés les postes de travail tertiaires des agents de l'entreprise, les applications de gestion et techniques hors temps réel de RTE et le réseau internet pour assurer les échanges avec l'externe.
- Le SI temps réel comprend les systèmes de contrôle commande des dispatchings et des postes électriques. Il est connecté à un réseau de télécommunications qui assure les échanges avec les Gestionnaires de Réseau de Transport européens.

Fig. 1. Le SI de RTE



Ces deux systèmes d'information ont été conçus comme étant séparés et exploités par des opérateurs différents (un infogérant externe pour le SI d'entreprise et des équipes régionales de maintenance de RTE pour le SI temps réel) ; ces deux mondes sont connectés entre eux au travers de coupe-feu.

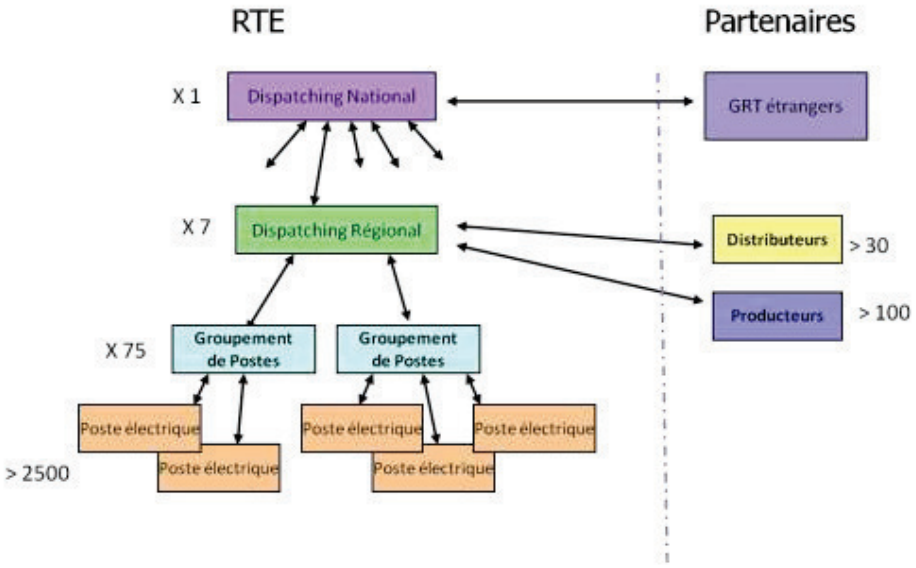
3 Présentation du rôle des dispatchings, des postes et de leur contrôle-commande

Le contrôle-commande du réseau électrique est organisé en quatre niveaux :

- Le dispatching national a pour mission de gérer le réseau 400 kV, l'équilibre entre l'offre et la demande d'électricité et les échanges d'énergie avec les pays voisins.
- Les 7 dispatchings ou Centres de conduite régionaux ont pour mission de gérer les réseaux de niveau de tension inférieures (de 225 kV à 63 kV) et de télécommander le réseau 400 kV sous la responsabilité du dispatching national.

- Les 75 groupements de postes ont pour mission la maintenance du réseau et ils assurent la conduite du réseau en secours du dispatching régional.
- Enfin, le contrôle-commande local des 2500 postes électriques constitue le secours ultime en cas d'indisponibilité des niveaux supérieurs.

Fig. 2. Les quatre niveaux de téléconduite à RTE



Chacun de ces niveaux est doté d'un SCADA (SCADA, acronyme de l'anglais Supervisory Control And Data Acquisition est un système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques).

4 Les différents paliers technologiques du contrôle commande et leur numérisation progressive

Le Contrôle-Commande d'un poste électrique assure la conduite, la protection et la reprise de service des différents constituants du poste, à savoir les départs des lignes de transport et de distribution y aboutissant et ses éléments internes comme les jeux de barre ou transformateurs. Un poste se compose de différentes fractions appelées tranches et dédiées à un constituant du poste (départ ligne, jeu de barres, transformateur,…).

Les installations du contrôle-commande de poste à RTE reposent sur des paliers technologiques, industrialisés à partir du début des années 1970 :

- Avant 1975, le palier *Ariane* s'applique aux postes de tous niveaux de tension avant 1975, lorsque les contraintes d'élimination des défauts électriques étaient suffisamment légères pour qu'on puisse se contenter de systèmes de protection électromécaniques à base de relais.
- A partir de 1975, le palier *Briséis* s'applique aux postes 400 kV pour tenir compte de l'évolution importante du réseau 400kV qui devait accueillir des centrales nucléaires, les systèmes de protection contre les défauts électriques étant alors en technologie électronique.
- A partir de 1983, le palier *Cynthia* s'applique aux postes 225 kV et HT pour tenir compte des nouvelles exigences de rapidité et de sécurité des protections des réseaux régionaux, en corrélation avec les contraintes du réseau 400 kV doté de systèmes de protection en technologie électronique à l'image du palier *Briseis*.
- A partir de 1986, le palier *Daphné* s'applique à tous les nouveaux postes. Ce palier n'apporte pas de changements technologiques majeurs (électronique ou numérique) au niveau des systèmes de protection, mais son installation a été conçue comme un produit industriel entièrement réalisé et testé en usine.

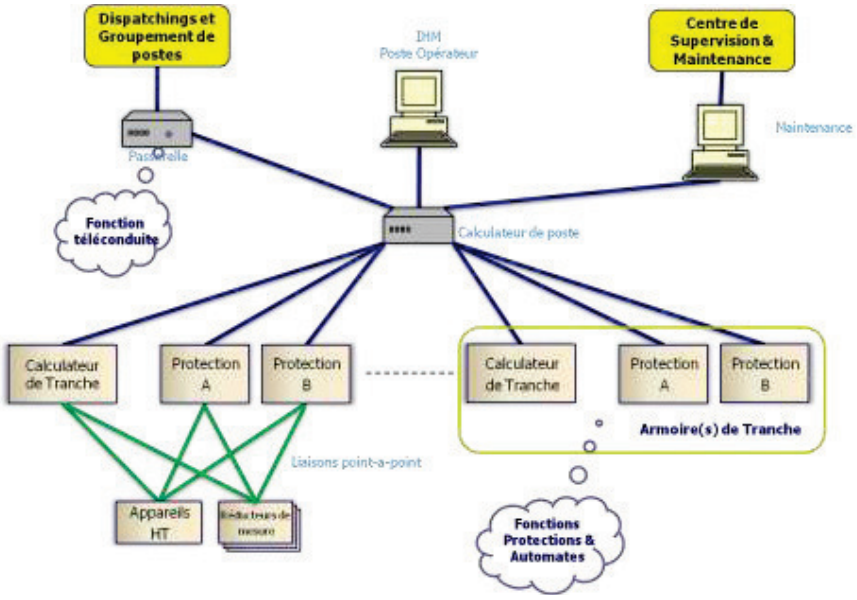
Ces paliers utilisent donc des équipements de protection et d'automatisme électromécaniques pour le palier *Ariane*, statiques pour les paliers *Briséis* et *Cynthia*, et enfin numériques pour le palier *Daphné*. Ces équipements, basés sur des technologies majoritairement propriétaires de leurs constructeurs, n'utilisent pas de mode de communication numérique. Ils ne sont pas (ou peu) sensibles aux attaques informatiques.

L'avènement du Contrôle-Commande Numérique (CCN) au milieu des années 2000, couplé au besoin de renouvellement des paliers obsolètes (*Ariane* et *Briséis*), a introduit les technologies de l'information et de la communication dans les postes électriques via un nouveau palier appelé *Electre*. Ces nouveaux systèmes numériques peuvent utiliser des composants matériels et logiciels sur étagère (OS Windows, switch & routeurs Ethernet,…) et offrir un accès distant, au travers de réseaux de communication propriétaires ou opérés, permettant la mise en œuvre de nouvelles fonctions de télé-supervision, télé-administration et télé-maintenance.

Dans un poste électrique de technologie Electre, on trouve :

- Un calculateur de poste, optionnel, qui assure le regroupement des informations issues des équipements de tranches et leur diffusion vers les PC locaux et la passerelle, ainsi que les automatismes de niveau poste ;
- Un calculateur par tranche, qui assure les fonctions de conduite et d'automatismes de la tranche ;
- Une ou plusieurs protections par tranche ;
- Des PC locaux (poste opérateurs et de maintenance), le PC de maintenance étant relié au centre régional de supervision et de maintenance ;
- Une passerelle de téléconduite qui assure la conversion de protocole et le dialogue avec les dispatchings et les groupements de postes.

Fig. 3. Schéma du contrôle-commande numérique d'un poste électrique



5 La sécurité informatique du SI industriel

5.1 Les années 2000 – Prise en compte de la sécurité

La sécurité informatique a été prise en compte par RTE au début des années 2000 pour son SI d'entreprise et pour la téléconduite de ses postes.

Concernant l'opérateur d'Importance Vitale qu'est RTE, outre la prise en compte de la sécurité dans son réseau informatique d'entreprise avec notamment la diffusion d'antivirus sur ses postes de travail, la gestion des patchs sécurité ainsi que la surveillance des accès au SI, les préoccupations de sécurité informatique de son SI industriel sont également survenues dès le début des années 2000 avec le déploiement de SCADA dans les Groupements de Postes.

Ces Systèmes ont été déployés avec un certain nombre de coupe-feu destinés à surveiller et contrôler tous les accès distants qui peuvent y être effectués. Un centre opérationnel d'administration et de supervision de la sécurité a été mis en place en 2004 pour gérer le parc de coupe-feu, pour contrôler les accès effectués depuis les zones de moindre niveau de sécurité, pour détecter les agressions sur la Téléconduite (Réseau industriel acheminant les informations temps réel échangées entre les postes électriques, les moyens de production et les dispatchings) et donc superviser la sécurité du SI temps réel de RTE.

5.2 2010 - L'arrivée de Stuxnet

2010 est une année charnière qui, avec l'arrivée du virus Stuxnet a montré que les postes électriques de RTE étaient sujets à des intrusions virales.

Le déploiement de systèmes numériques s'est poursuivi à partir de 2006 avec le déploiement des premiers Contrôles Commandes Numériques de Poste qui visent à renouveler d'ici 2018 le contrôle commande d'environ 40% de nos postes électriques (soit un millier à terme) qui étaient jusque-là dans des technologies anciennes (électromécanique ou analogique) non concernées par les problèmes de sécurité informatique.

Ces systèmes ont été déployés sans accès externes et sans lien direct avec le SI d'entreprise afin de garantir leur sécurité et on pouvait penser qu'ils étaient naturellement protégés des cyber-menaces.

Le virus Stuxnet, qui est apparu à l'été 2010, nous a démontré que ce n'était pas le cas.

En effet, ce virus qui exploitait des failles Windows de Microsoft a infecté les Systèmes de contrôle de surveillance et d'acquisition de données (SCADA) Siemens utilisés par l'Iran dans son programme nucléaire. Or, l'industrie électrique, y compris les postes électriques de RTE, utilise des briques communes à ces systèmes de contrôle-commande.

La campagne de détection virale qu'a faite RTE dès qu'il a été alerté de l'existence de ce virus a montré que ses propres Contrôles Commandes Numériques n'étaient heureusement pas impactés par ce virus, mais par contre que près de 20% des PC (Postes Opérateurs et PC de maintenance) gravitant autour de ses Contrôles Commandes Numériques étaient infectés par de nombreux autres virus.

Ces virus étaient inoffensifs, mais cette campagne a montré que nos systèmes de protection étaient défaillants, l'introduction de virus étant probablement survenue par des clefs USB, voire même introduits dès l'origine par mégarde par les fournisseurs.

Depuis 2010, des référentiels ont été mis en place pour mettre à jour les antivirus sur les PC (dans les cas où les systèmes fournis par nos partenaires industriels supportent leur présence) et avoir des supports amovibles dédiés à ces équipements critiques. Des contrôles internes réguliers permettent de vérifier l'application de ces référentiels.

Ces procédures restent cependant manuelles et sont donc susceptibles d'être omises par négligence tant que les produits du SI industriel n'auront pas été conçus de façon sécurisée à l'origine. Cette une difficulté est d'ailleurs commune à la plupart des secteurs industriels.

5.3 2012 - Analyse de risques sécurité du SI de RTE

Une analyse de risque sécurité du SI de RTE, menée en 2012, a montré que 16 événements pouvaient être redoutés.

RTE se trouve dans un contexte d'ouverture croissante de son Système d'Information (par exemple, du fait de la généralisation à venir d'accès externe à des fins de télémaintenance) et d'utilisation croissante de protocoles normalisés qui sont

connus des hackers. Aussi, afin de sécuriser ses infrastructures critiques, RTE a engagé une analyse de risques globale de son SI.

Cette analyse de risques a montré que seize événements pouvant générer des pertes d'intégrité, de disponibilité ou de confidentialité du SI de RTE en raison de malveillances étaient à redouter.

Ces événements peuvent, en synthèse, avoir trois conséquences sur le SI de RTE :

- Une altération malveillante de données affectant son intégrité,
- Une perturbation ou une indisponibilité suite à une intrusion ou un virus,
- Un vol de données confidentielles.

Des actions de réduction de risques ont été définies pour ces événements ; elles constituent la feuille de route de RTE pour sécuriser son Système d'Information. Les principales sont listées ci-dessous.

- RTE va progressivement remplacer sur son SI industriel les antivirus « classiques » par des produits fonctionnant sur le principe de la liste blanche (tous les exécutables sont interdits sauf ceux qui ont explicitement été déclarés à l'origine) ce qui résout l'épineux problème de la mise à jour des bases de signatures virales.
- RTE met en place un processus de veille sécurité sur les progiciels utilisés sur le SI industriel. Les responsables nationaux des applications industrielles sont alertés lorsque des nouvelles failles de sécurité sont publiées, ce qui leur permet d'intégrer ensuite les patchs sécurité dans les futures versions de leurs systèmes.
- RTE renforce ses systèmes de protection en ajoutant des coupe-feu à l'interface avec ses partenaires et en mettant en place des règles de filtrage sur les routeurs du réseau industriels. Les journaux de bord associés seront dirigés vers le centre de supervision de la sécurité.
- RTE étudier la faisabilité de l'utilisation des systèmes d'authentification du SI d'entreprise dans le monde du SI industriel (gestion des comptes et mots de passe).

6 Les évolutions à venir

6.1 Un plan d'action pour sécuriser structurellement les prochains systèmes de Contrôle Commande Numériques

La sécurité informatique doit être intégrée dès la conception d'un système, car elle intègre entre autre les processus mis en œuvre par les fournisseurs pour garantir l'absence de failles dans leurs développements.

Cependant, une organisation intégrant une alerte du client par les fournisseurs doit être mise en place pour surveiller ces failles de sécurité, ainsi que celles des composants sur étagère utilisés dans les systèmes, afin d'être à même de prendre les mesures adéquates sur détection d'une faille avérée.

De plus, l'analyse de risques sécurité nous a amenés à faire évoluer nos exigences de sécurité sur les systèmes de contrôle-commande numériques. Ces nouvelles exigences à l'intention de nos partenaires industriels portent sur :

- Le « hardening » des équipements, permettant de désactiver les matériels, fonctions et services inutilisés (par exemple, désactivation des ports USB ou des services Windows non utilisés),
- La protection des PC supportant des applications temps réel au travers de mécanismes de listes blanches,
- Une journalisation sécurisée des accès, c'est-à-dire la traçabilité des événements d'accès local ou distant au système, ainsi que des événements pouvant constituer une menace pour la sécurité (tentatives d'accès illicites par exemple),
- Une sécurisation des actions locales et distantes des opérateurs (hors conduite du réseau) au travers d'un équipement unique et protégé,
- Une surveillance temps réel des états des équipements et des réseaux.

6.2 Les réseaux de communications

Actuellement, les communications entre les postes électriques et le monde extérieur passent pas deux canaux distincts (représentés sur la figure 3 par les encadrés jaunes en haut du schéma).

- Le premier, qui supporte les flux de téléconduite vers les dispatchings, est basé sur des liaisons de télécommunications en partie de propriété RTE (fibres optiques, courants porteurs ligne,…) et en partie sur des liaisons opérées. Ces supports de communication sont organisés en mini-réseaux IP en forme de boucles, chaque boucle desservant quelques postes.
- Le deuxième, qui sert pour la télémaintenance et la supervision, utilise le réseau téléphonique commuté (RTC).

Dans les prochaines années, cette architecture de communication va profondément évoluer. Un nouveau réseau industriel supportera l'ensemble de ces communications. Le projet actuellement en cours a fait l'objet d'une étude de sécurité approfondie dès sa conception. La sécurité du futur réseau industriel sera administrée et supervisée depuis un centre de supervision unique.

Des bus de terrain à l'Industrial Ethernet / IP

Spécificités et impacts sur la sécurité des systèmes industriels

David Boucart, DGA Maîtrise de l'Information

david.boucart@intradef.gouv.fr

Abstract. Bien qu'utilisant de plus en plus de technologies issues du monde informatique, les réseaux industriels sont fortement contraints par les besoins des systèmes de commande-contrôle qu'ils hébergent. Cet article rappelle en première partie les spécificités des bus de terrain « historiques » et des protocoles mis en œuvre sur ces bus, en particulier les méthodes d'accès et les modes d'échanges. La deuxième partie est consacrée à la migration de ces réseaux vers Industrial Ethernet et aux différentes approches retenues par les acteurs du domaine pour adapter leurs protocoles : encapsulation, multicast, passerelle, interconnexion… Industrial Ethernet amène aussi de nouvelles fonctionnalités : création de réseaux virtuels ou de voies logiques, gestion du multicast, priorisation, contrôle des échanges. Ces considérations techniques permettent de mieux cerner les mécanismes de sécurité qui permettront de contrôler et d'améliorer la résilience des réseaux industriels.

Keywords: Systèmes de contrôle industriels (ICS), SCADA, protocoles, bus de terrain, Industrial Ethernet, sécurité.

1 Introduction

La dénomination « réseaux industriels » regroupe une multitude de technologies et de protocoles, qu'ils soient spécifiques à un domaine, liés au fournisseur d'une solution complète ou au contraire reconnus comme standards. La définition même de « réseaux industriels » est difficile à établir puisque le terme est utilisé pour qualifier les bus embarqués (automobile et aéronautique), les réseaux de contrôle des processus automatisés, les bus de mesures, les réseaux spécialisés dans la gestion technique des bâtiments, les réseaux de supervision et d'acquisition de données (SCADA) et même les réseaux informatiques utilisés dans des environnements industriels… Il semble ainsi utopique de pouvoir dresser une cartographie complète des solutions existantes et d'étudier précisément chacune de ces technologies, même si quelques-unes se sont démarquées tel que PROFIBUS dans le domaine du contrôle de processus automatisés ou les bus CAN pour l'automobile. L'objectif de cet article n'est d'ailleurs pas de présenter dans le détail ces technologies, ni de juger de l'intérêt d'un protocole sur un autre ou encore de justifier la migration vers Industriel Ethernet. Cet article a pour seul but d'aider à comprendre les spécificités des réseaux industriels (parfois hérités) et d'appréhender les impacts sur la conception de mécanismes de sécurité adaptés.

2 Spécificités des réseaux industriels

Les systèmes de contrôle industriels (ou ICS : Industrial Control System) se différencient des systèmes d'information traditionnels (aussi appelé IT pour Information Technologies) par le fait qu'ils pilotent des installations physiques (chaînes de production, distribution d'eau, d'énergie, infrastructures routières, ferroviaires, …), des véhicules (aéronautique, automobile, navires) et même des systèmes d'armes ou leurs servitudes (énergie, propulsion…). Les réseaux industriels permettant l'échange des informations nécessaires au fonctionnement de ces processus physiques doivent ainsi répondre à des contraintes spécifiques, notamment le transfert et la diffusion d'informations en « temps réel », le partage équitable et déterministe des ressources réseau, une sûreté de fonctionnement, une forte disponibilité et des contraintes physiques liées à l'environnement : encombrement, poussière, vibrations, températures…

Pour répondre en partie à ces contraintes, les technologies utilisées pour les « bus de terrain » en sont arrivées à présenter quelques spécificités communes. Ainsi l'utilisation d'un bus série multipoint (RS/EIA-485) reste très répandue, notamment pour réduire le câblage, initialement pour des raisons de coûts, mais encore aujourd'hui pour des raisons de poids et d'encombrement pour les bus embarqués.

La nécessité de partager des données en « temps réel » a conduit à optimiser les échanges de données en généralisant la diffusion de l'information : l'état d'une variable est ainsi connu « simultanément » par tous les acteurs concernés. La diffusion était d'ailleurs implicite avec l'utilisation de bus multipoints. Le format et la taille des trames sont adaptés pour faciliter le multiplexage (« émettre rapidement puis libérer le support ») : adresses ou identifiants courts (parfois sur un octet !), échanges limités à une variable. On est très loin d'une adresse IPv6 et d'une trame « jumbo » !

Enfin ces technologies ont dû adopter des méthodes d'accès au support et de pilotage des échanges afin d'assurer le partage équitable et déterministe du support de communication. Certaines solutions font ainsi usage d'un contrôle centralisé de type « maitre-esclaves » (tous les échanges sont à l'initiative du maître) ou d'un contrôle réparti à base de jeton (« token passing »), parfois même en combinant les deux (PROFIBUS). Plus exotique, la méthode « producteur / consommateur » (WorldFIP, DeviceNet) est basée sur le pilotage par un arbitre de bus qui demande la production d'une variable à partir d'une table de scrutation : l'équipement qui connait la valeur de la variable la diffuse sur le bus, tandis que les équipements qui en ont besoin se sont positionnés en attente lorsqu'ils ont détecté la demande de l'arbitre. Dans ce type de pilotage des échanges, aucun équipement n'est adressé : c'est l'identifiant de la variable qui remplit le rôle d'adresse.

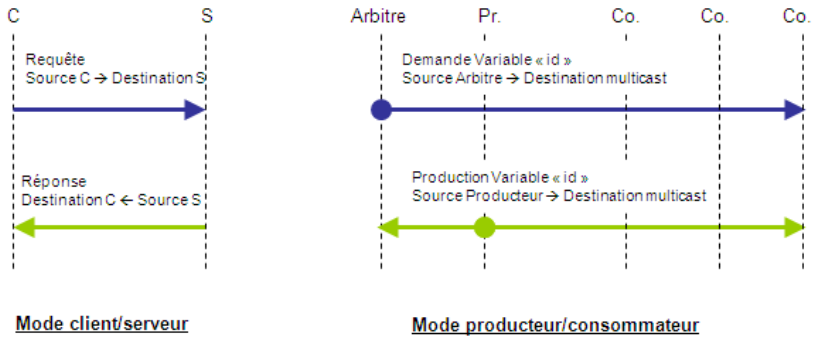


Fig. 1. Différences entre le mode client / serveur et le mode producteur / consommateur

Quelques technologies s'appuient sur un multiplexage synchrone de type TDMA. Des méthodes d'accès aléatoires telle que CSMA/CD popularisée par Ethernet n'ont pas retenu les faveurs des réseaux industriels, à l'exception de la variante CSMA/CR sur les bus CAN.

Il est toutefois important de noter que les spécificités des réseaux industriels sont très fortes au niveau des réseaux de capteurs/actionneurs (*Field Device Network*) et des réseaux d'automates (*Control Systems Network*) mais qu'elles tendent à s'estomper plus on monte dans les couches du modèle ISA-99, pour finalement se rapprocher des spécificités des réseaux informatiques.

3 Une migration difficile vers Ethernet

La généralisation de la technologie Ethernet pour les réseaux informatiques a évidemment séduit les équipementiers qui ont ainsi vu une opportunité de réduire les coûts mais aussi les exploitants qui ont ainsi envisagé la possibilité de standardiser toutes ces solutions. La méthode d'accès aléatoire mise en œuvre initialement sur Ethernet n'offrait toutefois pas le caractère déterministe, nécessaire pour des communications « temps réel ». Malgré plusieurs travaux de recherche et propositions d' « Ethernet Temps Réel » [2], c'est seulement avec l'apparition d'Ethernet commuté que la technologie Industrial Ethernet est devenue une alternative viable. Toutefois, derrière ce terme (commercial) se cache une multitude de variantes et d'adaptations parfois surprenantes.

Les constructeurs se sont effectivement confrontés à trois problèmes majeurs, à savoir reproduire une méthode d'accès spécifique sur Ethernet commuté , transposer un adressage parfois « enfoui » dans les applications en une adresse Ethernet et enfin modifier ou encapsuler leur protocole sur Ethernet ou IP.

3.1 Transposer la méthode d'accès et l'adressage

La nécessité de reproduire la méthode d'accès sur Ethernet est la conséquence d'une dépendance forte entre les applications et la couche liaison combinée au fait que certaines méthodes utilisaient la propriété native de diffusion implicite des bus de terrains. Généralement, les solutions se sont limitées à retranscrire le mode de dialogue dans le protocole applicatif et à généraliser la diffusion explicite sur l'adresse Ethernet « broadcast » ou « multicast » couplée éventuellement à IP multicast. C'est ainsi le cas pour EtherNet/IP (noter le « N ») qui est une évolution du bus de terrain DeviceNet (le pourquoi du « N ») de l'Open DeviceNet Vendor Association [4]. EtherNet/IP reproduit le mode producteur / consommateur de DeviceNet dans le protocole applicatif CIP (Common Industrial Protocol) au-dessus de TCP/IP et les variables sont identifiées par un connection-ID.

De même les mécanismes d'adressage ont pu aussi être conservés au niveau applicatif et il est courant d'empiler les adresses (l'adressage X-Way des réseaux FIPWAY, UNI-TELWAY, ETHWAY de Schneider est ainsi transposé directement sur TCP/IP à l'aide du driver XIP).

3.2 Adapter le format du protocole

Les solutions pour adapter le format du protocole à Industrial Ethernet sont toutes aussi variées que surprenantes. Elles peuvent être classées en trois catégories : l'adaptation de l'Ethernet standard, l'encapsulation sur Ethernet (valeur EtherType) ou l'encapsulation sur IP (ou même UDP/TCP). Les protocoles suivants permettent d'illustrer chacune de ces approches.

EtherCAT : une couche liaison Ethernet adaptée.

Une première approche rencontrée consiste à garder l'architecture physique (le support) et à modifier l'usage des trames Ethernet, sans impacter pour autant les commutateurs Industrial Ethernet. EtherCAT (Ethernet for Control Automation Technology, [5]), quoique basé sur Ethernet, adapte et modifie certaines caractéristiques. Les concepteurs d'EtherCAT considèrent, à juste titre, que l'utilisation individuelle de trames Ethernet par les équipements n'est pas adaptée au transfert cyclique de données de quelques octets (ce qui est classique sur un bus de terrain). Une trame Ethernet ayant une longueur minimale de 64 octets (84 octets en prenant en compte l'intervalle de temps entre trames), le ratio entre la charge utile et la taille totale est loin d'être efficace pour transmettre une donnée codée sur 3 à 4 octets. EtherCAT modifie donc l'utilisation des trames à l'aide d'un maître qui émet une trame cyclique contenant plusieurs champs de données et pour laquelle chaque nœud esclave du réseau pourra lire et écrire si les données lui sont adressées. La trame est retournée vers le maître par le dernier équipement du segment EtherCAT. La lecture des variables est réalisée lors du trajet du maître vers les esclaves et l'écriture des variables est possible lors du retour de la trame vers le maître.

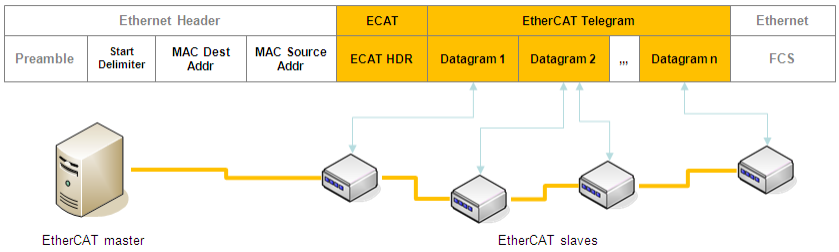


Fig. 2. Format d'une trame EtherCAT et mode de dialogue Master/slaves

Le maître EtherCAT utilise une interface Ethernet standard, ce n'est évidemment pas le cas des équipements esclaves !

AFDX : un Ethernet multicast.

Une autre approche plus respectueuse est basée sur l'encapsulation du protocole applicatif dans Ethernet, combinée à une utilisation du multicast. La technologie **A**vionics **F**ull-**D**uple**X** Switched Ethernet (AFDX [6]), qui remplace notamment les bus avioniques ARINC 429 et déjà mis en œuvre sur les Airbus A380 et A400M, est ainsi dérivée d'Ethernet. Les adresses MAC destination correspondent à une voie virtuelle (Virtual Link) à laquelle plusieurs nœuds peuvent être abonnés : il s'agit en quelque-sorte d'une émission « multicast » et la table de commutation de circuits virtuels dans les commutateurs AFDX est très proche d'une table de commutation multicast.

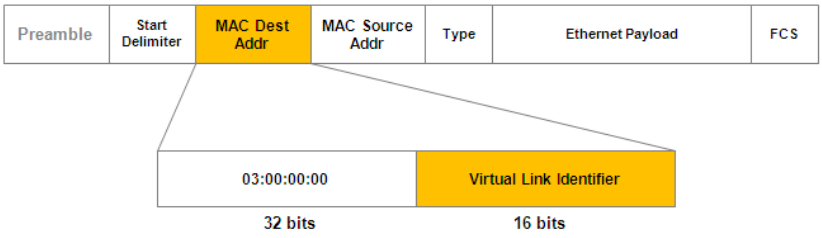


Fig. 3. Format d'une trame AFDX

AFDX précise également l'encapsulation du protocole IP et permet l'utilisation d'une adresse destination IP multicast pour identifier le Virtual Link (224.224.x.x). AFDX peut fonctionner avec des commutateurs Ethernet standards, notamment pour réaliser des tests sur plate-forme, mais la norme ARINC 664 intègre également des mécanismes de contrôle et de gestion des flux précisés sous forme d'un contrat de service (taille minimale et maximale, temps minimal entre deux trames…).

BACnet : UDP comme couche liaison !

D'autres protocoles ont également envisagé la possibilité de s'appuyer sur le protocole IP. BACnet [7], utilisé pour la gestion technique de bâtiments, s'adapte grâce à sa propre couche réseau à plusieurs supports : réseaux IEEE 802.2/802.3, Lontalk (réseau LonWorks), bus de communication MS-TP (Master-Slave/Token-Passing), liaison série RS-232 et même UDP (considéré comme une couche liaison !). L'encapsulation de BACnet dans UDP (dénommé BACnet/IP) fait ainsi apparaître un entête dénommé Virtual Link Control (liaison), un entête BACnet Network PDU (réseau) et enfin un BACnet Application PDU.

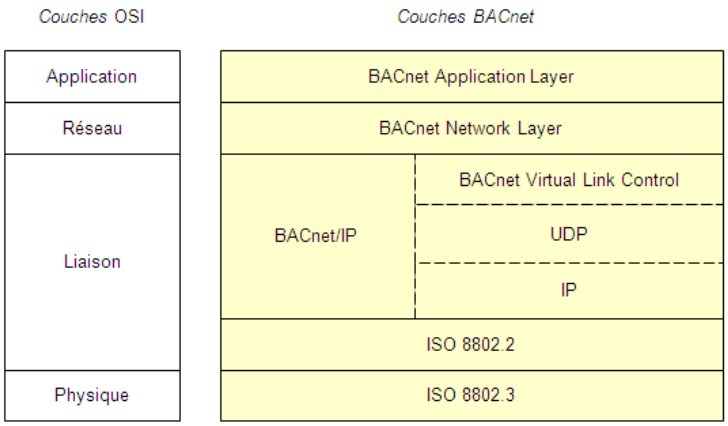


Fig. 4. Comparaison entre les couches OSI et le modèle BACnet/IP

L'utilisation du protocole BACnet sur IP a également amené le problème de l'utilisation du broadcast pour certains services du protocole BACnet entre différents réseaux BACnet. Ce service est offert par la couche réseau propre à BACnet (BACnet Network Layer). Au lieu d'implémenter la solution IP multicast, BACnet propose un équipement, appelé « BACnet/IP Broadcast Management Device », qui permet de relayer les messages broadcast vers les réseaux distants !

Des protocoles requête/réponse.

Enfin, certains protocoles basés sur un dialogue de type requête/réponse (ou maître/esclave) ont pu être transposés sans trop de difficulté sur TCP dans une approche client/serveur. C'est le cas de Modbus, avec sa déclinaison en Modbus TCP, ou encore du protocole S7 (Siemens), orienté connexion.

4 Interconnecter le tout

Dans beaucoup de situations, il n'est pas envisageable de migrer un bus existant vers Industrial Ethernet du fait d'un parc conséquent. Dans ce cas, des constructeurs

proposent des équipements d'interconnexion entre les différentes technologies réseaux. Il convient ici d'être très prudent sur la façon dont ces interconnexions sont réalisées, puisque là aussi les solutions sont multiples et variées.

Une solution assez classique exploite le positionnement central des automates dans un processus. Ceux-ci peuvent disposer de cartes de communications sur plusieurs bus, ce qui leur permet de questionner les différents capteurs et actionneurs sur chacun des bus avec les protocoles adaptés. Dans le domaine aéronautique, les informations peuvent être collectées sur un bus CAN par un calculateur, puis redistribuées par le réseau AFDX. D'autres solutions bénéficient de la transposition d'un protocole d'un support à l'autre. Ainsi des passerelles Modbus série/Modbus TCP permettent de changer de réseau sans modifier le protocole.

La traduction dynamique de protocoles semble difficilement réalisable, notamment par de fortes disparités entre les protocoles et les modes de dialogue. En général, la compatibilité entre les technologies est limitée aux variables manipulées. Ainsi, lorsque les primitives des protocoles permettent des opérations de lecture/écriture d'une variable, l'échange de données entre réseaux est possible en utilisant des tables de correspondance entre identifiants de variables (Babel Buster chez Control Solutions), des bases de données accessibles depuis plusieurs protocoles et réseaux (BradCommunications applicom GATEway), en simulant éventuellement un comportement maître ou esclave sur chaque segment (Anybus X-gateway de HMS Industrial Networks, SCADA Data Gateway de Triangle Microworks, Inc).

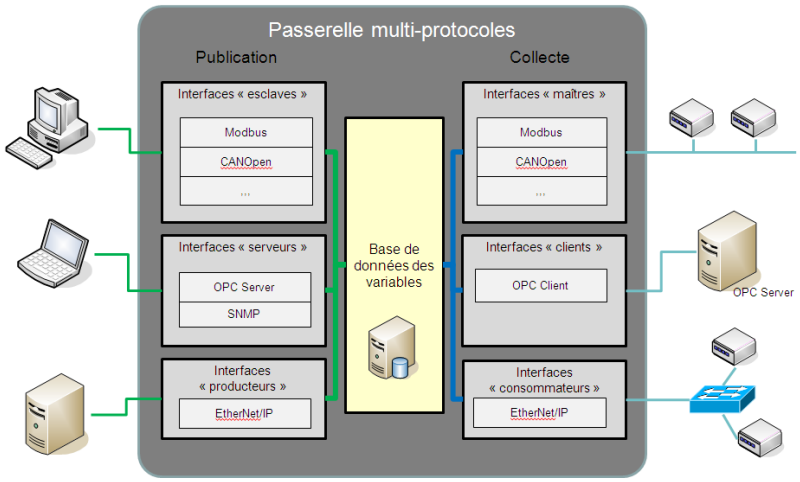


Fig. 5. Architecture d'une passerelle multi-protocole générique

Certaines passerelles permettent également de questionner les variables d'un bus de terrain Modbus série au travers du protocole SNMP à l'aide d'une traduction des registres Modbus en identifiants (OID) d'une MIB (PocketNet SNMP chez Adiscom).

5 Tirer profit des nouvelles fonctionnalités

Malgré les difficultés rencontrées lors de la migration des protocoles sur Ethernet, les constructeurs ont su également profiter du positionnement privilégié des commutateurs Ethernet et des nouvelles fonctionnalités disponibles.

Tout en restant transparent vis-à-vis des nœuds du réseau le commutateur assure un rôle d'arbitre en assurant le contrôle du flux et en les priorisant grâce à la norme IEEE 802.1p. Il a ainsi repris à son compte une partie des fonctions d'un arbitre de bus (producteur / consommateur) ou d'un maître (maître / esclave). Le mécanisme IGMP Snooping permet de contrôler la diffusion des flux multicast, notamment pour les protocoles basés sur le modèle producteur / consommateur.

L'utilisation de VLAN permet de créer des « bus de terrain » indépendants et reconfigurables logiquement. Elle permet également de séparer logiquement le réseau de contrôle (Control Systems Network) du réseau de terrain (Field Device Network), même si la séparation physique garantit un niveau de sécurité supérieur. La technologie VLAN n'a pas été conçue comme un mécanisme de sécurité : elle peut améliorer le cloisonnement mais elle ne doit pas être mise en avant notamment pour séparer le réseau informatique et le réseau industriel.

Les protocoles de gestion de la redondance sont également disponibles, soit sous leur déclinaison IEEE comme le Spanning Tree Protocol et ses multiples variantes, soit sous forme de protocoles simplifiés et plus rapidement convergents tel que Hi-PER Ring (Hirschmann), Media Redundancy Protocol (IEC) ou encore Resilient Ethernet Protocol (Cisco).

Enfin, l'intelligence embarquée des commutateurs Industriel Ethernet permet d'adapter leur comportement aux différentes approches d'encapsulation citées précédemment.

Parallèlement, la disponibilité d'outils pour Ethernet permet de faciliter l'analyse et la surveillance des protocoles. Des dissecteurs sont déjà disponibles pour Wireshark [9] ainsi que plusieurs publications associées [8].

6 Et la sécurité dans tout ça ?

Les mécanismes de sécurité déjà popularisés sur les commutateurs des systèmes d'informations sont disponibles et utilisables sur les commutateurs Industrial Ethernet et il serait dommage de ne pas en tirer parti. Le contrôle d'accès au réseau, au minimum par le contrôle de l'adresse MAC, le cloisonnement par VLAN et éventuellement des règles de filtrage basiques sont des recommandations de configurations et d'architectures qui, même si elles ne protègeront pas d'une cyber-attaque évoluée, permettront de contrer de nombreux incidents. Le support des mécanismes d'authentification IEEE 802.1x est également un avantage mais il nécessite l'intégration d'un protocole d'authentification et des paramètres associés dans chaque équipement.

Des équipements, tels que les passerelles, n'ont pas été conçus pour répondre à un besoin de sécurité mais leur mode de fonctionnement permet nativement de limiter les

primitives du protocole (par exemple, aux seules opérations de lecture et d'écriture d'une valeur d'un registre avec le protocole Modbus) et de filtrer les données accessibles depuis chacun des segments (une donnée non définie dans la table de traduction ne pourra pas être récupérée sur le segment Modbus à l'aide du protocole SNMP), du moins tant que la table de traduction n'est pas intentionnellement modifiée… Car ces produits n'ont pas été pensés comme des équipements sécurisés : la table de traduction est souvent transférée avec un protocole non sécurisé (FTP ou HTTP), le protocole SNMP lui-même est implémenté en version 1, sans modification possible du nom de communauté, l'interface web de configuration basique utilise classiquement le protocole HTTP.

Des pare-feux industriels sont également disponibles sur le marché. Ces équipements répondent à des normes de résistance pour des environnements contraignants et de sûreté mais une analyse rapide des documentations fait apparaître que ces produits ont surtout une connaissance des protocoles applicatifs issus du monde informatique (FTP, HTTP, SNMP, Telnet, SSH…). Il est même surprenant de découvrir que certains équipements annoncent des capacités d'analyse des protocoles de téléphonie comme SIP et H.323 ou de chat comme l'IRC, qui ne semblent pourtant pas des applications très répandues dans les systèmes industriels. Modbus semble être le seul protocole industriel parfois pris en compte, conséquence de la disponibilité de ses spécifications et d'un mode d'échange classique (d'un point de vue informatique). Les travaux réalisés en 2004 sur Modbus par Venkat Pothamsetty et Matthew Franz [12], et plus récemment en 2012 par Andrea Carcano et Igor Nai Fovino [13], ont ainsi abouti à une spécification et une implémentation d'un moteur d'analyse de Modbus.

L'implémentation de mécanismes de sécurité devra impérativement s'adapter aux spécificités des protocoles industriels. La compréhension du protocole permettra notamment d'identifier quels sont les critères pertinents pour assurer le contrôle ou la surveillance des flux. Le contrôle d'un protocole faisant largement usage de la diffusion multicast imposera l'analyse d'un critère supplémentaire comme l'identifiant de la variable demandée ou produite. De même le contrôle des échanges (« stateful ») devra prendre en compte par exemple les spécificités d'un mode d'échange de type producteur / consommateur et ne pas se limiter à un mode client / serveur. Enfin, le mécanisme de filtrage devra être le plus transparent possible, que ce soit au niveau de l'architecture qu'au niveau des temps de latence engendrés par les contrôles.

Avec le protocole IP, des protocoles de sécurité comme IPsec et SSL peuvent également être mis en œuvre pour assurer la protection des flux. Ces protocoles ne sont toutefois pas adaptés pour des échanges au niveau terrain du fait d'un usage multicast et de leur impact sur le volume des échanges. Le nombre d'équipements peut également constituer une limitation pratique à la distribution des clés et la négociation dynamique n'est probablement pas compatible avec la réactivité demandée au niveau d'un bus de terrain. La mise en œuvre de mécanismes cryptographiques devra ainsi être considérée en accord avec les choix d'architectures et les risques identifiés.

8 Conclusion et travaux à venir

La cybersécurité des systèmes industriels ne se limite pas aux réseaux et aux protocoles, mais ces derniers ne doivent pas pour autant être oubliés lors de la conception d'architectures robustes. La généralisation d'Industrial Ethernet et d'IP ne doit pas non plus laisser supposer que les solutions de sécurité issus des technologies informatiques pourront être appliquées à l'identique.

La sécurité de nos systèmes industriels nécessite aussi de mener plusieurs travaux sur les protocoles, les équipements, les mécanismes de sécurité adaptés et la conception d'architectures robustes.

DGA Maitrise de l'Information, en partenariat avec plusieurs écoles, centres de recherche, industriels de défense et organismes étatiques a ainsi lancé plusieurs thèmes d'études.

L'analyse des protocoles les plus répandus et la réalisation de dissecteurs permettra ainsi de mieux comprendre le fonctionnement des protocoles.

Les résultats de ces analyses permettront par la suite de spécifier au mieux les mécanismes de contrôle (cohérence protocolaire) et éventuellement de filtrage (pare-feu).

En complément, l'analyse dynamique d'un protocole et des flux ainsi que la caractérisation d'une empreinte comportementale permettra de renseigner les systèmes de détection d'intrusion. Le caractère déterministe et « physique » des systèmes industriels devrait en effet permettre de définir des modèles comportementaux prévisibles [14].

Enfin, l'étude des modèles de données et des passerelles pourra servir de base à la spécification de diodes travaillant uniquement sur les données et indépendantes des protocoles pour la phase de transfert des informations.

Tous ces travaux aboutiront à la conception d'architectures réseaux robustes contrôlant les échanges au point d'interconnexion et cloisonnant/isolant les zones les plus critiques, selon la philosophie du modèle ISA-99.

10 Références

1. *Introduction to Industrial Control Networks*. **Brendan Galloway and Gerhard P. Hancke**. 2012, Communications Surveys & Tutorials, IEEE, pp. 1-21.
2. *Real-Time Ethernet in Industry Automation*. [En ligne] http://www.realtime-ethernet.de/
3. PROFIBUS and PROFINET International. [En ligne] http://www.profibus.com
4. Open DeviceNet Vendor Association. [En ligne] http://www.odva.org
5. EtherCAT Technology Group. [En ligne] http://www.ethercat.org
6. *AFDX Training*. [En ligne] http://www.afdx.com
7. BACnet France. [En ligne] http://www.bacnetfrance.org/
8. *Analysing BACnet*. **Steve Karg**. BACnet Today, A Supplement to ASHRAE Journal. Novembre 2008. [En ligne] http://www.bacnet.org/Bibliography/BACnet-Today-08/Karg_2008.pdf
9. Wireshark Wiki, Protocol Reference, Fieldbus Protocol Family [En ligne] http://wiki.wireshark.org/FieldbusProtocolFamily
10. Industrial Ethernet Book. [En ligne] http://www.iebmedia.com
11. *Industrial Ethernet: A Control Engineer's Guide*. 2010, Cisco Systems Inc.
12. ModbusFW [En ligne] http://modbusfw.sourceforge.net/
13. *Modbus/DNP3 State-based Filtering System*. **Andrea Carcano, Igor Nai Fovino**. 2010, IEEE International Symposium on Industrial Electronics.
14. *Détection d'intrusion pour les systèmes industriels*. **Thomas Demongeot**. C&ESAR 2013.

Détection d'intrusion pour les systèmes industriels

Thomas Demongeot, DGA Maîtrise de l'Information

thomas.demongeot@intradef.gouv.fr

Abstract. Cet article présente un état de l'art des principaux travaux de recherche effectués dans le domaine de la détection d'intrusion pour les systèmes de contrôle commande industriels. Il présente en particulier un IDS (système de détection d'intrusion) placé sur un système d'exploitation proche de celui implémenté sur certains systèmes de contrôle commande (IDS Hôte). Cependant les IDS réseaux sont les plus communément développés dans le cadre des systèmes de contrôle commande. Si les IDS par signature sont majoritaires dans les systèmes d'information, du fait de certaines particularités des ICS (par exemple l'ensemble réduit d'utilisateurs et de protocoles utilisés, la simplicité de certains protocoles, la topologie simple des systèmes, des équations de contrôle des processus qui sont connues à priori,…) un modèle satisfaisant du fonctionnement normal d'un système de contrôle commande peut-être décrit et ainsi permettre de concevoir des IDS comportementaux pour ce type de systèmes. C'est pourquoi la plupart des travaux de recherche sur les IDS réseau pour les systèmes de contrôle commande se dirigent principalement vers cette voie.

Keywords: IDS (Intrusion Detection System, Système de détection d'intrusion), ICS (Industrial Control System, Système de Contrôle Commande Industriel), SCADA, Sécurité

1 Introduction

Les systèmes de contrôle industriels (1) (ou ICS : *Industrial Control System*) sont des systèmes destinés à assurer le suivi et/ou la conduite d'un procédé totalement ou partiellement automatisé. Ces systèmes reposent généralement sur l'utilisation d'un ou plusieurs automates programmables en réseau surveillant celui-ci à l'aide de capteurs et interagissant au moyen d'actionneurs.

On distingue deux catégories principales d'ICS :

- Les DCS (*Distributed Control System*) : qui sont chargés de la gestion d'un processus industriel, en transmettant les bonnes consignes aux actionneurs.
- Les SCADA (*Supervisory Control and Data Acquisition*) : qui sont chargés de la supervision distribuée destinée à contrôler des équipements dispersés géographiquement. Ils sont opérés depuis des centres de contrôle vers lesquels remontent les différentes informations du terrain, situation courante et alarmes. Ils gèrent des évènements pour revenir à l'état nominal.

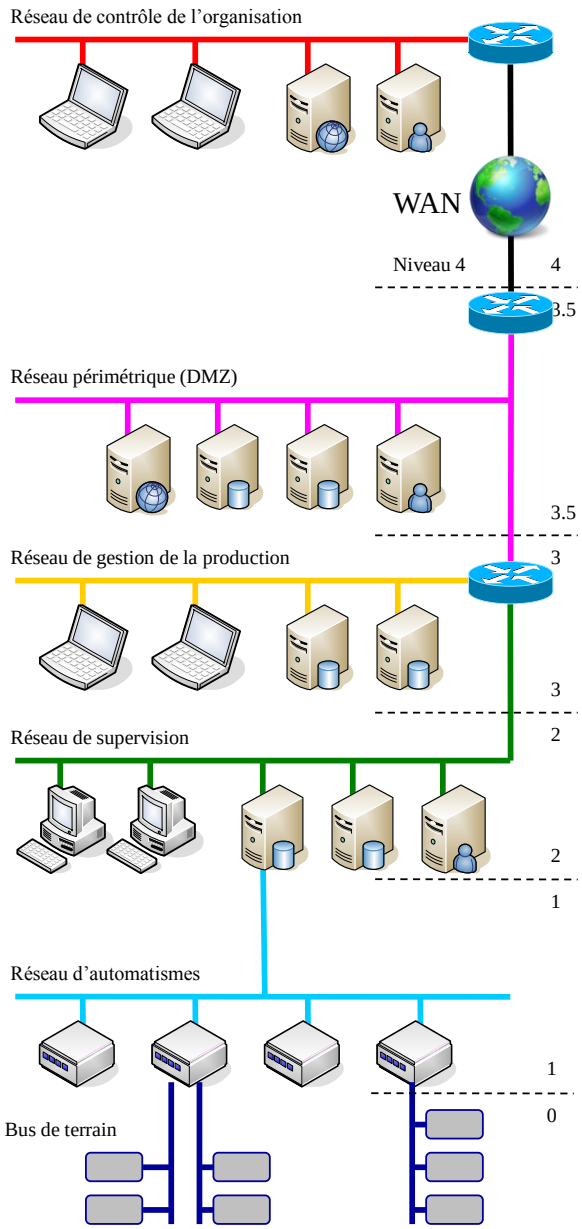


Figure 1. Exemple d'architecture d'un réseau de système de contrôle commande

Historiquement, les systèmes d'automatismes étaient bien isolés des réseaux extérieurs. Beaucoup de concepteurs et de dirigeants ont toujours tendance à considérer que leurs réseaux industriels sont isolés dans la mesure où ils ne sont pas censés être connectés directement à des réseaux publics dont Internet, ou à d'autres comme ceux de l'entreprise.

L'hypothèse de base selon laquelle de tels réseaux sont sécurisés (ou du moins peu vulnérables) car « isolés » est fausse. De très nombreux liens existent entre ces réseaux et les réseaux publics, qu'il s'agisse de transferts de périphériques, de branchements de postes de programmation, de configuration ou d'audit qui ont été directement ou indirectement connectés à ces réseaux.

La **Figure 1** présente un exemple d'architecture d'un réseau de système de contrôle commande. Le niveau 0 (processus) est constitué des différents appareils sous contrôle en contact direct avec le processus industriel mis en œuvre. Le niveau 1 (contrôle local) est constitué des équipements réalisant la première série de traitements, en contact direct avec les appareils de terrain. Le niveau 2 (supervision) regroupe les équipements permettant d'interférer avec le système. Le niveau 3 (gestion des opérations) est destiné à des opérations de plus haut niveau sur des infrastructures informatiques classiques. Le niveau 4 (entreprise) fait partie du réseau de l'entreprise ou de l'organisation en charge du ou des sites mettant en œuvre des systèmes automatisés. Il s'agit le plus souvent du réseau destiné à la conduite des opérations des différents sites, comprenant la logistique et l'organisation générale.

Prévenir l'ensemble des menaces pesant sur les systèmes et les réseaux n'est clairement pas possible et en particulier pour les systèmes de contrôle commande dont les évolutions matérielles et logicielles sont beaucoup plus lentes que l'évolution des technologies et des méthodes d'attaque. Surveiller ces systèmes est alors essentiel à la fois pour notifier rapidement qu'une situation dangereuse est en cours mais aussi pour mettre en œuvre dans certains cas des réactions automatiques (en particulier dans les cas de correction des erreurs).

La suite de cet article est organisée de la façon suivante. La section 2 présente les grands principes de la détection d'intrusion. La section 3 étudie les principales sources de données utilisées pour la détection d'intrusion pour les systèmes de contrôle commande. La section 4 présente les principales méthodes de détection d'intrusion réseau pour les systèmes de contrôle industriels. La section 5 présente quelques travaux liés à la corrélation et visualisation d'alertes pour les systèmes de contrôle industriels. Enfin la section 6 conclue cet article.

2 Détection d'intrusions

L'objectif principal de la détection d'intrusion est de détecter les activités illégales dans un système d'information et de les signaler à un opérateur. On appelle activité illégale dans un système d'information une intrusion, c'est-à-dire une violation de la politique de sécurité du système d'information en termes de confidentialité, intégrité

ou disponibilité. Les attaques sont l'ensemble des tentatives d'intrusion que celles-ci soient réussies ou non.

2.1 Fonctions d'une sonde de détection d'intrusions

La **Figure 2** présente les principales fonctions d'une sonde de détection d'intrusion (IDS : *Intrusion Detection System*) selon la description de l'IDWG (*Intrusion Detection exchange format Working Group*). Une sonde de détection d'intrusion est composée d'un ou plusieurs capteurs qui envoient les évènements qu'ils ont collectés vers un analyseur. Les capteurs reçoivent les informations qu'ils collectent d'une source de données qui est un sous-ensemble de l'activité générée sur un système vulnérable, c'est-à-dire un système qui subit des attaques. Les analyseurs détectent les occurrences d'intrusions (ou, bien souvent, les occurrences d'attaques) en comparant les évènements transmis par les capteurs avec un certain nombre de règles et qui génèrent des alertes en conséquence. Ces alertes sont alors transmises à un manager qui va permettre soit la visualisation des alertes directement par un opérateur soit la consolidation de ces alertes à l'aide d'autres informations (comme par exemple celles provenant d'autres capteurs, mais aussi les informations provenant d'une base de biens). Les deux fonctions principales d'une sonde de détection d'intrusion permettent de fournir une première classification des sondes de détection d'intrusion selon les sources de données utilisées par les capteurs et selon les méthodes de détection des intrusions utilisées par les analyseurs.

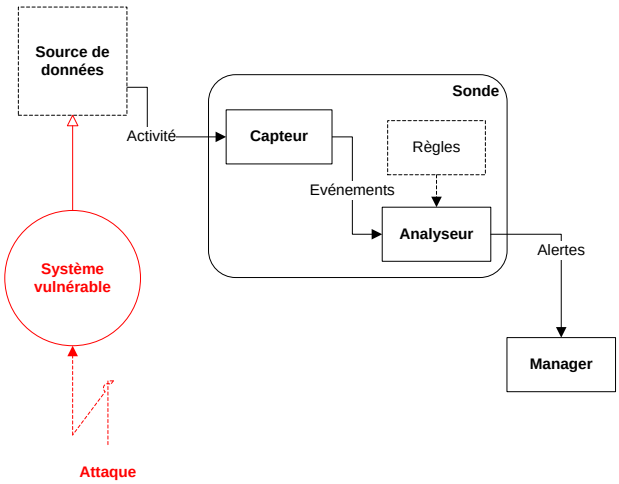


Figure 2. Les principales fonctions d'une sonde de détection d'intrusion (d'après (2))

Source de données des capteurs

On distingue principalement les IDS placés sur les hôtes (HIDS[1]) et ceux permettant de surveiller les réseaux (NIDS[2]). Cette distinction ne s'applique pas seulement à l'endroit où est placé l'IDS mais surtout aux informations collectées. Un HIDS est autonome et collecte les informations émises par un système d'exploitation ou une application. Un NIDS analyse quant à lui l'ensemble du trafic réseau.

Méthodes de détection des analyseurs

Deux approches sont possibles : les IDS par signatures se basent sur les actions générées par les attaques connues (par exemple le contenu des messages,…) alors que les IDS basés sur la détection d'anomalies recherchent les anomalies par rapport à un comportement normal ou attendu du système. Le comportement normal du système étant obtenu soit par apprentissage du système soit par spécification manuelle des caractéristiques du système.

2.2 Efficacité d'une sonde de détection d'intrusion

Les auteurs de (3) proposent de retenir cinq mesures afin de qualifier l'efficacité d'un système de détection d'intrusion : la pertinence, la complétude, la performance ainsi que la tolérance aux fautes et sa ponctualité. La tolérance aux fautes, c'est-à-dire la capacité du système de détections d'intrusion à résister aux attaques ainsi que la ponctualité, c'est-à-dire la capacité du système à propager l'information afin de permettre une réaction sont deux qualités indispensables d'un IDS cependant dans le cadre de cet article nous ne retiendrons que les trois critères suivants afin de qualifier l'efficacité des sondes de détection d'intrusion pour les systèmes de contrôle-commande.

La pertinence

La pertinence d'un système de détection d'intrusion est la capacité de ce système à ne pas produire de fausses alarmes (ou faux-positif), c'est-à-dire que le système ne produit pas d'alarme lorsque le système supervisé n'est pas attaqué.

La complétude

Un système de détection d'intrusions est dit complet s'il émet une alarme pour chacune des attaques se produisant sur le système. Il est caractérisé par l'absence de faux négatif, c'est-à-dire l'absence d'attaque non détectée.

[1] Host-Based IDS
[2] Network-based IDS

La performance

La performance d'un système de détection d'intrusion est caractérisée par la vitesse à laquelle les évènements sont analysés. Plus la performance d'un système de détection d'intrusion est faible moins celui-ci sera capable d'alerter en temps-réel.

La **Figure 3** présente les principales erreurs de détection d'un IDS. L'approche comportementale consiste à modéliser le comportement normal d'un système. Dans cette approche il est nécessaire de modéliser l'ensemble des actions légales du système. Une action illégale autorisée par le modèle de comportement normal va conduire à un faux négatif. A l'inverse une action légale non spécifiée dans le modèle de comportement normal va conduire à la production d'un faux positif. Dans les systèmes d'information, la modélisation de l'ensemble du comportement normal d'un système est un problème difficile. De ce fait les faux positifs sont relativement nombreux dans le modèle de détection comportemental.

A l'inverse l'approche par scénarios consiste à modéliser l'ensemble des actions illégales sur le système. Une action légale présente dans la base de signatures d'attaques va conduire à la production d'un faux positif. A l'inverse une action illégale non spécifiée dans la base de signatures va conduire à un faux négatif. La modélisation de l'ensemble des actions illicites d'un système est un problème difficile. De ce fait les faux négatifs sont relativement nombreux dans le modèle de détection par scénarios.

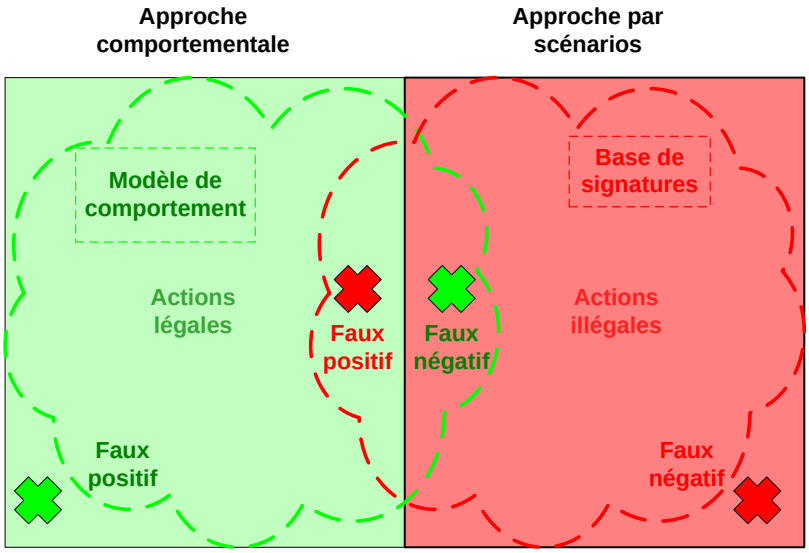


Figure 3. Erreurs de détection d'un IDS (d'après (2))

3 Source de données des capteurs

Les données utilisées par les IDS sont principalement de deux types : les données fournies par les différents équipements et systèmes (en particulier sous forme de logs ou de journaux d'activité), ainsi que les données provenant des échanges réseaux. Les données provenant des équipements et des systèmes sont peu utilisées dans le cadre des ICS du fait des contraintes et les limitations propres à ces systèmes ne permettent pas dans la plupart des cas d'importer directement les techniques issues des systèmes d'information. Cependant quelques travaux sont basés sur ces techniques que nous présentons dans la section 3.1. L'évolution actuelle des automates devrait conduire à des ressources disponibles accrues permettant la mise en œuvre d'IDS systèmes. Néanmoins la source de données la plus utilisée par les IDS dans le cadre des systèmes de contrôle-commande reste l'enregistrement des échanges réseaux. Cependant cette analyse reste le plus souvent difficile du fait de la multiplicité des protocoles réseaux utilisés par les systèmes de contrôle commande. Nous présentons quelques travaux liés à l'analyse de protocoles dans la section 3.2.

3.1 Détection d'intrusion système

Les systèmes SCADA permettent de contrôler l'état d'un système. A ce titre certains systèmes SCADA peuvent enregistrer plusieurs milliers d'évènements par jour. Ces évènements permettent d'enregistrer les évènements concernant l'activité des utilisateurs. Les auteurs de (4) proposent d'utiliser ces logs comme source de données d'un IDS. A cet effet c'est la sémantique des différents messages échangés qui est considérée et non seulement l'aspect protocolaire ou générique des attaques considérées. Cette approche est intéressante car elle est générique et s'appuie sur l'architecture de supervision fonctionnelle déjà présente sur les réseaux. Cependant cette approche ne peut permettre de se prémunir contre des attaques visant à modifier l'intégrité de la chaîne de supervision et en particulier à modifier les logs ou à les effacer. De plus les logs générés par les systèmes SCADA ont une visée fonctionnelle et non de sécurité.

Les HIDS quant à eux ont vocation à être placé directement sur les systèmes de façon à pouvoir les superviser directement. Cependant dans le cadre des ICS, le développement de tels ICS se heurte à deux contraintes : les faibles ressources de calcul disponibles sur les équipements terminaux (automates ou PLC par exemple), mais aussi aux fortes contraintes temps réel de ces systèmes. Néanmoins les auteurs de (5) proposent un HIDS pour les ICS. Cet HIDS a vocation à être positionné sur des périphériques de contrôle intelligent d'un réseau électrique. Ces périphériques servent à collecter et à contrôler les informations en provenance d'un certain nombre de capteurs. Les capacités de ces périphériques peuvent varier grandement : par exemple le SEL 3354[3] est équipé d'un processeur X86 à 1,6Ghz et peut embarquer un système

[3] http://www.selinc.com/WorkArea/DownloadAsset.aspx?id=6196

Linux. L'HIDS proposé permet de contrôler les appels système d'un noyau Linux afin de détecter les séquences d'appel utilisés par les malware. Cet HIDS nécessite une phase d'apprentissage afin de définir le comportement normal du système. Les résultats expérimentaux montrent un *overhead* de l'ordre de 5% et la détection d'un grand nombre de techniques utilisées par le *malware*. Néanmoins aucun test n'a été effectué sur un véritable ICS, les tests ayant été menés sur un Pentium 4 2 GHz avec 768 MO de RAM. De plus, aucun travail n'a été effectué sur la sécurisation de l'HIDS, celui-ci pouvant être utilisé comme base d'attaque par un malware.

Cependant, dans la plupart des cas, les automates ne peuvent être modifiés afin d'accueillir un HIDS ou ne présentent pas les ressources nécessaires à leur exécution. C'est pourquoi la plupart des travaux ce sont centrés sur le développement d'IDS réseaux pour les systèmes de contrôle commande.

3.2 Décodage des trames réseaux des systèmes industriels

Le principal problème de l'analyse réseau pour les ICS réside dans la multiplicité des protocoles réseaux utilisés. Les auteurs (1) de recensent plusieurs dizaines de protocoles différents. Ecrire des décodeurs pour l'ensemble de ces protocoles est une tâche complexe qui n'a pas encore été complètement effectuée.

Néanmoins les auteurs de (6) proposent développent un convertisseur MODBUS RTU/ASCII vers MODBUS TCP/IP permettant ainsi d'utiliser les règles SNORT développées pour MODBUS TCP/IP afin de détecter les attaques sur MODBUS RTU/ASCII. Le décodage de trame permet ainsi parfois de réutiliser les règles écrites pour un autre langage de trame.

Afin de permettre l'analyse des protocoles spécifiques aux ICS, Digital Bond (7) fournit des préprocesseurs pour les protocoles DNP3, ModBus et Ethernet/IP permettant l'analyse de ces protocoles par les règles SNORT.

D'autres auteurs, comme par exemple les auteurs de (8) ou (9), proposent d'analyser directement les flux réseau au niveau binaire sans décodage de protocole afin d'y déceler soit des anomalies soit des signatures d'attaques.

4 Détection d'intrusion réseau

4.1 IDS par signature.

La majorité des IDS commerciaux destinés aux ICS sont basés sur des signatures. Ainsi Digital Bond (7) fournit un ensemble de signatures pour des attaques sur des systèmes contrôle commande pour l'IDS réseau SNORT. Cet ensemble de signature correspond à la signature SNORT de vulnérabilités connues sur les systèmes de contrôle commande. Afin de permettre l'analyse des protocoles spécifiques aux ICS, Digital Bond fournit des préprocesseurs pour les protocoles DNP3, ModBus et Ether-

net/IP permettant l'analyse de ces protocoles par les règles SNORT. Ces règles ont pour la plupart été adaptée pour l'IDS réseau open-source SURICATA (10).

Les auteurs de (11) présentent un IDS Snort modifié permettant de surveiller un réseau simulé IEC 61850 (*automated electric substations*). Celui-ci se révèle capable de détecter des attaques en déni de service, ainsi que des attaques contre les mots de passe et la confidentialité. L'IDS est placé sur un port miroir et de ce fait n'a aucun effet sur les performances du système.

Cependant les IDS par signatures nécessitent la description précise des attaques. Du fait du domaine particulier des ICS peu de descriptions d'attaques sont disponibles et de ce fait la construction d'un IDS pour un protocole particulier part souvent de zéro. De la même façon un IDS par signature est incapable de détecter les attaques non connues à ce jour (*zero-day*). De ce fait les IDS par signature pour les systèmes de contrôle commande présentent un taux très important de faux négatifs.

Une autre approche de la détection d'attaque par signature consiste à analyser un protocole de communication afin d'en identifier les vulnérabilités intrinsèques ou le cadre d'emploi normal. De cette analyse en est extrait un certain nombre de signatures d'exploitation de vulnérabilités ou d'exploitation du protocole hors du cadre normal. Les auteurs de (12) proposent ainsi un ensemble de règles de détection d'intrusions pour MODBUS/TCP dérivées de l'analyse des vulnérabilités du protocole MODBUS. Les auteurs de (13) proposent un modèle de système normal qui repose sur une modélisation du protocole Modbus/TCP (format des trames, des charges utiles,…) ainsi qu'une modélisation des flux autorisés au sein du réseau (« qui est autorisé à communiquer avec qui »). Ils comparent ensuite le comportement du réseau avec ce modèle de comportement nominal. Ils ont développé à cet effet une version de SNORT modifiée mettant en œuvre leur modèle comportemental. Aucune évaluation détaillée des performances de l'IDS n'est fournie.

4.2 IDS par détection d'anomalies.

Certaines particularités des ICS (par exemple l'ensemble réduit d'utilisateurs et de protocoles utilisés, la simplicité de certains protocoles, la topologie simple des systèmes, des équations de contrôle des processus qui sont connues à priori,…) peuvent être exploitées afin de décrire un modèle satisfaisant du fonctionnement normal d'un système de contrôle commande et ainsi permettre de concevoir des IDS comportementaux pour ce type de systèmes. C'est pourquoi de nombreux travaux de recherche explorent cette piste.

Les auteurs de (14) proposent de classifier ces travaux suivant deux grands axes :

- les IDS avec état (*stateful IDS*) qui prennent en compte des informations au niveau du système (à ne pas confondre avec les *stateful firewall* qui prennent en compte l'état des connexions réseaux) ;
- les IDS sans état (*stateless IDS*) qui incluent toutes les autres approches.

Plus un IDS prend en compte d'informations plus il sera précis. A contrario il sera également plus consommateur de temps processeur et de bande passante. Ces aspects sont fondamentaux et doivent être pris en compte en fonction des situations.

IDS agnostique au système

Afin d'être agnostique au système supervisé et permettre néanmoins la définition d'un modèle de comportement normal, de nombreux auteurs proposent d'enregistrer un trafic supposé sain et de déduire le modèle de comportement normal de cet enregistrement. Le principal intérêt de cette méthode réside dans le fait que l'IDS est alors capable automatiquement de s'adapter à n'importe quel système. Cette méthode présente néanmoins deux limites importantes. Il est en effet difficile de s'assurer que le comportement d'un système est normal pendant la phase d'enregistrement et que ce comportement est exempt d'attaque. De plus si l'enregistrement est effectué dans un environnement que l'on sait être sain comment s'assurer que ce comportement est représentatif de l'utilisation du système en production.

Les auteurs de (15) et (16) enregistrent du trafic sur un réseau industriel et en exhibent un certain nombre d'invariants qui peuvent être utilisés afin de définir un comportement normal. Ils exhibent en particulier les invariants suivants : le débit, les adresses IP et ports utilisés, la taille moyenne des paquets, le temps e latence et la durée des flux, la durée moyenne des flux entre les terminaux, la forme et le contenu de la charge utile des paquets, l'association adresse MAC/IP, les protocoles réseaux utilisés, la configuration des protocoles, le nombre de connexions,… Ils ne fournissent cependant aucune implémentation d'un IDS utilisant ces invariants comme base de détection.

Les auteurs de (17) proposent un IDS permettant la détection d'anomalies sur un trafic périodique. Ils considèrent à cet effet le trafic sur un réseau d'ICS comme périodique. Ils adaptent à cet effet des outils venus de l'analyse spectrale et en particulier la transformée de Fourrier. Leur IDS est efficace face à des attaques qui provoquent la génération d'évènements inhabituels comme par exemple les attaques de découverte (scan de port par exemple), les attaques en déni de service ou les débordements de tampons,…

L'analyse N-Gram consiste à analyser un flux pour en déduire la probabilité d'apparition d'un N-Gram, c'est-à-dire une suite de N octets formant un mot. Les auteurs de (8) proposent d'adapter l'analyse N-Gram pour la détection d'intrusions. Ils testent en particulier leur méthode sur le protocole Modbus. Ils enregistrent pour cela un trafic d'un réseau de contrôle industriel normal supposé ne pas contenir d'alerte. Cet enregistrement a été effectué pendant une durée de 30 jours et contenait en particulier du trafic Modbus/TCP. Ils ont ensuite déduit de cet enregistrement une base de N-Gram. Ils ont ensuite comparé un trafic contenant des attaques avec cette base de n-gram suivant différents algorithmes. Les résultats sont très prometteurs. Avec certains algorithmes ils obtiennent des taux de détection de l'ordre de 96% avec

un taux de faux positifs très faible (de l'ordre de 0,00007%). Ces résultats sont liés au fait que le trafic Modbus est très prédictif et que les messages sont de 8 octets. L'analyse N-Gram semble donc très prometteuse dans le cadre de la construction d'IDS pour les systèmes de contrôle commande. Néanmoins cette analyse nécessite une période d'apprentissage et la base de n-gram nécessaire pour les algorithmes les plus précis (de l'ordre de 260 GB pour des 5-grams).

IDS prenant en compte l'état du système

Lorsque des informations concernant l'ensemble du système sont utilisées, les attaques et les fautes peuvent être détectées mais aussi prédites. Cela permet à l'IDS de raisonner non pas sur les mécanismes d'attaque mais sur les buts de l'attaquant. Ceci est particulièrement utile dans le cadre d'attaques qui modifient lentement l'état du système vers un état non-sûr. Ce type de menace n'est le plus souvent pas détecté lorsque seule la surveillance du trafic réseau est utilisée, alors que la détection est plus efficace lorsque l'ensemble des opérations sur le système sont prises en compte.

Les auteurs de (18) proposent de comparer l'état du système avec des situations potentielles non-sûres (par exemple un réservoir rempli au-delà d'une limite maximum avec les valves de sûreté fermées) clairement identifiées. En surveillant le trafic réseau, le statut des périphériques et leur configuration, l'IDS calcule une sorte de distance entre l'état courant du système et les situations non –sûres stockées en mémoire. Si la distance est plus faible qu'une certaine limite, une alarme est générée.

La validation de la technique a été effectuée sur un réacteur à vapeur simplifié. Performances et précision sont antinomiques. En effet, afin d'améliorer la précision, des informations précises sur l'état courant du système sont nécessaires ce qui génère un trafic réseau supplémentaire. Cela conduit à des pics de trafics qui affectent les nécessaires communications en temps réel. Dans un papier plus ancien (19) les auteurs présentaient l'implémentation de leur technique dans un réseau Modbus.

Les auteurs de (20) proposent de modéliser le fonctionnement d'un système SCADA sous la forme de *workflows* dans lequel ils identifient les branches « non sûres ». L'IDS capture les commandes envoyées aux systèmes de contrôle-commande et simule leur effet sur le *workflow* avant d'envoyer effectivement la commande si le chemin est jugé sûr. Les performances de l'IDS ne sont pas évaluées même si sa précision semble bonne.

Les auteurs de (21) et (22) ont développé un *framework* permettant d'extraire les informations nécessaires d'un modèle de communication à partir de fichiers décrivant un système de contrôle commande. Le modèle de communication est ensuite utilisé pour générer les fichiers nécessaires à la mise en œuvre d'un IDS comportemental. L'implémentation de leur IDS est basée sur SNORT. La principale contribution de leur papier consiste en l'utilisation des fichiers de configuration des automates afin de dériver les règles de détection d'intrusion.

Les auteurs de (23) proposent d'utiliser les fonctions de transfert des automates afin de pouvoir déduire les sorties de l'automate en fonction de l'entrée et inversement. Cette méthode est utilisée afin de détecter les attaques par le milieu visant à falsifier des données d'entrée ou de sortie.

Les auteurs de (24) proposent une approche de haut niveau mixant une analyse par signature et comportementale par modélisation du système. Ils cherchent à détecter l'utilisation de commandes qui sont licites la plupart du temps mais qui peuvent, en fonction de l'état du système, interrompre le comportement normal du système. Ils proposent à cet effet deux modèles de langage : un langage de signatures qui permet de décrire les paquets à surveiller et un langage permettant de décrire les états critiques du système pour lesquels une signature particulière doit-être activée. Ils proposent une implémentation de leur modèle pour les protocoles ModBus et DNP3. Les premiers tests présentés montrent que leur système est efficace pour des débits inférieurs à 180kb/s. Ils considèrent que ce débit est acceptable du fait de la faible bande passante utilisée dans les systèmes de contrôle industriels.

5 Corrélation et visualisation d'alertes

Nous avons présenté dans cet article un ensemble de travaux visant à développer des systèmes de détection d'intrusion pour les systèmes de contrôle commande. Cependant, dans la plupart des cas, il est nécessaire de coupler plusieurs IDS réseaux entre eux afin de maximiser la surface de détection. Les auteurs de (25), (26), et (27) présentent ainsi plusieurs modèles de distribution d'IDS réseaux permettant de couvrir à la fois le problème de la distribution des agents au sein d'un réseau de capteurs ((25), (26)) mais aussi le problème de la répartition et de la coopération des IDS réseaux entre les différentes couches du modèle de réseau de système de contrôle-commande présenté sur la **Figure 1.** Exemple d'architecture d'un réseau de système de contrôle commande (27).

Cependant afin de limiter le nombre de messages présentés à l'opérateur de supervision de la sécurité et de corréler les différentes alertes envoyées par ces outils il est nécessaire de mettre en œuvre des solutions de type SIEM (*Security Information and Event Manager*). Les auteurs de (28) ont proposé une utilisation du SIEM ArcSight dans le cadre d'un réseau de transport d'énergie. Ils ont en particulier centrés leurs travaux sur la détection, la corrélation et la visualisation d'une attaque réseau où un attaquant pénètre successivement les différentes couches du système de contrôle-commande afin de contrôler les automates critiques permettant de contrôler la distribution d'énergie. L'utilisation du SIEM permet en particulier de représenter sur un graphe l'évolution de l'attaque au cours du temps.

6 Conclusion

Nous avons présenté dans cet article quelques pistes de recherches utilisées dans le cadre de développement de systèmes de détection d'intrusions pour les systèmes industriels. Les principaux IDS pour les systèmes de contrôle commande développés par les industriels sont des modèles par signature d'attaques. Cependant le nombre de signatures d'attaques disponible pour les systèmes de contrôle commande reste aujourd'hui relativement faible par rapport au nombre de protocoles utilisés.

Malgré tout, certaines particularités des ICS (par exemple l'ensemble réduit d'utilisateurs et de protocoles utilisés, la simplicité de certains protocoles, la topologie simple des systèmes, des équations de contrôle des processus qui sont connues à priori,…) peuvent être exploitées afin de décrire un modèle satisfaisant du fonctionnement normal d'un système de contrôle commande et ainsi permettre de concevoir des IDS comportementaux pour ce type de systèmes. C'est pourquoi de nombreux travaux de recherche explorent cette piste.

L'analyse N-Gram (cf. (8)) semble une piste intéressante pour le développement d'IDS comportementaux dans le cadre des systèmes de contrôle commande néanmoins celle-ci nécessite une phase d'enregistrement d'un trafic représentatif sain difficile à obtenir et surtout à garantir. Il serait intéressant de développer des méthodes permettant de transformer une description de haut niveau du comportement attendu et spécifié du réseau en modèle de comportement normal utilisable par un IDS.

Un des problèmes de l'analyse comportementale est le compromis entre performances et précision. Plus le modèle théorique est complet, plus celui-ci prend de place en mémoire et plus les comparaisons occupent du temps processeur.

Un autre problème est lié à l'évolution actuelle des systèmes de contrôle commande. De plus en plus ces systèmes ont tendance à se rapprocher du monde des systèmes d'informations avec des systèmes de contrôle commande plus proche des ordinateurs personnels actuels que des automates. Dans le cadre de cette évolution le trafic réseau deviendra de moins en moins prédictif et de ce fait les modèles comportementaux seront aussi inefficaces que sur les systèmes d'information. Il conviendra alors de développer des HIDS pour les systèmes de contrôle commande.

Travaux cités

1. *Introduction to Industrial Control Networks.* **Galloway, B. et Hancke, G.** 2012, Communications Surveys & Tutorials, IEEE , pp. 1-21.

2. **Hiet, Guillaume.** *Détection d'intrusions paramétrée par la politique de sécurité grâce au contrôle collaboratif des flux d'informations au sein du système d'exploitation et des applications : mise en oeuvre sous Linux pour les programmes Java.* 2008. Thèse de Doctorat.

3. *A Revised Taxonomy for Intrusion Detection System.* **Debar, Hervé, Dacier, Marc et Wespi, Andreas.** 2000, Annales des Télécommunications.

4. *MELISSA: Towards Automated detection of Undesirable User Actions in Critical Infrastructures.* **Hadziosmanovic, Dina, et al., et al.** s.l. : IEEE, 2011. Seventh European Conference on Computer Network Defense.

5. *Intrusion detection for resource-constrained embedded control systems in the power grid.* **Reeves, Jason, et al., et al.** s.l. : Elsevier, 2012, International Journal of Critical Infrastructure Protection.

6. *A Retrofit Network Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems.* **Morris, Thomas, Vaughn, Rayford et Yoginder-, Dandass.** s.l. : IEEE, 2012. 45th Hawaii International Conference on System Sciences. pp. 2338-2345.

7. **Digital Bond.** Quickdraw SCADA IDS. *Digital Bond.* [En ligne] http://www.digitalbond.com/tools/quickdraw/.

8. *N-Gram against the Machine: On the Feasibility of the N-Gram Network Analysis for Binary Protocols.* **Hadziosmanovic, Dina, et al., et al.** [éd.] S. Stolfo and M. Cova D. Balzarotti. s.l. : LNCS, 2012. RAID 2012. Vol. 7462, pp. 354-373.

9. *Denial of service attacks on network-based control systems: impact and mitigation.* **Long, Men, Wu, Chwan-Hwa et Hung, John Y.** 2, s.l. : IEEE, May 2005, IEEE Transactions on Industrial Informatics, Vol. 1.

10. [En ligne] http://www.digitalbond.com/blog/2011/03/28/quickdraw-scada-ids-signatures-on-emerging-threats-pro/.

11. *An Intrusion Detection System for IEC61850 Automated Substations.* 4, Octobre 2010, IEEE Transactions on Power Delivery, Vol. 25, pp. 2376-2383.

12. *Deterministic Intrusion Detection Rules for MODBUS Protocols.* **Morris, Thomas, et al., et al.** 2013. 46th Hawaii International Conference on System Sciences. pp. 1773-1781.

13. *Using model-based intrusion detection for SCADA networks.* **Cheung, S., et al., et al.** 2007. Proc. SCADA Security Symposium. pp. 1-12.

14. *Review of Security Issues in Industrial Networks.* **Cheminod, Manuel, Durante, Lucas et Valenzano, Adriano.** 1, February 2013, IEEE Transactions on Industrial Informatics, Vol. 9, pp. 277-293.

15. *Feature Selection for Machine Learning Based Anomaly Detection in Industrial Control System Networks.* **Mantere, Matti, Sailio, Mirko et Noponen, Sami.** 2012. IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing.

16. *Challenges of Machine Learning Based Monitoring for Industrial Control System Networks.* **Mantere, Matti, et al., et al.** 2012. 26th International Conference on Advanced Information Networking and Applications Workshop.

17. *Towards Periodicity Based Anomaly Detection in SCADA Networks.* **Ramos, Rafael, et al., et al.** s.l. : IEEE, 2012.

18. *A multidimensional Critical State Analysis for Detecting Intrusion in SCADA Systems.* **Carcano, A., et al., et al.** 2, May 2011, IEEE Transactions on Industrial Informatics, Vol. 7, pp. 179-186.

19. *State-Based Network Intrusion Detection Systems for SCADA Protocols: A Proof of Concept.* **Carcano, Andrea, et al., et al.** s.l. : LNCS, 2009. Proc. of CRITIS 2009. Vol. 6027, pp. 138-150.

20. *A workflow-based non-intrusive approach for enhancing the survivability of critical infrastructures in cyber environment.* **Xiao, Kun, et al., et al.** s.l. : IEEE, 2007. Third International Workshop on Software Engineering for Secure Systems (SESS'07).

21. *Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration.* **Hadeli, Hadeli, et al., et al.** [éd.] IEEE. 2009. Proc. 14th IEEE Int. Conf. Emerging Technol. Factory Automation. pp. 1-8.

22. *Generating Configuration for Missing Traffic Detector and Security Measures in Industrial Control Systems Based on the System Description Files.* **Hadeli, Hadeli et Schierholz, Ragnar, Braendle, Markus, Tuduce, Cristian.** s.l. : IEEE, 2009.

23. *A transfer Function based Intrusion Detection System for SCADA Systems.* **Papa, Stephen, Casper, William et Nair, Suku.** s.l. : IEEE, 2012.

24. *Modbus/DNP3 State-based Intrusion Detection System.* **Fovino, Igor Nai, et al., et al.** s.l. : IEEE, 2010. IEEE International Conference on Advanced Information Networking and Applications.

25. *A Distributed Intrusion Detection System for Industrial Automation Networks.* **Schuster, Franka et Paul, Andreas.** s.l. : IEEE, 2012.

26. *Multi-Agent Intrusion Detection System in Industrial Network using Ant Colony Clustering Approach and Unsupervised Feature Extraction.* **Tsang, Chi-Ho et Kwong, Sam.** s.l. : IEEE, 2005.

27. *Detecting Cyber Intrusions in SCADA Networks Using Multi-Agent Collaboration.* **Shosha, Ahmed F., et al., et al.** s.l. : IEEE.

28. *Detection, Correlation, and Visulisation of Attacks Against Critical Infrastructure Systems.* **Briesemeister, Linda, et al., et al.** s.l. : IEEE, 2010. Eight Annual International Conference on Privacy, Security and Trust.

29. *Possibilistic Decision Trees for Intrusion Detection in IEC61850 Automated Substations.* **Premaratne, Upeka, Ling, Charles, Samarabandu, Jagath et Sidhu, Tarlochan.** 2009. Fourth International Conference on Industrial and Information Systems.

30. *Real-Time Intrusion Detection in Power System Operations.* **Valenzuela, Jorge, Wang, Jianhui et Bissinger, Nancy.** 2, 2013 : s.n., IEEE Transactions on Power Systems, Vol. 28.

Sécurité informatique des systèmes de contrôle industriels

Détection et Surveillance au niveau des équipements et du bus de terrain.

Jean-Michel Brun –Architecte senior en sécurité informatique - Schneider Electric
Laurent Platel - Architecte en sécurité informatique - Schneider Electric
Fabrice Tea – Développeur offre services cyber-sécurité - Schneider Electric

jean-michel.brun@schneider-electric.com

Résumé :

Les systèmes industriels (habituellement appelés OT de l'anglais Operationnal Technology) et particulièrement les Systèmes de Contrôle Industriels (SCI) ont toujours privilégié la robustesse (disponibilité, sécurité fonctionnel…) et la performance à toute autre considération. Il est donc encore plus important de surveiller le système du point de vue sécurité informatique. Les solutions actuelles de surveillance de sécurité commencent à prendre en compte les applications logicielles comme le SCADA. Il est essentiel d'aller plus loin en établissant aussi une surveillance au niveau des équipements tout en tenant compte des spécificités du bus de terrain et des systèmes et architectures industrielles. En effet, ces architectures ont montré des incompatibilités avec les solutions de sécurité informatiques standards suite aux exigences de déterminisme et de disponibilité de ces systèmes industriels ainsi qu'à leurs contraintes ressources.

Ce présent document expose d'une part, les besoins de surveillance et d'autre part, les spécificités d'un Système de Contrôle Industriel) que les solutions de surveillance de sécurité doivent prendre en compte pour apporter leur pierre à « l'édifice » de la sécurité du monde OT.

Ce document se focalisera particulièrement sur le Niveau 2 (Procédé) d'un Système de Contrôle Industriel, qui pilote le procédé de production.

La présentation, lors des journées C&ESAR 2013, inclura une vidéo montrant des scénarios d'attaques détectés par la surveillance au niveau des équipements industriels.

1 Le contexte des Systèmes de Contrôle Industriel (Rappel)

1.1 Le contexte de sécurité informatique

La sécurité informatique n'est plus une exigence secondaire dans le monde du contrôle industriel contemporain.

Les systèmes de contrôle industriel(SCI), basés sur des technologies informatiques et des réseaux de qualité industrielle, sont en usage depuis des décennies. Les premières architectures de système de contrôle furent développées avec des technologies propriétaires et étaient isolées du monde extérieur. Très souvent, la protection des accès physiques était jugée suffisante et la sécurité informatique n'était pas une préoccupation majeure.

Aujourd'hui, de nombreux systèmes de contrôle utilisent des technologies répandues ou ouvertes et standardisées tels que les systèmes d'exploitation Windows© de Microsoft™, les réseaux de technologie Ethernet TCP/IP et la technologie Web pour réduire les coûts et améliorer les performances. De nombreuses architectures utilisent également la communication directe entre les systèmes de contrôle industriel et les systèmes de gestion d'entreprise pour améliorer l'efficacité opérationnelle et la rentabilité des actifs de production.

Cette évolution technique expose les systèmes de contrôle industriel aux menaces qui ciblent les applications IT et le réseau bureautique de l'entreprise. A ces menaces héritées des technologies du monde IT, Stuxnet et ses dérivés ajoutent une menace spécifique et très avancée (type APT Advanced Persistent Threat) dédiée aux systèmes de contrôle industriel, qui sont désormais vulnérables à des attaques « internes » (attaques ciblant spécifiquement les technologies de l'OT) et « externes » (les attaques ciblant les technologies de l'IT).

Le succès de la connectivité Ethernet/Internet peut amener aussi à « passer outre » les règles élémentaires de sécurité et privilégier la facilité (de maintenance par exemple) en connectant directement les systèmes SCI sur Internet, là ou il y avait auparavant l'utilisation de liaison spécialisée pour la surveillance et la maintenance à distance et donc comportant des risques de sécurité beaucoup plus faibles.

La sécurisation des systèmes industriels passe donc par une compréhension poussée de leurs spécificités et de leurs contraintes.

Parmi les défis de la sécurité dans le monde du contrôle industriel, citons :

- La multiplicité des frontières logiques et physiques : un système de contrôle industriel est composé d'équipements très différents, sur des réseaux de technologie et de capacités différentes, utilisant des protocoles variés et véhiculant des données variées.
- Des architectures couvrant plusieurs sites sur de larges zones géographiques
- Les effets indésirables de la mise en œuvre de la sécurité sur la disponibilité des processus

- L'ouverture au web des réseaux de communications de l'entreprise (informatique mobile, BYOD, réseaux sociaux) qui augmente l'exposition aux virus et vers, qui peuvent migrer du réseau d'information au réseau de contrôle
- L'exposition croissante aux logiciels malveillants par l'usage accru des lecteurs portables (clef ou disque USB), d'ordinateurs portables (service technique, fournisseur de services) et des réseaux sans-fils.
- L'impact direct des systèmes de contrôle sur les systèmes physiques et mécaniques, qui peut induire des risques sur la sécurité physique des personnes.

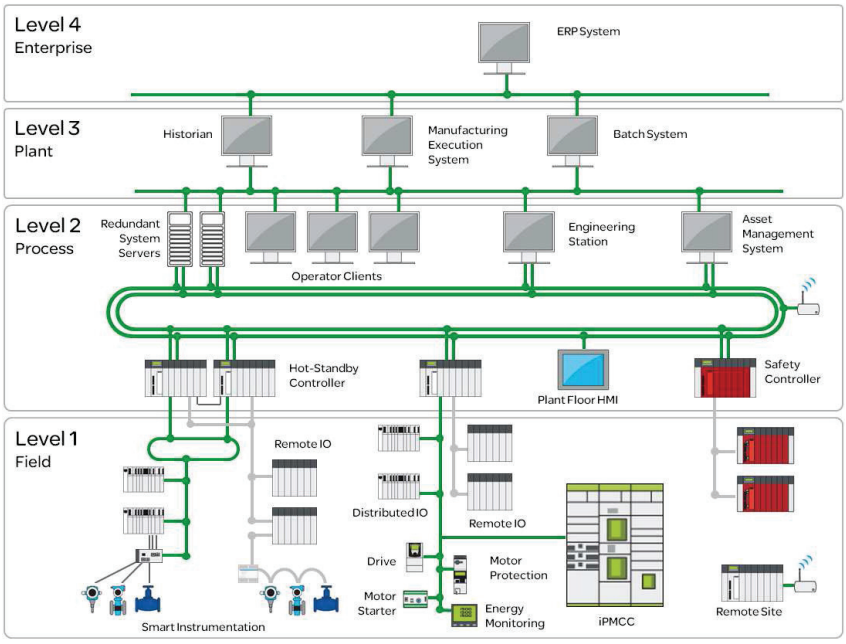
La mise en place d'un firewall n'a jamais été suffisante pour garantir la sécurité des installations industrielles. Par une approche de défense en profondeur, les entreprises doivent être vigilantes dans le choix des mesures à prendre pour sécuriser ces installations: une attaque informatique peut entraîner une perte de production, une atteinte à l'image de l'entreprise, une catastrophe écologique et dans le pire des cas, des pertes humaines. Sur cette approche, le contrôle industriel doit s'inspirer des leçons tirées du monde IT.

Mais, comme nous l'avons démontré dans une autre publication C&ESAR 2013 intitulé « *Cyber Sécurité des systèmes de Contrôle Industriel : Les spécificités des SCI, un challenge pour leur sécurité* », les solutions de sécurité informatique qui ont été normalisées pour le monde IT, ne peuvent pas entrer facilement dans le monde OT et particulièrement les systèmes de contrôle industriel.

.

1.2 Description d'un Système de Contrôle Industriel (rappel)

La norme ISA95 a pour but de fournir un modèle d'entreprise qui contient les fonctions de gestion et de production. Le modèle définit plusieurs niveaux, chaque niveau est dédié à une fonction différente, avec des contraintes différentes.



Niveau 1 (Level 1 Field): le niveau bus de terrain est dédié au contrôle (mesure) et à la commande du Procédé de production.

Niveau 2 (Level 2 Process): le niveau Procédé est dédié à la surveillance et prise de décision du système de production, donc il pilote les équipements du Niveau 1. A l'intérieur de ce niveau Procédé, on peut identifier deux sous-niveaux :

- Le niveau SCADA (Supervisory Control and Data Acquisition) qui affiche l'état du processus à l'aide de représentations graphiques, gère les alarmes, enregistre les données recueillies et assure la conduite du Procédé.
- Le niveau Automate (PLC : Programmable Logic Controller) qui effectue le contrôle automatisé du Procédé. Il prend en entrée les données fournies par les équipements du niveau 1, des IHM (petits terminaux graphiques permettant la saisie de valeurs par un utilisateur), ou du SCADA et il calcule ces informations pour générer des commandes à travers ses sorties.

Niveau 3 (Level 3 : Plant): le niveau Usine est dédié à la gestion et la répartition de la production en fonction de la charge des ateliers, des recettes de production (généralement via un système MES /Manufacturing Execution System).

Niveau 4 (Level 4 Enterprise) : le niveau Entreprise a pour mission :

- De planifier la production en fonction des commandes des clients
- De gérer les commandes de matériels et matières premières
- De gérer la livraison au client et la logistique en général

Remarque: ISA 95 est une norme internationale pour développer une interface automatisée entre les systèmes de contrôle et l'entreprise. Il est utilisé dans ce document pour illustrer les différentes couches d'applications et de dispositifs de commande industriels. Ainsi, ISA 95 n'est pas pertinente pour décrire d'autres systèmes industriels tels que les systèmes électriques ou le « Smart Grid ».

2 Pourquoi la surveillance est si importante pour les systèmes de contrôle industriel

L'idéal est de prévenir, mais la détection est essentielle
(SANS Institute – Defense In Depth –v.2013)

Le principe de défense en profondeur doit être appliqué pour sécuriser n'importe quel système. Des vérifications régulières et des tests de pénétration doivent être planifiés pour vérifier le niveau de sécurité du système. Une fois les mesures de sécurité informatique mises en place, il est obligatoire de surveiller le système sinon le propriétaire du système est sans visibilité sur le niveau de sécurité réel.

Rappelons que Les experts en sécurité informatique estiment que les hackers peuvent casser une nouvelle technologie de sécurité en 5 ans !

Dans le cas des Systèmes Industriels, du fait de la grande quantité d'équipements, de leur faible niveau de sécurité et de l'évolution constante de leurs applications, configurations ou systèmes, il est primordial de surveiller tout événement dans l'architecture afin :

- d'évaluer le niveau de sécurité actuel
- de détecter tout comportement anormal des équipements
- d'être en mesure de faire la différence entre un état exceptionnel de l'application / système et une attaque sur l'application / système

3 Les besoins de surveillance au niveau des équipements.

En tirant parti des analyses du fonctionnement de Stuxnet, nous pouvons identifier des besoins de surveillance et de détection au niveau des équipements, et dans l'idéal, entre les équipements et les capteurs/actionneurs.

Les paragraphes suivants présentent les fonctions de surveillance qui sont importants à mettre en œuvre, en se focalisant au niveau des équipements, bien qu'elles soient applicables pour la plupart au superviseur SCADA.

3.1 Surveillance de l'intégrité et gestion du changement

Surveiller l'identité des équipements (numéro de série).

Le scénario requiert un accès physique à l'équipement, ce qui le rend délicat. Mais, il n'est pas impossible que, lors d'une action de maintenance préventive ou curative, un équipement soit remplacé par un autre équipement illégitime.

Pour prévenir ce scénario, il est nécessaire de détecter tout changement de matériel.

La détection automatique du changement de matériel permettrait aussi de faciliter la maintenance et plus précisément la traçabilité des actions de maintenance.

Cette identité et type de l'équipement va aussi permettre d'établir une liste des services réseaux et des données sensibles utilisées/gérées par l'équipement à surveiller.

Cette identité peut être plus complexe à gérer si l'équipement est modulaire et permet une flexibilité fonctionnelle.

Surveiller l'accessibilité / disponibilité de ses appareils.

La disponibilité des équipements d'un système de contrôle industriel est primordiale à son bon fonctionnement. Il est d'ailleurs communément accepté que, dans le domaine industriel, la disponibilité prévale dans le triptyque traditionnel de la sécurité (confidentialité, intégrité, disponibilité)

Il est alors important de surveiller l'accessibilité et la disponibilité des équipements à tout instant.

Surveiller les évolutions.

La gestion des versions logicielles est tout aussi importante, sinon plus importante dans le monde industriel que dans le monde informatique.

Par exemple, le programme applicatif d'un automate programmable est développé et testé avec des logiciels / firmware de l'équipement correspondant à une certaine(s) version(s) : L'utilisation de ces programmes applicatifs avec d'autres versions logicielles / firmware pourrait avoir des conséquences inattendues (comportement différent, dysfonctionnement…) dues à des différences entre les versions.

La longue durée de vie des systèmes de contrôle industriel est un véritable challenge pour la gestion de ces compatibilités et la prise en compte de tous les cas.

Il est aussi nécessaire de connaître les versions logicielles utilisées afin de détecter les versions comportant des vulnérabilités majeures de sécurité. La gestion des mise à jour logiciel/firmware sera à traiter au cas par cas selon la criticité et les contraintes de

disponibilité et de fonctionnement des systèmes industriels (exemple d'équipements d'automatismes qui fonctionnent 24 heures sur 24, contrôlant un procédé qui ne doit pas arrêté).

Il est alors important de surveiller les versions logicielles déployées sur site.

Surveiller l'intégrité

Les équipements d'un système de contrôle industriel sont programmés pour accomplir des tâches précises (ouverture de vanne par exemple) sous des conditions précises (niveau de fluide atteint par exemple)

Il est alors important de détecter toute modification malicieuse de ces programmes.

Détection d'une liste d'actions sensibles.

Les systèmes de contrôles industriels pilotent des équipements mécaniques ou électriques qui assurent un service rendu tout en respectant des contraintes de sécurité (notamment la protection des personnes), contraintes environnementales ou de qualité.

Certaines actions ou commandes (par exemple, une commande d'arrêt ou une modification des paramètres de configuration) de ces systèmes peuvent alors impacter tout ou partie de ces éléments. Il est alors important d'identifier ces actions sensibles et de surveiller leur utilisation.

3.2 Détection d'attaque

La détection des attaques passe d'abord par la connaissance des scénarios classiques d'attaques. Pour cela, il faut constituer une base avec les incidents connus, analyser les faiblesses exploitées, et placer des mesures et règles de corrélations en face de ces exploits. Le monde IT a développé une communauté active pour ces phases de compilation et de d'analyse. Cela permet d'enrichir rapidement les outils de surveillance, et de maintenir un haut niveau de sécurité.

Le monde OT n'a pas encore atteint cette maturité, et le simple recueil des incidents s'avère une tâche délicate, la publication des incidents n'est pas obligatoire en France (contrairement aux Etats-Unis), et les habitudes de redémarrage au plus vite de l'industrie permettent rarement de mener une analyse de l'incident. Les outils repris du monde IT permettent de détecter les attaques connues ciblant des services réseau Ethernet et services Web du système industriel par exemple, mais ils ne couvrent qu'une faible partie des fonctions exposées par le système de contrôle. La protection des services purement OT reste à étudier, et la communauté est à créer.

Il nécessite pour cela d'avoir une connaissance de la logique du protocole et de la logique de l'application de contrôle industriel.

Il convient aussi d'améliorer la capacité de trace (log) de type sécurité pour enregistrer tout événement ou toute action au niveau des équipements.

4 Pourquoi les solutions de surveillance IT ne satisfont pas les exigences des SCI et quelles sont les spécificités à prendre en compte?

Reprenant la classification faite en début de document, le Niveau 2 qui est étudié ici, se découpe en Niveau 2 Superviseur (SCADA) et Niveau 2 Equipements (Automates/PLC,...).

Les paragraphes suivants vont analyser les fonctions de surveillance au niveau d'un SCADA puis au niveau des équipements, et enfin au niveau de la communication.

4.1 Surveillance des SCADA

Pour répondre aux besoins définis dans le chapitre précédent, le système de surveillance a besoin de se connecter et d'échanger des données avec le SCADA et les automates. Comme le SCADA est généralement basé sur du matériel informatique standard et des systèmes Windows©, on peut dire que les solutions existantes (SIM, SEM ou SIEM) comme AlienVault, Splunk, QRadar, Security Manager Enterprise, conçues pour l'IT et sa technologie, sont une solution possible pour surveiller les SCADA.

Ces solutions devront être adaptées pour couvrir les besoins et les challenges décrits dans les paragraphes suivants.

Surveiller l'identité des postes SCADA.

Ce sont en général des postes sous Windows© ou Windows© Server, disposant de grandes capacités de traitement. Il peut y avoir un antivirus, mais la mise à jour n'est pas fréquente.

La présence d'un agent local d'un SIEM est possible, mais il n'y a pas de publication de compatibilités. Les impacts d'un SIEM agent sur le système sont à étudier, que ce soit les impacts sur la performance ou les impacts sur l'exécution de batch déclenchés par le SCADA lors de circonstances exceptionnelles (gestion de crise par exemple). Le blocage d'un de ces batch ou utilitaire n'est pas envisageable au regard des contraintes de disponibilité du système.

Surveiller l'accessibilité des postes SCADA.

La surveillance d'un poste Windows© est à la portée d'un SIEM.

Cependant, les SCADA sont souvent redondés, c'est-à-dire que 2 postes sont organisés pour assurer la fonction SCADA elle-même, un des poste est en mode actif, l'autre est en mode secours (Stand-by) dans le cas où le premier 'disparait', le tout utilisant des protocoles d'échange propriétaire. La fonction à surveiller est alors un couple de PC, plus qu'un poste unique. Ce n'est pas trivial avec un SIEM classique.

Surveiller l'évolution des postes SCADA.

Surveiller et journaliser les installations ou les mises à jour du système d'exploitation, surveiller et journaliser les installations et mise à jour des applications (SCADA, SQL Server,…), surveiller les ressources utilisées (charge des processeurs, occupation RAM, bande passante sur les cartes réseaux,…) est dans le domaine des SIEM.

Cependant, certains protocoles spécifiques utilisés (OPC, OPC-UA) au niveau du SCADA (ou les réseaux non IP) ne seront pas surveillés par ces outils.

Surveiller l'intégrité des postes SCADA.

L'intégrité de ces postes est à la portée des SIEM classiques : En effet, l'intégrité d'application peut être gérée par la fonction AppLocker de Windows© ou par l'agent du SIEM ; certains systèmes d'exploitation sont capables de vérifier eux-mêmes leur intégrité.

Il reste à remplir les conditions que l'installation d'un agent doit être compatible avec les performances du système SCADA, et que les options de démarrage sécurisé soient activées sur ces postes.

Détecter les actions sensibles.

Redémarrage sauvage (pour forcer le basculement avec le Standby), restauration de vieux paramètres (merci à l'outil Registry Recovery dans l'environnement Windows©) : Ce sont des modifications qui peuvent être gérées par un SIEM.

Mais le logiciel SCADA contient lui aussi une configuration complexe et précise, dont la modification peut gravement nuire à la disponibilité du SCADA et des données. Il faut prévoir un agent ou un script capable de surveiller les actions faites par un utilisateur du SCADA à l'intérieur du SCADA, afin de couvrir réellement le spectre des actions malveillantes.

Détection des attaques.

Les SCADA comportant des services classiques, les outils du monde IT vont pouvoir assurer une détection des attaques sur les services Web, les vulnérabilités connues du système d'exploitation ou de la base de données. Par contre, une attaque DoS sur les ports spécifique de gestion de la redondance lui échappera. Ces protocoles et ces ports sont propriétaires, parfois sur un autre réseau IP. Il faut donc prévoir une installation spécifique et des scripts ou paramètres spécifiques pour pouvoir détecter ces comportements.

4.2 Surveillance des Equipements/Automate.

Nous avons répété que les automates (PLC) sont basés sur des technologies spécifiques, absentes des réseaux informatiques classiques.

La connexion à ces équipements nécessitent des protocoles spécifiques, et souvent propriétaires. Le protocole Modbus, exemple bien connu, est utilisé pour échanger les données du procédé, et ne peut pas être utilisé directement pour échanger des informations sur l'état du PLC. Cet état n'est accessible que par des jeux de requêtes spécifiques à chaque équipement. En effet, la récupération des informations nécessaires (numéro de version du matériel ou du logiciel, par exemple) nécessite la compréhension de la structure mémoire de l'équipement (les informations sont stockées différemment dans chaque modèle).

Les SIEM classique sont aveugles à ce niveau. Certes, quelques uns (Industrial Defender, par exemple) connaissent des protocoles propriétaires et sont capables de récupérer des données à partir de l'adressage mémoire propre à chaque gamme de d'équipements (PLC,…). Mais la gamme d'équipement couverte est faible pour l'instant.

Surveiller l'identité des postes équipements/Automates.

Ces équipements possèdent des informations d'identités propres à chaque gamme d'équipement. Le tout est d'accéder à ces infos, par des requêtes spécifiques sur des protocoles industriels. On peut citer :

- Numéro de série
- MAC adresse pour les équipements TCP/IP
- Version du firmware
- Version d'application
- Services actifs : ce ne sont pas des services IT. Certes on peut trouver un port 80, mais il y a aussi des ports 502, 1089, 2000, 2222, 3840, 47808,44818, selon les protocoles (industriels ou propriétaire) supportés

Donc il faut que les solutions de surveillance intègrent de nouvelles bibliothèques de script et de requêtes, permettant d'accéder à ces informations.

Surveiller l'accessibilité des Equipements/Automate.

Un SIEM va proposer une fonction de vérification régulière des services supportés par un poste IT que propose un SIEM est intéressante, mais il doit être adapté aux services Industriels. Sur certains services, une absence de 10 secondes est déjà un problème. D'une scrutation lente (1 par heure) par défaut, les solutions de surveillance doivent pouvoir réellement analyser le trafic et réagir à un silence d'1 seconde d'un équipement.

Surveiller l'évolution des Equipements/Automate.

L'état de l'art de la gestion d'actif est transposable sur le monde OT :

- version des firmware
- version de l'application (PLC)
- évolution du temps de cycle

Toutefois, ces informations sont disponibles au travers des interfaces de diagnostics, parfois basées sur des protocoles standardisés ou connu du monde IT (Modbus, Ethernet/IP, SNMP).

Mais, la plupart du temps, il faut recourir à des requêtes propriétaires, spécifiques à chaque gamme/constructeur.

Surveiller l'intégrité des Equipements/Automate.

Les logiciels de ces équipements supportent tous une gestion de version

- version de firmware
- version de l'application (contrôle des applications PLC)
- date des pages web

Dans le monde OT, les systèmes ne possèdent pas la fonction de vérification d'intégrité, et il est impossible d'ajouter un agent pour le faire (contrainte de ressource, contrainte de temps de cycle par exemple).

La surveillance de l'intégrité doit donc se faire dans l'environnement (surveillance du réseau pour noter les transferts d'application, de firmware, scrutation dédiée des équipements pour vérifier les versions installées).

Détecter les actions sensibles sur les Equipements/Automate.

Même si les applications ou configurations évoluent, il y a des 'paramètres' qui ne doivent pas évoluer une fois que le système est mis en production. Par exemple :

- Modification de l'horodateur
- Modification des paramètres réseaux
- Modification des services actifs sur un équipement (apparition ou disparition)

Une scrutation des ces valeurs est possible, mais en utilisant des requêtes spécifiques à chaque équipement, et en étendant la surveillance à des ports/protocoles nouveaux.

Détection des attaques sur les Equipements/Automates et protection associée.
Ce paragraphe liste les différentes attaques possibles, classées par type de fonction de protection ciblée et/ou décrivant quelques exemples de type de données ou de services réseaux à surveiller :

- protéger la propriété intellectuelle:
  - détecter les accès non autorisés de données protégées
    - Protéger le firmware lui-même : Téléchargement du Firmware
    - Protéger l'application client : Téléchargement de l'Application

- protéger les processus:
  - détecter les attaques ciblant les équipements
    - Passage en STOP/RUN/STOP…
    - Ordre de redémarrage (reboot)
    - Passage en mode Installation de firmware.
  - détecter les actions 'interdites'
    - commande de mode de marche (Modification en ligne par exemple)
  - détecter les redémarrages d'équipement
    - Redémarrage de l'équipement : se pose ici la question de la cause : action de maintenance ou attaque suite à une vulnérabilité ?

- Protéger l'intégrité des données et applications
  - Vérifier l'intégrité des données
    - Détecter l'écriture de données : Ecriture par une station inconnue
    - Ecriture d'une zone définie comme sensible
  - Vérifier l'intégrité des applications (checksum d'applications d'automates)

- Détection d'une attaque Man In The Middle (MiTM ou Homme du Milieu) entre le SCADA et PLC
  - Altération des réponses par un reverseProxy ou un MiTM
  - Filtrage des trames par un MiTM

- Détecter les attaques par spoofing sur les réseaux industriels
  - Réponses en double (émise par un équipement indésirable)
  - Toute communication avec un équipement visé par un ARP poisoning

4.3 Surveillances de la communication

Les communications entre équipements (SCADA-PLC, PLC-PLC et SCADA-SCADA, PLC-actionneurs) doivent également être surveillées. Un dispositif compromis peut envoyer une demande qui peut nuire au processus de production ou à la sécurité des personnes.

Au niveau SCADA.

Les outils comme l'IDS, le NIDS / HIDS sont conçus pour surveiller le trafic réseau et sont capables de déclencher des événements à destination de l'analyste de la sécurité pour tout le trafic qui traverse l'interface de surveillée (NIDS) ou tout le trafic de l'hôte sur toutes ses interfaces (HIDS).

Au niveau Automate

Parmi les protocoles utilisés par le système de contrôle industriel, seuls quelques protocoles (Modbus, DNP3,…) sont gérés par les produits NIDS. Il faut donc poursuivre l'effort de couverture des protocoles industriels, en gérant les protocoles largement utilisés tels que Profinet, BACnet ou OPC pour avoir une surveillance digne de ce nom du système industriel.

Les échanges SCADA-PLC ou PLC-PLC se caractérisent par des échanges très fréquents, sur des requêtes courtes et arrivant en rafale, tout ce que « n'apprécie » pas les NIDS. Et le temps de réponse de ces échanges est inférieur à 10ms, ce qui est peu compatible avec une analyse de flux traversant d'un NIDS.

De plus, aucun système HIDS n'existe pour les équipements industriels dont les OS sont spécifiques (OS temps réel, …).

5 Conclusion

Des événements ou des comportements inhabituels peuvent être le signe d'une attaque, en particulier dans les systèmes de contrôle industriel où les équipements répètent en permanence les mêmes échanges voire les mêmes données pendant les phases de production.

La détection de ces événements est la clé pour assurer la sécurité du système. Telle que présentée, l'aventure de la surveillance des systèmes de contrôle industriel ne fait que commencer. Des scripts dédiés Modbus et DNP3 sont publiés pour Snort, et Industrial Defender propose une solution pour surveiller certains automates. D'autres fournisseurs annoncent la prise en compte de certains protocoles industriels. Mais ce sera un travail de longue haleine avant de pouvoir surveiller tous les modèles de tous les fabricants.

Enfin, l'amélioration de la capacité de journaliser et de transmettre des événements (actions, commande, etc..) au niveau des équipements fournira un moyen complémentaire à la surveillance du système industriel.

6 Glossaire

IT: Technologies de l'information
OT: Operational Technology, désigne les technologies utilisées dans les systèmes industriels
PLC : (Programmable Logic Controller) : Automates programmables
IED: Intelligent Electronic Device, Equipement Electronique Intelligent, terme utilisé dans les systèmes électriques
HMI/IHM: Interface Homme Machine
SCADA: Supervisory Control And Data Acquisition, télésurveillance et acquisition de données ou Superviseur Industriel
IDS : Intrusion Detection System, Système de détection d'intrusion

- NIDS: Network Intrusion Detection System, Système de détection d'intrusion sur réseau
- HIDS: Hosted Intrusion Detection System, Système de détection d'intrusion sur un poste.

IPS: Intrusion Prevention System, , Système de prévention d'intrusion

Whitelisting: Contrôle d'applications qui n'autorise à démarrer et s'exécuter que les process logiciels sûrs (liste blanche), bloquant tous les autres process.

Cyber Security of Industrial Control System

Detection and Monitoring at the Controller and Field level.

Jean-Michel Brun – Cyber Security Senior Architect - Schneider Electric
Laurent Platel - Cyber Security Architect - Schneider Electric
Fabrice Tea – Cyber Security Services Business Developer - Schneider Electric

jean-michel.brun@schneider-electric.com

Abstract: Industrial systems (usually named Operational Technology system) and specially the Industrial CONTROL System (ICS) always focused the robustness (availability, safety…) and performances to any other considerations. This makes it even more important to monitor the system from the point of view cyber-security. A first step is performed at the level of software solutions like SCADA. It is essential to go further by establishing a level monitoring equipment while taking into account the specificities of fieldbus and industrial systems and architectures. Indeed, these architectures have shown inconsistencies with standard IT security solutions on the requirements of determinism and resource constraints.

This presentation will include a video showing cyber-attack scenarios detected by monitoring at the device level.

Keywords: Defense in Depth, monitoring, detection

1 The context of industrial control systems

1.1 Cyber security context

Cyber security is no longer a secondary requirement in the world of contemporary industrial control.

The industrial control systems (ICS) based on computer technology and industrial grade network are in use for decades. The first control system architectures were developed with proprietary technologies and were isolated from the outside world. Often physical perimeter security was deemed adequate and cyber security was not a primary concern.

Today, many control systems use common or open and standardized technologies such as the Microsoft™ Windows ©, IP network technology Ethernet TCP / IP and Web technology systems to reduce costs and improve performances. Many architectures also use some direct communications between the industrial control systems and the business management systems to improve operational efficiency and profitability of production assets.

This technical evolution exposes the industrial control systems to threats that target IT applications and office corporate network. Upon these threats inherited of the IT world technologies, Stuxnet and its derivatives add a specific threat and very advanced (type APT Advanced Persistent Threat) dedicated to industrial control systems. ICS are now vulnerable to "internal" attacks (attacks specifically targeting technology OT) and "external" (attacks propagated by IT technology).

The success of the Ethernet / Internet connectivity can also lead to "override" the basic safety rules and focus on ease (e.g. maintenance) by directly connecting the ICS systems on the Internet, or where there was previously using specialized monitoring and remote maintenance connection and therefore security risks much lower.

The security of industrial systems therefore goes through a thorough understanding of these characteristics and the constraints.

Among the security challenges in the world of industrial control include:

- Multiple logical and physical boundaries: an industrial control system is composed of very different devices on different network technology and different capacities, carrying a variety of protocols.
- Architectures with multiple sites over large geographical areas.
- The adverse effects of the implementation of the security on the process availability.
- The opening to the Web of the company’s networks (mobile computing, BYOD, social networks), which increases exposure to viruses and worms which could migrate from information network to monitoring network.
- The increasing exposure to malware by the increased use of portable drives (USB key or disk), laptops (technical service provider) and wireless networks.

- The direct impact of the control systems on the physical and mechanical systems, which can induce risks to safety (injury or death).

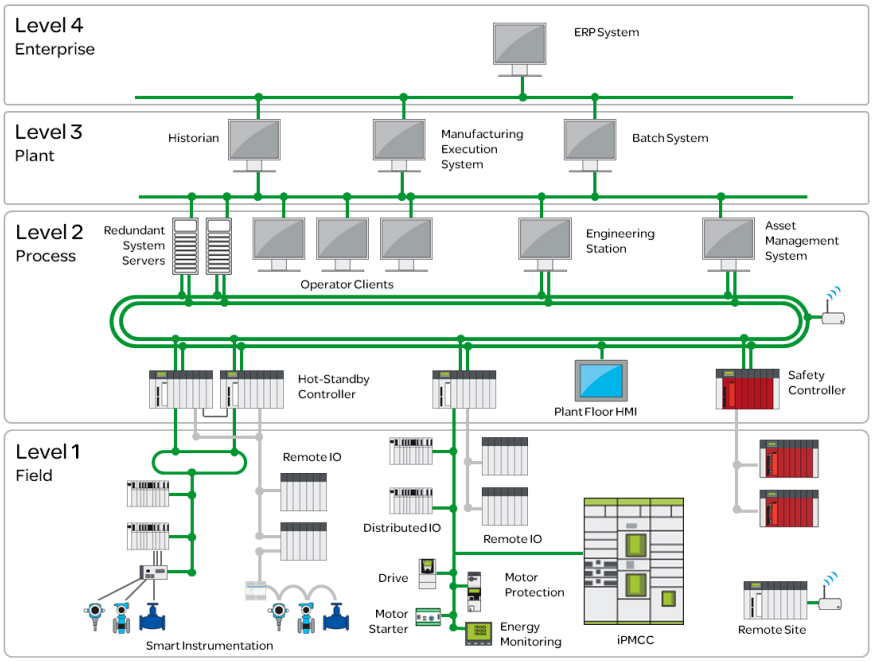
The implementation of a firewall has never been sufficient to ensure the safety of industrial installations. With a defense in depth approach, companies must be vigilant in choosing the measures to secure these facilities: a cyber attack can cause a loss of production, damage the image of the company, an ecological disaster in the worst case, loss of life. On this approach, industrial control should draw lessons from the IT world.

But, as we have demonstrated in another publication C&ESAR 2013 entitled "Cyber Security for Industrial Control Systems: The specificities of ICS, a challenge to their Security", the security solutions that have been normalized to the IT world, can not easily enter the OT world and particularly industrial control systems.

In this document, we intend to describe on the one hand the need for monitoring, on the other hand the specificities of the Industrial Control System. The cyber security solutions must manage these specificities in order to create an efficient security in the OT world.

1.2 Industrial Control Systems description

ISA95 intends to provide a model of a company including management and operational functions. The model defines several layers, layers dedicated to different functions and with different constraints.



Level 1 or field level is dedicated to sense and manipulate the production process.

Level 2 or Process level, is dedicated to monitor and control the production process, ie these equipments drive the level 1 devices.
Inside Level 2, one can identify two sub-level:

- SCADA level (Supervisory Control And Data Acquisition) that displays the process status within a graphic interface, manages alerts, log data and allows an operator to drive the process
- PLC level (Programmable Logic Controller), automated control of the process. It receives input from level 1 devices, from HMI or from SCADA and process the information to drive the outputs

Level 3 or Plant level, is dedicated to manage, dispatch the production according to workflow, recipes…

Level 4 or Enterprise level is dedicated

- to plan the production according to customer's orders
- to manage material orders and delivery
- to manage other logistic issues

Remark: ISA 95 is an international standard for developing an automated interface between enterprise and control systems. It is used in this document to illustrate the different layers of Industrial Control applications& devices. ISA 95 is not relevant to describe other systems like Smart Grid or electrical systems.

2 Why monitoring is important at the ICS level?

Prevention is ideal but detection is essential…
(SANS Institute – Defense In Depth –v.2013)

Security experts say that hackers are able to break a new security technology/mechanism every 5 years.

Principles of Defense in Depth have to be applied to secure any system. Regular test and penetration test have to be planned to check the security level of the system. Once cyber security measures are set up, it is mandatory to monitor the system otherwise the system owner is blind about the security level status.

With the Industrial use cases, according the big quantity of equipments & devices, their low level of security, the constant modification/evolution/upgrade of the ICS, it becomes more important and critical to monitor any event of the ICS in order to

- evaluate the current cyber security level
- detect any abnormal behavior of the devices
- be able to make the difference between exceptional status of the process application and attack

SIEM, IDS tools are some good tools to monitor cyber security event and detect any attack or abnormal traffic but we will see in the next chapter, that these tool are made for the IT system and need adaptation to the ICS field level.

3 The need for monitoring at equipment level.

Leveraging analysis of the Stuxnet operating mode, we can identify the needs of monitoring and detection level devices and between devices and sensors / actuators.

3.1 Management of integrity and Change management

Monitoring device identity (serial number)

The scenario requires physical access to the equipment, which makes it tricky. But it is not impossible that in an action for preventive or corrective maintenance, equipment to be replaced by other improper equipment.

It is also possible that maintenance is carried out in a hurry taken him into the system equipment 'out of the box' without any update for example.

To prevent this scenario, it is necessary to detect any change in hardware.

Automatic change detection equipment would also facilitate maintenance and more specifically traceability of actions maintenance.

Monitoring accessibility of these devices

Availability if ICS is essential to its proper functioning. It is also generally accepted that in the industrial sector, the availability prevail within the traditional triptych of security (confidentiality, integrity, availability). It is therefore important to monitor the accessibility and availability of equipment at any time.

Change management

The management of software versions is just as important in the industrial world in the computer world. Application programs are developed and tested with a certain version of the operating system. The use of these application programs with other software versions could have unintended consequences (different behavior, failure ...) due to differences between the versions. It is therefore important to monitor deployed on-site software versions.

Integrity Checking

The device in an ICS are programmed to perform specific tasks (eg valve opening) under specific conditions (fluid level reaches for example). It is therefore important to detect any malicious modification of these programs.

Detection of sensitive actions

The ICS are operating mechanical or electrical equipment that provide a service while respecting constraints including safety, environmental or quality. Some actions or commands (for example, a stop command) of these systems can then impact all or part of these elements. It is therefore important to identify these sensitive actions and monitor their use..

3.2 Attack detection

Detection of an attack requires building a database of the classical scenarios of attacks. To do this, you must make a list of all known weaknesses exploited, then to analyze incidents in order to create measures and correlations rules in front of these exploits. The IT world has developed an active community for these phases of compilation and analysis. This allows IT world to quickly enhance monitoring tools, and maintain a high level of security.

The OT world has not yet reached the maturity and simple collection of incidents proves a difficult task, reporting an incident is not compulsory in France, and habits to restart quickly the process rarely permit to conduct an analysis of the incident. The tools from the IT world can detect the well-known attack targeting the web-services of an industrial system, but they cover only a small portion of the exposed functions. Protection services purely OT remains to be studied, and community is to be created.

4 Why IT monitoring solutions don't fulfill the ICS requirement, and what are the specificities to consider?

Taking up the classification made at the beginning of the document, the Level 2 that is studied here is divided into Level 2 Supervisor (SCADA) and Level 2 equipment (PLC / PLC, ...).

The following paragraphs will analyze the monitoring functions at a SCADA level, then at equipment level and finally at the communication level.

4.1 Monitoring the SCADA

To meet the needs identified in the previous chapter the (cyber-security) monitoring system needs to connect and exchange data with SCADA and PLCs. As SCADA is usually based on standard hardware and Windows © systems, we can say that the existing solutions (SIM, SEM and SIEM) as AlienVault, Splunk, QRadar, Enterprise Security Manager, designed for IT and technology are a possible solution to monitor SCADA.

Monitor the identity of SCADA

These are generally positions Windows© or WindowsServer©, with large processing capacity. There may be a antivirus, but the update is not frequent.

The presence of a local agent of a SIEM is possible, but there is no publication of compatibility. The impacts of a SIEM agent on the system are to study, whether the impacts on performance or impact on the performance of batch triggered by the SCADA exceptional circumstances (e.g. crisis management). Blocking one of these batch or utility is not conceivable.

Monitor availability of SCADA

Monitoring availability of a Window© computer is a SIEM mission. However SCADA are often redundant, that is to say that two computers are held to ensure the SCADA function itself, one station is active, the other is in StandBy in case the first 'disappears', using proprietor exchange protocols to check their status. The monitor function is then the couple of PCs, more than a single station. This is not trivial with a classic SIEM.

Change management of SCADA

Monitoring and logging setup or updates of the operating system or applications (SCADA, SQL Server ...), compute some statistic about resources used (load Processors, RAM occupation, bandwidth network cards) is in the area of SIEM.

Beware though the specific protocols used OPC OPCUA or non-IP networks will not be monitored by these tools.

Integrity check on SCADA

Integrity can be done using AppLocker application or agent of SIEM, the operating system can verify their integrity themselves on this computer. The integrity of these positions is to the scope of traditional SIEM. Provided that the installation of an agent is consistent with the performance of the SCADA system, providing secure boot options are enabled on these positions.

Detect sensitive actions

Unplanned restart (to force the switch with standby), restoring old settings (thanks to Service Registry Recovery): these are changes that can be detected by a SIEM. But again, the SCADA software also contains a complex and precise configuration, including changes can severely affect the availability of SCADA and data. There must be an agent or a script that can monitor the actions made by a user of SCADA within the SCADA to really cover the spectrum of malicious actions.

Attack detection

SCADA uses traditional services (SQL, Web, FTP), so tools from the IT world will be able to ensure detection of attacks on web services, known vulnerabilities in the operating system or database. By cons, a DoS attack on specific ports redundancy management escape him. These proprietor protocols and ports, sometimes on dedicated IP network, should require a specific script or specific parameters to be monitored.

4.2 Monitoring the Device/PLC

Controllers (PLC) are based on specific technologies, absent from conventional computer networks.

The connection to these devices requires specific protocols, and often proprietor one. The well-known Modbus protocol example, is used to exchange process data, and can not be used directly to exchange information about the status of the PLC. This state is accessible only by specific sets of queries for each device. Indeed, the recovery of information (version number of hardware or software, for example) requires to know the memory mapping of the equipment for example (the information is stored differently in each model).

The classic SIEM are blind to this level. While some (Industrial Defender, for example) have proprietary protocols and are able to recover identity information from the memory mapping of a device (PLC…). But the range of covered equipment is small at the moment.

Monitor the identity of device/PLC

These devices have their own identity information. The problem is to access these informations, usually using specific queries on industrial protocols.

- Serial number
- MAC address for TCP/IP equipment
- Firmware version
- Application version
- Active services: these are not IT services. Of course we can find a port 80, but there also has 502 ports, 1089, 2000, 2222, 3840, 47808.44818, according to the protocols (industrial or proprietor) supported

It is necessary that monitoring solutions include new libraries and scripting applications, providing access to this information.

Monitor the availability of device/PLC

The activity of regular testing of supported services that offers SIM is interesting, but it must be adapted to the industrial service. On some services, an absence of 10 seconds is already a problem. So you can not use a hourly scan, you must really analyze the traffic and react to a silence of one second for some devices.

Change management for device/PLC

The state of the art of asset management can be transposed to the world OT:

- Firmware version
- application version (for PLC)
- cycle time evolution

But again, information are available through diagnostic interfaces, sometimes based on standard protocols (Modbus, EtherNet / IP) or through SNMP. But most of the time, we must resort to proprietary requests, specific to each range / manufacturer.

Integrity check for device/PLC

All of the device's software supports a version management:

- firmware
- application (PLC application)
- date of web pages

In OT world, operating system doesn't have a function to check integrity of file/binary. And it is impossible to add a dedicated Agent to do this (resource constraints, cycle time constrain for example).

The integrity check must be done by the cyber-security environment (network monitoring to detect the application transfer, firmware update, or dedicated scanning of the device to check the installed versions)

Detect sensitive actions on device/PLC

Although applications or configuration change, there has 'parameters' that should not change once the system is put into production.

Changing the clock

Changing network settings

Changing the active services on equipment (appearance or disappearance)

A scan of these values is possible, but using specific requests to each device, and extending the monitoring to new ports / new protocols.

Detection of attacks on device/PLC

- Protect intellectual property:
  - Detect unauthorized access to protected data
    - Protect the firmware itself: firmware upload
    - Protect customer application: application upload

- Protect the industrial process:
  - Detect attacks targeting equipment
    - Bursts of SOTP/RUN/STOP request
    - Request for Reboot Operating system
    - Switching to specific mode: firmware update, debug…
  - Detect 'forbidden' action
    - as defined just above
  - Detect the restart of device
    - Restart after which event (maintenance activity or vulnerability exploit) ?
- Protect data integrity
    - Detect data writing: Who sent this request? Did we already see this request?
    - Detect write in area defined as critical!
  - Detect an strange modification of application
    - No download have been detected but application checksum is modified?
- Detect Man In The Middle (MiTM) between SCADA and PLC
  - Tampered frame by a reverseProxy or a MiTM
  - Missing frame, destroyed by a MiTM
- Detect spoofing attacks on industrial network
  - Double result frame (modbus poisoning)
  - Any communication with device after an ARP poisoning attack?

4.3 Monitoring the communication

Communications between equipment (SCADA-PLC, PLC-PLC and SCADA-SCADA, PLC-actuators) should be monitored. Device can send a compromise request that can harm the process of production or safety.

At SCADA level

Again, tools like IDS, NIDS / HIDS are designed to monitor network traffic and can trigger events to the security analyst for all traffic passing through the interface monitored (NIDS) or traffic on all host interfaces (HIDS).

At PLC level

Among the protocols used by the industrial control system, only Modbus and DNP3 are managed by the NIDS products. Other widely used such as Profinet, BAC-net or OPC should be supervised to really monitor an industrial network.

Communication between SCADA and PLC or PLC-PLC is characterized by very frequent exchanges on burst of short queries, exactly what NIDS dislikes. And the response time of these exchanges is less than 10ms, which is incompatible with an analysis in depth of flow through a NIDS.

In addition, no system exists for these HIDS equipment which are using specific OS.

5 Conclusion

Unusual events or unusual behavior can be a sign of an attack in particular in the industrial control systems or equipment constantly repeat the same exchanges see the same data during the production phases.

1. The detection of these events is the key to ensure the safety of the system. As presented, the adventure of monitoring industrial control systems is just beginning. Scripts dedicated to Modbus and DNP3 are published for Snort and Industrial Defender provides a solution to monitor some machines. But it will be a long process before you can watch all models from all manufacturers.
2. Device must implement some feature to monitor its communication
3. Devices must implement a log and alert capability to provide fine information to a SIEM

6 Glossary

IT: Information Technology
OT: Operational Technology
PLC : Programmable Logic Controller
IED: Intelligent Electronic Device
HMI: Human Machine Interface
SCADA: Supervisory Control And Data Acquisition,
IDS : Intrusion Detection System,
NIDS: Network Intrusion Detection System
HIDS: Hosted Intrusion Detection System
IPS: Intrusion Prevention System
Whitelisting software: Software application that allows to start and run the authentified process (white list), blocking all other processes.

Investigating requirements models completeness in a unified process for safety and security

Vikash Katta[*†], Christian Raspotnig[*‡], Peter Karpati[*]

[*]Institute for Energy Technology, Halden, Norway
[†]Norwegian University of Science and Technology, Trondheim, Norway
[‡]University of Bergen, Bergen, Norway
vikash.katta@hrp.no, christian.raspotnig@hrp.no,
peter.karpati@hrp.no

Abstract. Requirements completeness is one of the characteristics of adequately specified requirements. Defects in requirements are one of the major sources of accidents and undesired events pertaining to the use of computer-based systems in safety-critical operations. Addressing completeness of safety and security requirements while developing SCADA systems is therefore required. In this paper, we will look into the completeness aspects of requirements models produced by using CHASSIS, a method for combined assessment of safety and security. Furthermore, we will investigate how a traceability approach called SaTrAp can support addressing some of the completeness issues. We will utilise a SCADA example - a cyber-physical system used for transporting a polluting substance- to demonstrate our approach.

Keywords: safety, security, requirements, models, completeness, SCADA

1 Introduction

Increasingly, computer-based systems are being used to perform safety functions in safety critical domains. Systematic hazard identification and assessment of such systems is required, in order to mitigate failures of the systems that could result in harm to people or environment. In the case of Supervisory Control and Data Acquisition (SCADA) systems, which generally use multiple computer-based components deployed in different physical locations, there is a need to not only identify safety hazards to the system but also to identify the security threats to the system. Due to the interconnectivity and information exchange between the different components in a SCADA system, vulnerabilities in one component can be exploited to attack other components and jeopardise the safety functions of the SCADA system.

Due to the possibility of having large number of threats and vulnerabilities in these systems, there is a need for better development and assessment methods, especially methods which look into both safety and security aspects. In this regard, we have developed a method called Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS) that proposes a unified process for safety and security assessment. CHASSIS integrates safety and security assessment into the system

development process, in particular into the requirements engineering process [12-13]. Available techniques for requirements modelling, safety assessment and security assessment are combined by CHASSIS in order to identify and model hazards, threats and mitigations to a system. The results from using CHASSIS are diagrams (requirements models) describing both normal and undesired behaviour of a system. In order to use such a method, the completeness of the diagrams produced is vital for obtaining valid and complete set of safety and security requirements. Eliciting a valid set of requirements is essential as "errors in requirements are the most numerous in the software life-cycle and also the most expensive and time-consuming to correct" [6]. These observations are also applicable for safety-critical systems as incompleteness and flaws in software requirements are major cause of accidents [3-4].

In this paper, we present the concepts behind requirements completeness and we investigate how CHASSIS along with a supporting traceability approach addresses some of the completeness issues. The rest of the paper is structured as follows. Sec. 2 provides an introduction to requirements completeness and why it is important for SCADA systems. In Sec. 3, we briefly present the CHASSIS method, the techniques included and a traceability approach using an example SCADA system. Sec. 4 presents our findings and further work needed. Related work is presented in Sec. 5. Finally we conclude the paper in Sec. 6. Parts of the work presented in this paper, in particular Sec. 3 and Sec. 5, were reported in our earlier publications. The work[1] presented in this paper will also be published through other venues.

2 Requirements completeness

According to [2], completeness of a specification can be defined as "the extent that all of its parts are present and each part is fully developed". In order for a specification to be complete, the following properties should be satisfied [2]: 1) no understated information, 2) no non-existent references, 3) no missing specification items, 4) no missing functions and 5) no missing products. With respect to what constitutes sufficient completeness, Zowghi et al [7] states that: "Decision on what is sufficient completeness would have to be defined with respect to the type of system being implemented". For safety-critical systems, sufficient completeness may be defined with respect to safety design constraints and safety requirements identified during safety assessment [5][8]. Similarly for SCADA systems, sufficient completeness can be defined with respect to safety and security requirements which might be identified during safety and security assessments, together with completeness of system functional and other non-functional requirements.

[1] This work is a part of PhD projects carried out in collaboration between the Institute for Energy Technology/Halden Reactor Project, Norwegian University of Science and Technology and University of Bergen. Halden Work Reports (HWRs) and Enlarged Halden Programme Group Meeting papers are not publicly distributed, and can be provided upon request.

2.1 Importance to SCADA

When developing SCADA systems, a systematic process for identifying safety and security requirements must be followed. There exist several safety and security methods and techniques which could be used to identify hazards and threats, assess the risks to the system and identify mitigations. It is essential that methods used are able to elicit requirements in a way ensuring completeness, correctness and consistency. The former is important while developing systems, in order to, among other things:

- have a valid set of requirements satisfying the customer needs as well as safety and security objectives
- have a consistent set of requirements thereby avoiding conflicting requirements, e.g. between safety and security requirements
- have an end product implementing the requirements that satisfies the safety and security objectives
- demonstrate – e.g. by using assurance cases- that the safety and security requirements reflect the results of the safety and security assessment

2.2 Achieving requirements completeness

Achieving or demonstrating absolute completeness of requirements is probably not practicable. As stated in [8]: "demonstrating the completeness of the set of identified safety requirements is therefore more a question of producing confidence than of providing a proof in the mathematical sense". The same applies to demonstration of completeness of security requirements. To attain confidence, a systematic process applying the best combination of methods should be followed for identification of safety and security requirements. It is also necessary to show that all relevant safety and security requirements mitigate the hazards and threats identified during safety and security assessments. Here, traceability between safety and security requirements to the safety and security assessments – basically to their respective hazards and threats – ensures that the requirements reflect the results of the assessments. It should also be demonstrated that these safety and security requirements are fulfilled by the subsystem or component of the system. To achieve this, one needs to ensure that subsystem requirements, design specifications and implementations are complete with respect to the specified system safety and security requirements. One way of achieving this is to ensure forward traceability from system-level requirements to sub-system or component level requirements, design and implementation.

According to Firesmith [1], requirements completeness could be interpreted as completeness of: 1) Requirements analysis models, 2) Individual requirements, 3) Metadata describing individual requirements, 4) Requirements repositories, 5) The set of requirements documents, 6) Individual requirements specification documents, 7) A requirements baseline. In this paper, the focus is on the completeness of the requirements analysis models, as we will investigate this in particular for CHASSIS. "Requirements models are models that document various views of the needs of the system. They can be graphical, textual, or mathematical. A requirements model is complete if it contains all important information needed to completely develop its associ-

ated requirements. Because different requirements models have different components, different models can have different kinds of missing or incomplete information." [1]. Completeness of requirements analysis models is a prerequisite for deriving complete requirements from these models.

There exists no single requirements model which could describe or model all the needed information of a system and its environment. Development team has to consider a combination of different requirements models in order to describe all the mandatory information. As listed in [1], there are different requirement model types which could be used to describe certain aspects of the system:

- Context Models – describes environment of the system
- Data Models – describes objects or data and their relationships
- Decision Models – describes business rules
- Event Models – describes events and their causes and consequences
- Formal Models – describes mathematically the properties and behaviour
- Performance Models – describe performance objectives and relevant scenarios
- Process Models – describes functions and relationships between them
- Safety Models – describes system safety aspects
- Security Models - describes system safety aspects
- State Models – describes states and transitions
- Use Case Models – describes the actors and their interaction with system

To summarise, even though achieving absolute completeness is not practicable, we can in principle achieve confidence in completeness of requirements models, by ensuring that:

1. each type of requirements model describe all the mandatory information it needs to document
2. all the different types of requirements model together consistently (without any conflict) describe all the mandatory information of the system
3. safety and security requirements reflect the results of the assessments by documenting the traces between requirements to the results of assessments

However, ensuring the above principles is not straightforward. Since different methods and processes are used for safety and security assessments, this will result in different types of requirements models which are not necessarily consistent with each other. In practice, it is not uncommon to have different expert teams looking into safety and security aspects, and it is also not uncommon that the communication between these teams is not effective, thereby leading to misunderstandings and proposing incomplete and conflicting requirements.

3 CHASSIS – a method for combined assessment of safety and security

The CHASSIS method defines a unified process for combining safety and security assessments [12-13]. Fig. 1 shows the process overview diagram of CHASSIS, which consists of three main activities: (1) Eliciting Functional Requirements, (2) Eliciting Safety/Security Requirements and (3) Specifying Safety/Security Requirements.

The first activity is the elicitation of functional requirements, where users, system functions and services are described using use case diagrams (D-UC), textual use cases (T-UC) and sequence diagrams (SD). The second activity focuses on the elicitation of safety and security requirements. With users, functions and services as input, misusers, hazards, threats and mitigations towards the functions and services are identified and described using misuse case diagrams (D-MUC). Textual misuse cases (T-MUC) and function sequence diagrams (FSD) will further detail the hazardous scenarios for safety. Updating the D-MUC and further detailing the T-MUC and FSD will be iterative. For security, misuse sequence diagrams (MUSD) are used to describe threat scenarios. During trade-off analysis, the mitigations identified will be compared in order to investigate their consistency. The third activity is specification of safety and security requirements. For detailed description of CHASSIS refer to the guideline for CHASSIS [13].

CHASSIS supports an iterative process for identifying hazards and threats and thereafter for elicit safety and security requirements. During this process, several diagrams (views of system) of the system are created and thereafter modified. These diagrams need to be complete and consistent in order to have a valid set of safety and security requirements. We need to specify and maintain the history of creation of diagrams and thereafter their evolution.

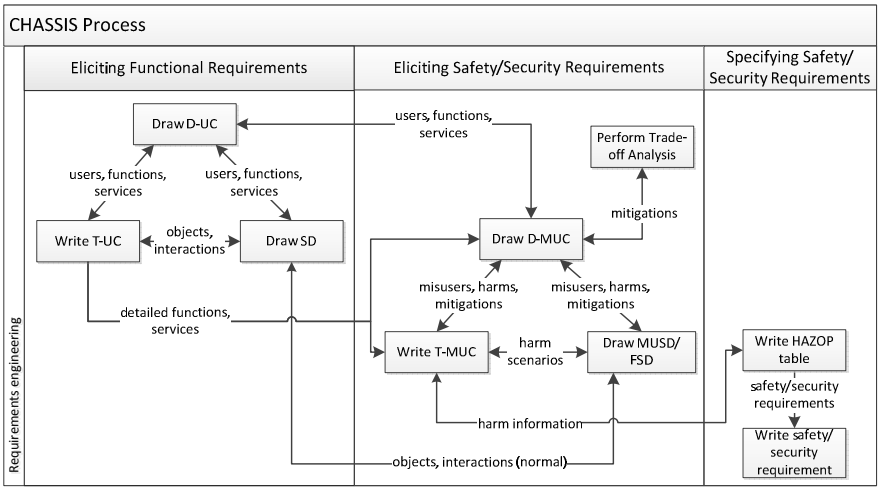


Fig. 1. CHASSIS process overview diagram

3.1 Desktop example: Cyber-physical system

In an earlier work [14], CHASSIS was applied on an example SCADA system, which could be used for transporting a polluting substance. The example system is based on a similar system described in [28-29]. The system was referred to as *cyber-physical system*, to mean that the system consists of a computer-based system that controls physical components. The physical part of the system consists of a pipeline for transporting polluting substance. Pumps placed throughout the pipeline are used to pump the substance stream forward and valves are used to allow or block the stream. The cyber part consists of a protection system which includes remote Control-Center (CC) and Remote Telemetry Units (RTU). RTU collects pressure values from pumps and valves, controls pumps and values operations, sends data and alarm signals to CC, receives instructions from CC.

The protection system was assessed for hazards and threats using CHASSIS. The result is a collection of diagrams describing both the normal and undesired behaviour of the system. Fig. 2 presents the D-MUC representing the functions and failures and threats to the system – left part shows the safety part, right part shows the security part. T-MUC, FSDs[2] and MUSD were also created to elaborate the misuse cases described in the D-MUC, thereby exploring the functionality, hazardous scenarios and threat scenarios to the system.

Fig. 3 and Fig. 4 present FSDs modelling the scenario which could lead to a hazard of water hammer resulting in pipeline break and pollution spilling. Water hammer in a pipeline occurs due to high pumping pressure and then suddenly closing a downstream valve. As shown in the figures, the pipeline break is the consequence of a water-hammer caused by either a faulty (unlucky) operator or due to the failure of the SCADA system. Fig. 3 presents water hammer scenario at a high-level (SCADA system level), whereas Fig. 4 details the scenario showing the inner failures (red/dashed notation) of the SCADA system by decomposing parts of the SCADA lifeline into architectural components (e.g. CC, RTU1).

Fig. 5 presents an MUSD, which models the interactions of an attacker (shown as red/dashed notation) misusing the vulnerabilities of components of the systems in order to achieve a water hammer attack. The MUSD describes a scenario where an attacker gains access to the system, manipulates the data/signals of the system to cause the water hammer. Based on the new information elicited with FSD and MUSD, a new D-MUC was created. The new D-MUC (not shown in this paper) includes failures and mitigations.

[2] Note that due to space reason we have not included the complete decomposed FSD in Fig. 4, which excludes the failures 1 and 2, and hazard 1 from Fig. 3. Mitigations were not described in FSDs and MUSDs

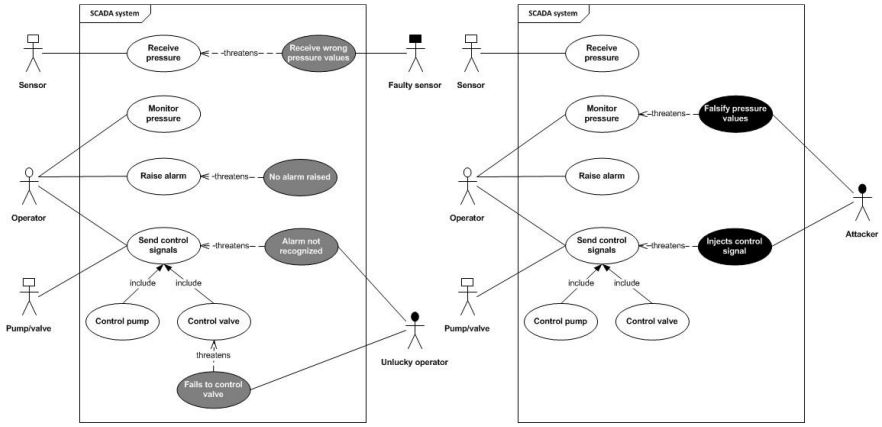


Fig. 2. D-MUC showing some of the use cases and misuse cases

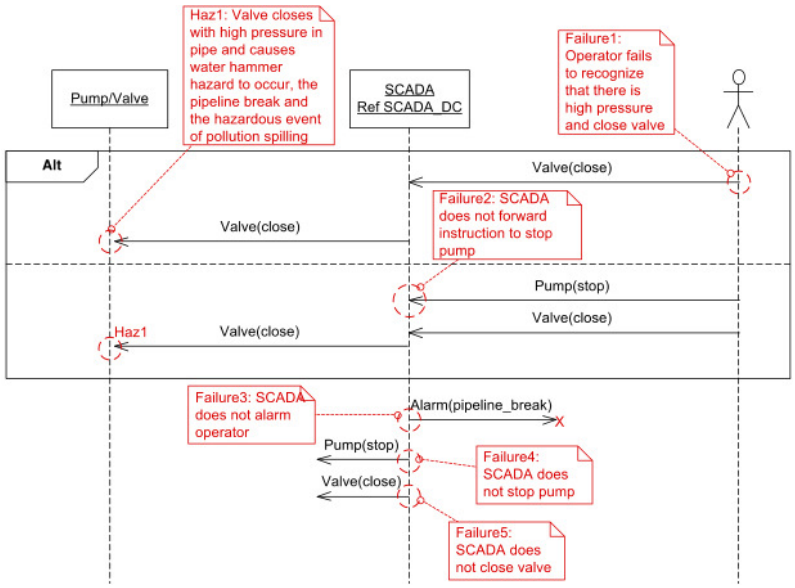


Fig. 3. FSD providing the overview of failures in the SCADA system [14]

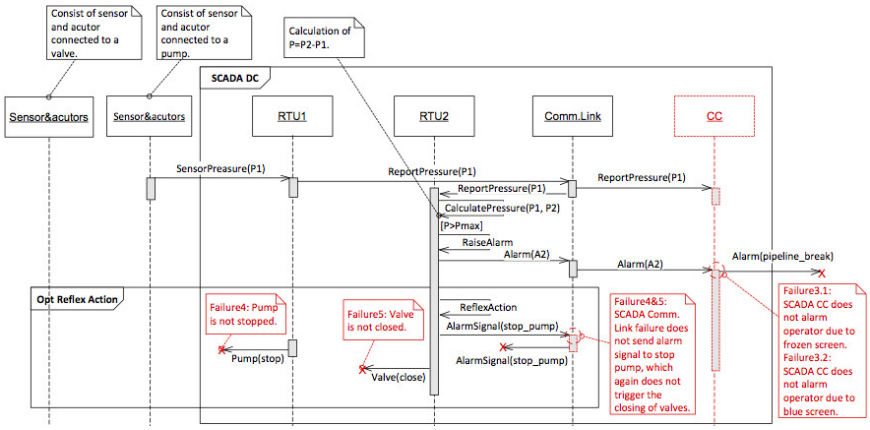


Fig. 4. A decomposed FSD showing the failures related to the components of the SCADA system (based on [14])

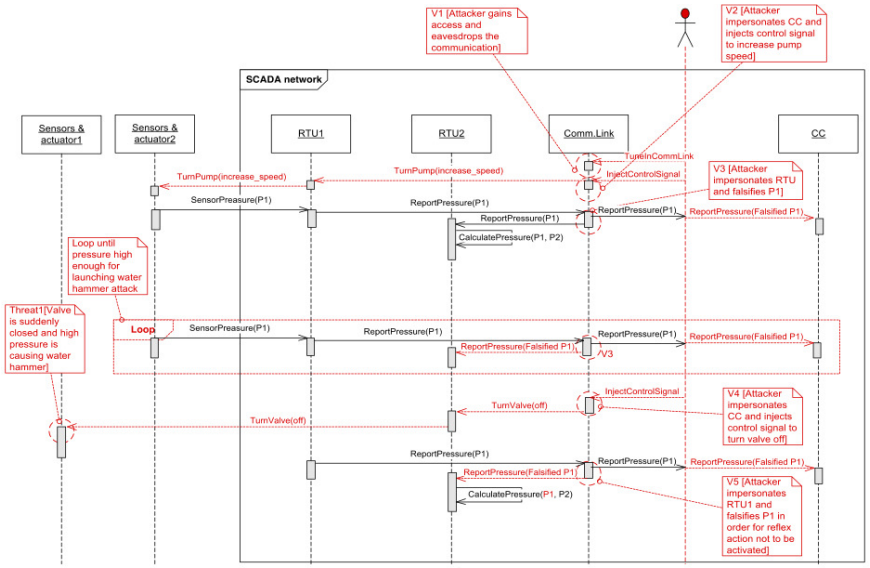


Fig. 5. Misuse sequence diagram for a water hammer attack [14]

3.2 SaTrAp – a traceability approach

For traceability support, i.e. to capture traces and to perform change impact analysis, we have utilized a traceability approach called SaTrAp (Safety Traceability Approach). SaTrAp was developed as a part of our on-going work on improving traceability for safety systems [9-11]. The approach aims to provide traceability support

for some of the tasks of the stakeholders, in particular the tasks of the safety analyst and safety case author. For example, safety analyst could use traceability information to verify and validate whether all the safety requirements have been implemented, whereas safety case author could use traces to identify the impact and manage the safety case according to the changes during systems development. The approach consists of a process model and meta-models. A process model is like a blueprint describing a process that needs to be followed by the stakeholders for capturing traces during development process. The traceability-process model describes "what" kind of artefacts and relations should be captured and "when", i.e. at what levels, to capture them. The scope of SaTrAp's process model is ten abstraction levels starting from development of system concept to system installation. Meta-models categorise different types of artefacts and relations and define rules (syntax and semantics) for them.

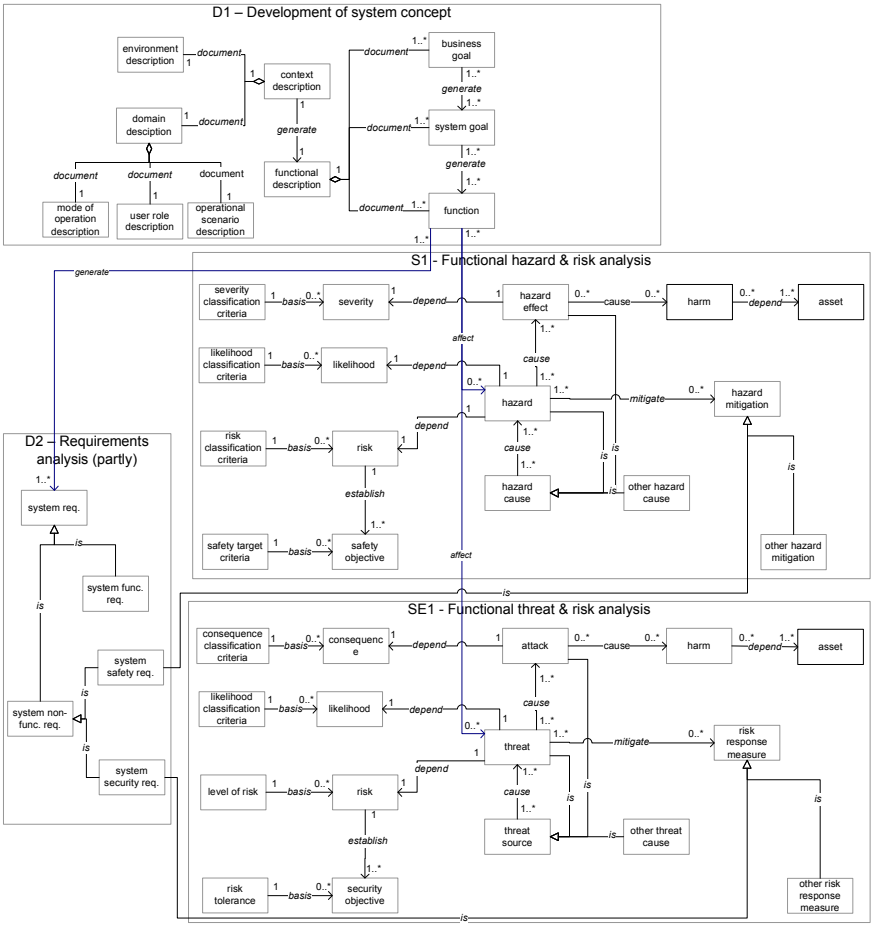


Fig. 6. Part of SaTrAp process model with artefacts and relations

We have extended SaTrAp to include artefacts related to security assessment at the levels of system concept and requirement analysis, and functional threat analysis [9-10]. Fig. 6 presents parts of the traceability process model, with system concept (D1), requirement analysis (D2), functional hazard analysis (S1), and functional threat analysis (SE1) abstraction levels. The process model shows the types of development, safety and security artefacts and the relation types between them. The lower part (SE1) of the figure shows the security part. At the D1 level, artefacts related to the system domain and environment is described. In S1, possible hazards to system, risk associated with hazards, and identified hazard mitigations are documented. In SE1, security assessment results are documented. At D2, system level requirements, including safety and security requirements are documented.

In [10], we have discussed how SaTrAp can be used for requirements management while developing safety systems with security considerations. We also discussed how the approach supports different traceability analysis to identify impact of a change. In [11], we have shown how SaTrAp can be used to extract valid set of artefacts that can be used to generate and maintain safety case, especially extracting evidences for safety case. The focus of this paper is, however, to investigate how SaTrAp can be used to address some of the issues related to completeness of requirements models. Reflecting on the discussions in Sec. 2, SaTrAp could be used support the development of SCADA systems by addressing the following completeness aspects:

- what type of mandatory information should be documented by requirements models by using the process model as a baseline
- how to capture the history of safety and security requirements by tracing them to safety and security assessments by using the process model
- verify and validate that requirements (and other artefacts) are complete with respect to a change by using traceability analysis

Fig. 7 presents a snapshot from a tool implementing SaTrAp. Snapshot shows parts of the graph documenting the traceability information of the cyber-physical system. Functions in the graph (represented as F1, F2 etc.) corresponds to the use cases (white ovals) in Fig. 2. Initially, these use cases were documented in a use case diagram (D-UC1). Safety related hazards/hazardous events related to the functions are shown on the right part of the graph (represented as Haz1, Haz2 etc.). Similarly the threats are also shown (represented as Threat1, Threat2). Hazard and threat information were documented in misuse case diagrams D-MUC1 and D-MUC2 respectively.

Fig. 7 also shows the impact analysis to function “send control signals” (represented as F4). The highlighted artefacts - functions F5 and F6, hazards Haz3 and Haz4, hazard effect HazEffect1, threat Threat2 – might be affected. Fig. 7 shows only a simple example of a traceability graph. However, you could use SaTrAp and its supporting tool to extensively capture traces during overall development process and to perform several traceability analyses. For example, you could verify whether a hazard has been addressed, and whether the safety requirements addressing the hazard has been considered in the system design and thereafter implemented. The tool implements the process models and meta-models proposed by SaTrAp– thereby incorporating the traceability rules defined by them.

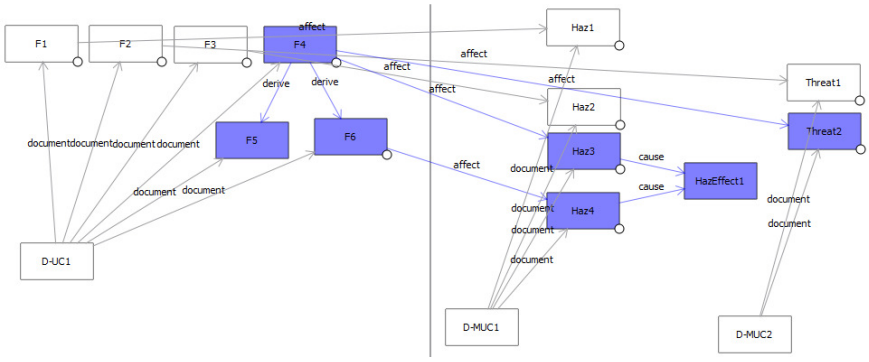


Fig. 7. Traceability graph showing impact to F4 (function: send control signals)

4 Investigating models completeness

We have used the recommendations provided in [1], by preparing a list of mandatory information which the models should describe in order to be complete. Note that these model types are not mutually exclusive, i.e. a diagram (or model of a system) could fall into more than one of the model types. For example, markov chains that are used during safety analysis could fall under both safety models and state models.

In accordance with the three principles of completeness stated in Sec. 2, we will verify whether the diagrams produced by CHASSIS describe this mandatory information. We will also verify to what extent SaTrAp can support tracing the mandatory information, in particular traces between safety and security requirements to the results of assessments. Table 1 presents an overview of the results of our analysis.

Table 1. Requirements models completeness coverage by CHASSIS and SaTrAp

Model type	Mandatory information	CHASSIS	SaTrAp
Context Models	external systems, relationships between system and external systems, characteristics of relationships	Partially. Relations between systems and external systems using use cases.	Yes.
Data Models	data, semantics of data, relationships	No.	Yes.
Decision Models	decisions, consequences of a decision	No.	No.
Event Models	events, causes of events, probability and consequences of events, associated risk	Yes. Hazardous and threat events using D-MUC; T-MUC, FSD and MUSD.	Yes. events can be traced to their causes, consequences and risk

Formal Models	statements of system properties or functions	No. Techniques used by CHASSIS are based on UML, a semi-formal language.	Partially. Artefacts such as function and requirement expressed formally.
Performance Models	scenarios, scenario steps, performance budgets, evaluation and verification results showing that the performance budgets can be met	Partially. Performance requirements as pre-conditions in textual use cases.	No.
Process Models	functions, relationships: functional decomposition, control flow, data flow	Yes. Using use cases and misuse cases	Yes.
Safety Models	asset , accident, hazard , safety risk	Yes. Might need additional models (e.g. event tree) for risk calculations.	Yes.
Security Models	asset, attacker, attack, threat, security risk	Yes. Might need additional models (e.g. BDMP) for risk calculations.	Yes.
State Models	states, state transitions, triggering events, guard conditions on transitions	No.	Yes.
Use Case Models	use case name, description, actors, preconditions, post-conditions, invariants, use case relationships	Yes.	Yes.

CHASSIS, i.e. the diagrams produced, does not cover all the information that is needed to elicit complete requirements. The focus and strength of CHASSIS is on safety and security assessment and therefore can be used to produce complete models describing safety and security aspects. With help of D-UC, T-UC, D-MUC and T-MUC, the use case models - not only describing normal scenarios but also abnormal scenarios – are covered. Models related to describing data, decision (business rules) and states of system are not considered as a part of CHASSIS. Therefore, development and assessment teams using CHASSIS must consider using other methods or techniques to describe information such as business rules and state models.

Even though coverage of all information is not within the scope of CHASSIS, there is a need to describe how CHASSIS could be systematically used along with other available techniques to achieve the completeness. In this regard, we looked into how CHASSIS could be combined with a technique called Boolean Logic Driven Markov Processes (BDMP) [15] which can provide a thorough quantitative risk assessment of

hazardous and threat events [14]. Further work is needed on combining CHASSIS with other techniques in order to address aspects such as system performance and business decisions which can have an impact, especially during trade-off analysis, on safety and security aspects of the system.

Checking the completeness of CHASSIS related diagrams is a manual task, so far. We need tool support for automatic checking of the diagrams for their completeness. SaTrAp along with its supporting tool can be used to automatically verify some of the completeness issues related to CHASSIS, in particular traces between requirements and safety and security assessments.

5 Related work

Related to our work on traceability approaches, Ramesh and Jarke [15] have proposed traceability models that can be used by two groups of users – high end and low end users. Even though these traceability models are comprehensive, they are limited to the development process and not targeted to address traceability concerns of safety systems, as our approach is. TACO Traceability Model facilitated traceability by representing the requirements changes in terms of a change history [16]. The strength of the model is that it formally defines the model and the semantics underlying the change types. To a large extent, the emphasis of TACO Traceability Model is on the requirement management activity. The Information model proposed in [17] for model driven safety requirements management is based on SysML, and the model is made compatible with the standard ANSI/EIA-632. The information model is not elaborate and fine grained with respect to granularity of the development and safety analysis activities, and the types of artefacts considered. Automated traceability capturing and extraction are based on information retrieval techniques and are normally tied to the modelling languages (e.g. UML and SysML) or integrated tool environments used during development. For example, the work in [18] is specialized towards SySML focusing on traceability between safety requirements and design.

However, disadvantage of using generic models and tools is that it is left to the stakeholders' subjective reasoning to use and extend the models according to their needs. In development projects with different stakeholders, such generic models does not provide a clear picture on what artefacts should be created and traced at a particular level and who is responsible for that. SaTrAp builds upon the common process for system development, assessment and certification proposed in [19], and the generic traceability models proposed in [15] [16], by extending these models to incorporate safety and security aspects.

There is several security methods related to CHASSIS, with CORAS as the closest [20]. Earlier work in the CORAS project also combined UML with more traditional safety techniques, such as HAZOP and FMEA [21]. However, the method focuses on security aspects and does not aim at unifying safety and security assessments. The idea of MUSD in CHASSIS is similar to what is outlined in [25], where an approach is suggested that integrates CORAS with a component-based system development process for formalizing risk interaction. In [25], sequence diagrams (SD) are used by

modelling the attacker and the asset as lifelines, and using *palt* operator to provide the probabilistic choice. However, MUSD does not represent probability and is used to outline harm scenarios, opposed to formalizing the risk interaction identified and document by CORAS in threat diagrams. Another approach has been suggested for using SD to represent misuse case as scenarios [26]. They use UML SD that includes the attacker as a stereotyped actor, and they generate Finite State Machines (FSM) to show whether the attack can be successful or not. CHASSIS does, however, neither supplement misuse case scenarios with FSM, nor aim at testing the mitigation models.

There are also other methods that allow visualizing threats, such as Secure Tropos [22] and Abuse Frames [23]. Both of these methods extend methods from the software development process, but do not address safety aspects. Firesmith proposed an information model for Defensibility Engineering in [24] by aligning the concepts of safety, security and survivability. The unified concepts were our starting point when considering the combination of safety and security assessment. For more on related work on CHASSIS refer to [12]. [27] provides an exposition of the area of requirements elicitation, in which issues of relevance to software systems, in particular with respect to completeness, traceability, and possibilities for automation are identified and discussed.

6 Conclusions

This paper discusses about requirements completeness in the context of completeness of the requirements models that can be used to elicit requirements. We have argued why requirements completeness is important while developing SCADA systems which have both safety and security considerations. The concepts behind requirements models completeness and how it can be achieved were presented. We looked into how some of the issues related to requirements models completeness were addressed in CHASSIS, a method for combined safety and security assessment.

References

1. Firesmith, D.: Are Your Requirements Complete? Journal of Object Technology, vol. 4, no.1, pp. 27-43 (2005)
2. Boehm, B.W.: Verifying and Validating Software Requirements and Design Specifications. Software, vol.1, no.1, pp.75-88, IEEE (1984)
3. Lutz, R. R.: Analyzing Software Requirements Errors in Safety-critical Embedded Systems. In: 1st IEEE International Symposium on Requirements Engineering, pp. 35-46 (1993)
4. Leveson, N.G.: Safeware: System Safety and Computers. Addison-Wesley (1995)
5. Leveson, N. G.: Completeness in Formal Specification Language Design for Process-Control Systems. In: 3rd Workshop on Formal Methods in Software Practice, pp. 75-87(2000)
6. Aurum, A., Wohlin, C.: Requirements Engineering: Setting the Context. Engineering and Managing Software Requirements. Springer (2010)

7. Zowghi, D., Gervasi, V.: On the Interplay between Consistency, Completeness, and Correctness In Requirements Evolution. Information and Software Technology, Vol. 45, Issue 14, pp. 993-1009 (2003)
8. Sivertsen, T.: Software Safety Demonstration. Technical report HWR-1056, OECD Halden Reactor Project (2013)
9. Katta, V., Stålhane, T.: Traceability of Safety Systems: Approach, Meta-Model and Tool Support. Technical report HWR-1053, OECD Halden Reactor Project (2013)
10. Katta, V., Raspotnig, C., Karpati, P., Stålhane, T.: Requirements Management in a Combined Process for Safety and Security Assessments. In: International Workshop on Security in Air Traffic Management and other Critical Infrastructures (2013)
11. Katta, V., Raspotnig, C., Stålhane, T.: Presenting A Traceability Based Approach For Safety Argumentation. In: European Safety and Reliability conference (2013)
12. Raspotnig, C., Karpati. P., Katta, V.: A Combined Process for Elicitation and Analysis of Safety and Security Requirements. Enterprise, Business-Process and Information Systems Modeling, pp. 347-361 Springer Berlin Heidelberg (2012)
13. Raspotnig, C., Karpati, P., Katta, V.: CHASSIS Guide-line (draft). Retrieved April 10, 2012, https://bora.uib.no/handle/1956/6172
14. Kriaa, S., Raspotnig, C, Bouissou, M., Pièrre-Cambacedes, L., Karpati, P., Halgand, Y., Katta, V.: Comparing Two Approaches to Safety and Security Modelling: BDMP Technique and CHASSIS Method. In: Enlarged Halden Programme Group Meeting, OECD Halden Reactor Project (2013)
15. Ramesh, B., Jarke, M.: Toward reference models for requirements traceability. IEEE Transactions on Software Engineering 27(1), pp. 58–93 (2001)
16. Sivertsen, T., Fredriksen, R., Thunem, A. P.-J., Valkonen, J., Holmberg, J. E., Ventä, O., Andersson, J.-O.: Traceability and Communication of Requirements in Digital I&C Systems Development. NKS-103 report, Nordic Nuclear Safety Research (2005)
17. Guillerm, R., Demmou, H., Sadou, N.: Information model for model driven safety requirements management of complex systems. In: Complex Systems Design & Management (CSD&M '10), pp. 99-111, Springer Berlin Heidelberg (2010)
18. Nejati, S., Sabetzadeh, M., Falessi, D., Briand, L., Thierry, C.: A SysML-based approach to traceability management and design slicing in support of safety certification: Framework, tool support, and case studies. Information and Software Technology, vol. 54(6), pp. 569-590 (2012)
19. Papadopoulos, Y., McDermid, J. A.: The potential for a generic approach to certification of safety critical systems in the transportation sector. Journal of Reliability Engineering and Systems Safety, vol. 63(1), pp. 47-66, Elsevier Science (1999)
20. Lund, M.S., Solhaug, B., Stølen, K.: Model-Driven Risk Analysis - The CORAS approach. Springer (2011)
21. CORAS: The CORAS Method. http://coras.sourceforge.net/
22. Giorgini, P., Mouratidis, H.: Secure tropos: A security-oriented extension of the tropos methodology. Journal of Autonomous Agents and Multi-Agent Systems (2005)
23. Lin, L., Nuseibeh, B.A., Ince, D.C., Jackson, M., Moffett, J.D.: Analysing security threats and vulnerabilities using abuse frames. Technical Report 2003/10, The Open University, Walton Hall, United Kingdom (2003)
24. Firesmith, D.G.: Common Concepts Underlying Safety, Security, and Survivability Engineering. Technical Note CMU/SEI-2003-TN-033, Software Engineering Institute (2003)
25. Brændeland, G., Stølen, K.: Using model-based security analysis in component-oriented system development. In: 2nd ACM Workshop on Quality of Protection, pp. 11–18, ACM (2006)

26. Whittle, J., Wijesekera, D., Hartong, M.: Executable misuse cases for modeling security concerns. In: 30th International Conference On Software Engineering, pp. 121–130, ACM (2008)
27. Henriksdóttir, S., Raspotnig, C., Katta, V., Fredriksen, R.: Requirements Elicitation – Completeness, Traceability, and Automation. Technical report HWR-1054, OECD Halden Reactor Project (2013)
28. Pietre-Cambacedes, L., Bouissou, M.: Modeling Safety and Security Interdependencies with BDMP (Boolean Logic Driven Markov Processes). In: International Conference on Systems, Man, and Cybernetics, pp. 2852-2861 (2010)
29. Fovino, I. N., Masera, M., De Cian, A.: Integrating Cyber Attacks within Fault Trees. Reliability Engineering & System Safety, vol. 94, no. 9, pp. 1394–1402(2009)

Certifications de sécurité.

Panorama, intérêts et limites pour les Systèmes Industriels.

Frédéric Guyomard

Ingénieur Chercheur, EDF Recherche et Développement

1 avenue du Général De Gaulle, 92141, Clamart Cedex

frederic.guyomard@edf.fr

Mots clés: certification, cyber-sécurité, systèmes industriels, scada, risques.

Abstract. Cette publication a pour objectif de présenter les potentiels processus de certifications applicables aux systèmes industriels et à leurs composants, et d'identifier s'ils peuvent constituer une réponse fiable aux nouvelles problématiques de sécurité informatique du secteur industriel, et dans une certaine mesure, contribuer à l'amélioration des processus de protection, par exemple en s'intégrant dans le principe d'une défense en profondeur, avec d'un coté des certifications indépendantes et de l'autre des certifications régies en partie par des autorités de régulation représentatives (par exemple celles de l'ANSSI en France). Seront présentés quelques exemples d'initiatives internationales méritant, selon l'auteur, d'être connues ou mieux connues. Enfin, avant de faire une conclusion, seront étayés des avis et articles d'experts qui se sont intéressés aux avantages et inconvénients des certifications, en les transposant dans le contexte décrit par ce papier.

1 Introduction

Depuis désormais quelques années, la criticité des systèmes numériques de pilotage et de conduite des infrastructures industrielles est mise en avant. Que ce soit dans le domaine du transport, de l'énergie, de la distribution ou du traitement de l'eau, de l'aéronautique, de la santé, et plus globalement de tout processus industriel automatisé plus ou moins informatisé, l'augmentation des attaques informatiques (dans le monde) sur ces systèmes a démontré l'intérêt de certains groupes activistes et plus particulièrement du monde de la cybercriminalité pour ce secteur d'activités. L'implication des États dans le domaine de la cyber-défense, voire même dans celui des cyber-attaques est grandissant. Pour l'industrie, le maitre mot s'apparente désormais à « complexité » car ce monde change et les menaces évoluent, alors que les bases de matériels installés et potentiellement vulnérables sont énormes. Les certifications peuvent-elles constituer une solution en matière de sécurisation informatique de ce secteur, quelles sont-elles et quel niveau de confiance leur accorder ?

2 Contexte et intérêt des certifications

Pour ces secteurs, les principales certifications que l'on trouve sont relatives à la sécurité fonctionnelle[1], notion elle-même étroitement liée à la « sûreté de fonctionnement ». Comme décrit en préambule du forum de l'ISA-France qui s'est tenu à l'Ecole Centrale de Lille le 25 octobre 2012, « l'automatisation moderne exige que soient respectés, au niveau des systèmes de contrôle-commande, des critères stricts de disponibilité et de sécurité fonctionnelle répondant à des normes telles que l'IEC 61508 et l'IEC 61511. Des techniques particulières de surveillance, telles que les algorithmes de détection et de localisation des défauts ou de diagnostic, utilisant des redondances matérielles ou analytiques, peuvent être utilisées ».

Dans de nombreuses industries, les besoins en matière de sûreté de fonctionnement constituent depuis longtemps un enjeu majeur dans le domaine de la gestion des risques. Cet enjeu sera indiscutablement impacté par de nouveaux facteurs, induits par la modernisation des systèmes et par la mise en œuvre de nouvelles technologies (électroniques, informatiques, télécoms, etc.).

En parallèle, la sécurité des systèmes d'information est devenue une nécessité absolue dans un monde où le partage des informations est souvent indispensable et où l'utilisation des systèmes numériques est croissante. De manière générale, la mise en œuvre de ces systèmes et leur exploitation implique le développement et la mise en place d'environnements de confiance. Cette constatation est de plus en plus avérée pour le domaine des systèmes de contrôle et de supervision industriels, qui intègrent désormais presque systématiquement des services et technologies largement utilisées dans le secteur des télécoms et de l'informatique dite « tertiaire ». Or, l'interconnexion des systèmes et les besoins de maintenance conduisent à une augmentation des menaces sur l'ensemble des technologies numériques, y compris pour les architectures qui étaient jusqu'alors plutôt épargnées. Ce contexte fait apparaitre de nouveaux risques pour les infrastructures sensibles ou critiques des États et de certains secteurs d'activités dits « d'importance vitale » (SAIV).

Aux Etats-Unis, en 2011, le *Department of Homeland and Security* (DHS) a conduit 78 évaluations dans des sociétés exploitants des systèmes de contrôle, permettant à celles-ci d'identifier des écarts de sécurité et de prioriser des mesures de réductions de ces écarts. Le DHS a également fortement encouragé les propriétaires et opérateurs de ces systèmes à réaliser des tests d'auto-évaluation dans l'objectif final de réduire les risques.

L'estimation des garanties et de l'assurance que peut apporter une certification n'est pas une chose simple. En effet, en matière de certification, de quoi parle-t-on vraiment ? D'exigences portées sur un système complet, sur certaines parties d'un système, de ces composants, de certains de ses composants, de certaines de ses fonctionnalités, de certaines briques logicielles ou matérielles mises en œuvre par ces

[1] La sécurité fonctionnelle est la partie du système de sécurité général qui dépend du fonctionnement correct des processus ou équipements en réponse à ses entrées.

fonctionnalités ? Par ailleurs, tient-on réellement compte de l'environnement dans lequel un système ou composant certifié est installé, et surtout de l'assurance qui est apportée par les autres éléments installés dans l'environnement du système lui-même ? Autant de questions à multiples réponses pour des environnements complexes tels que les systèmes industriels.

3 Premiers éléments de réflexion

Sans moyens de défense complémentaires, les systèmes d'automatismes et de contrôle de procédés ne sont pas réputés pour leur absence de vulnérabilités. L'une des stratégies communément recommandées pour améliorer et traiter cette problématique est d'intégrer la sécurité tout au long du cycle de vie des produits (conception, installation, maintenance, retrait). La couverture de ces aspects par les différentes certifications de sécurité est d'une importance primordiale, mais très variable selon les certifications considérées. Dans ce secteur, certaines certifications tentent de répondre aux nouveaux besoins de confiance et d'assurance.

Toutefois, ces certifications, si elles peuvent paraître rassurantes de prime abord, ne doivent pas masquer la dérive possible de la mise en place d'une confiance trop importante dans des systèmes ou composants certifiés. Un système industriel est constitué de multiples éléments interconnectés. Il faut garder en tête que la sécurité globale reposera toujours sur le niveau de confiance et de sûreté apporté à l'élément le plus faible ou le plus exposé de l'ensemble, incluant également les interventions et opérations humaines.

Le domaine de la certification est foisonnant. La figure 1 présente une recherche d'acteurs internationaux sur la thématique, en fonction des mots clés apparaissant dans les cinq rectangles de couleurs différentes :

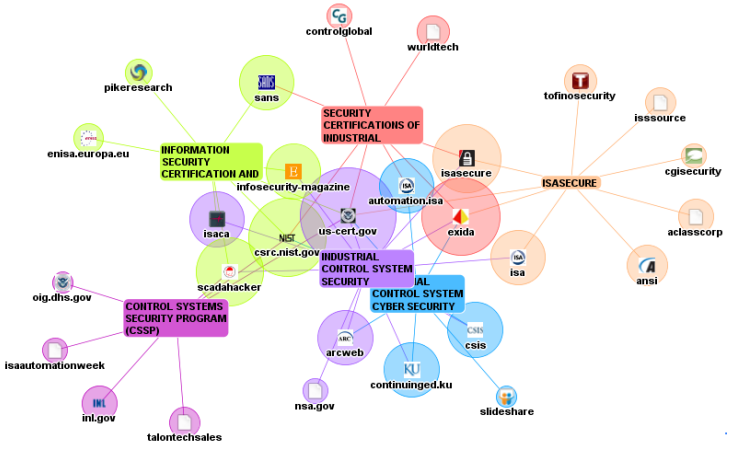


Fig. 1. : Résultat d'une recherche cartographique sur la thématique avec l'outil « Touchgraph »

4 Principes de certification

4.1 Définition

Selon l'organisme d'accréditation français COFRAC [1] *« La certification est une procédure par laquelle une tierce partie, l'organisme certificateur, donne une assurance écrite qu'un système d'organisation, un processus, une personne, un produit ou un service est conforme à des exigences spécifiées dans une norme ou un référentiel. La certification est un acte volontaire qui peut procurer aux entreprises un avantage concurrentiel. C'est un outil de compétitivité qui établit la confiance dans leurs relations avec leurs clients. Elle est délivrée par des organismes certificateurs indépendants des entreprises certifiées ainsi que des pouvoirs publics. »*

En France, les référentiels publiés par l'AFNOR[2] (ou par les organismes ayant reçu une délégation de l'AFNOR), sont appelés « normes françaises homologuées » et sont par principe d'application volontaire (article 17 du décret de 2009[3]) mais certaines prennent force de loi, devenant d'application obligatoire par arrêté signé du ministre chargé de l'Industrie et du ou des ministres intéressés. Les normes rendues d'application obligatoire sont listées sur le site internet de l'AFNOR et référencés dans les lois, décrets et arrêtés.

Quoiqu'il en soit, tous les standards, normes et guides de bonnes pratiques ne donnent pas systématiquement lieu à des certifications. Selon *Wikipédia, « en marge des normes et standards,* le terme **« bonnes pratiques »** *désigne, dans un milieu professionnel donné, un ensemble de comportements qui font consensus et qui sont considérés comme indispensables par la plupart des professionnels du domaine, qu'on peut trouver sous forme de guides de bonnes pratiques (GBP). Ces guides sont conçus par les filières ou par les autorités. Ils peuvent se limiter aux obligations légales, ou les dépasser. Comme les chartes, ils ne sont opposables que s'ils ont été rendus publics. Ils sont souvent établis dans le cadre d'une démarche de qualité ».*

4.2 Objectifs

Le but originel de la certification et la quintessence même de son existence est de mettre en place de la confiance. Cette confiance, élément essentiel pour tout système informatisé ou automatisé est obtenu par la mise en œuvre de mécanismes permettant de garantir que les fonctions s'exécutent normalement et sans perturbations aucune. Comme le décrit Christian Damour dans son papier présenté à SSTIC[4] en 2007 [2], « en matière de sécurité des systèmes d'information, la problématique de la confiance est une préoccupation essentielle de tous les acteurs : confiance dans les produits mis

[2] Association Française de Normalisation

[3] Le Décret nº 2009-697 du 16 juin 2009 relatif à la normalisation, paru au JORF du 17 juin 2009, explicite le fonctionnement du système français de normalisation et rappelle la mission d'intérêt général de l'Afnor, ainsi que la procédure d'élaboration et d'homologation des projets de normes et les modalités d'application des normes homologuées

[4] Symposium sur la Sécurité des Technologies de l'Information et de Communication

en œuvre, confiance dans les offres de service des opérateurs, confiance dans le système d'information de l'entreprise et les processus mis en œuvre, confiance dans les acteurs qui sont concernés au premier chef par le niveau de sécurité global d'un système d'information ».

Dans les domaines de l'industrie et des services, il existe plusieurs types de certifications qui répondent chacun à des besoins différents. Un dispositif de certification peut porter sur tous les domaines d'activité ou seulement sur certains secteurs bien délimités ; il peut s'appliquer à toute l'entreprise ou seulement à certaines de ses fonctions. L'évaluation peut porter sur certains processus, sur des personnes physiques, sur des produits ou sur des services particuliers.

On peut rencontrer des démarches de « labellisation » ou « contrôlé par un organisme indépendant ». Elles ne constituent pas des certifications. Ces pratiques ne sont pas encadrées par des dispositions réglementaires mais sont licites tant qu'elles n'induisent pas de confusion avec une véritable certification dans l'esprit du public. Il faut également noter qu'une certification n'est pas une indication d'origine ou de provenance géographique comme peut l'être un label. Ces différences et subtilités doivent bien sûr être prises en compte dans l'appréhension de la problématique de la certification sécurité des systèmes numériques industriels.

Dans le domaine de la sécurité informatique, la grande innovation des ITSEC[5] et des Critères Communs a été d'exiger la formalisation et la mise en œuvre des bonnes pratiques dans les processus de développement, d'évaluation et de production. Dans quelle mesure sont-elles adaptées au contexte industriel ? Plus généralement, quel degré de confiance accorder dans ces conditions à un système certifié ? N'est-ce pas une manière de s'affranchir de certaines responsabilités pour des fournisseurs, ou pour un propriétaire ou opérateur de système industriel de se fourvoyer pour un quant au réel apport de la certification ? Quelle pérennité en matière de garanties apportées pour la sécurité informatique, domaine dans lequel nous savons évidemment que la réalité des garanties accordées à un instant ou une période données vont forcément changer, plus ou moins rapidement, en fonction de l'évolution des menaces ?

4.3 Référentiels de certifications

Pour être reconnue et faire preuve de sa valeur, une certification doit s'appuyer sur un référentiel de normes et standards partagés par la communauté du secteur d'activité considéré. Ce référentiel est donc constitué de documents techniques définissant les caractéristiques que doivent présenter un produit pour répondre à un certain nombre de critères satisfaisant des objectifs prédéfinis.

De plus, d'après [3] le référentiel de certification peut prendre en compte les points suivants :

[5] *Information Technology Security Evaluation Criteria*

- La nature et le mode de présentation des informations considérées comme essentielles et qui doivent être portées à la connaissance des consommateurs ou des utilisateurs ;
- Les méthodes d'essais, de mesures, d'analyses, de tests ou d'évaluations utilisées pour la détermination des caractéristiques certifiées et qui, dans la mesure du possible, devront se référer aux normes homologuées existantes ;
- Les modalités des contrôles auxquels procède l'organisme certificateur et ceux auxquels s'engagent à procéder les fabricants, importateurs, vendeurs des produits ou prestataires de services faisant l'objet de la certification ;
- Le cas échéant, les engagements pris par les fabricants ou prestataires concernant les conditions d'installation des produits ou d'exécution des services certifiés, les conditions du service après-vente et de la réparation des préjudices causés aux utilisateurs ou consommateurs par la non-conformité du produit ou du service aux caractéristiques certifiées.

5 Standards spécifiques au domaine industriel

5.1 Les standards ou référentiels approuvés

Il existe plusieurs normes et standards internationaux qui permettent d'appréhender la problématique de la **sécurité informatique pour les systèmes industriels**. Dans ce chapitre, nous allons aborder les principaux référentiels qui peuvent donner lieu à des certifications ou à des labellisations de produits de sécurité utilisables dans le secteur dit « industriel ».

- **FERC/NERC CIP 2 à 9** [4]; Energy FERC (*Federal Energy Regulatory Commission*) Elle couvre l'ensemble des aspects de la sécurité, y compris deux originalités: le processus de déclaration d'un incident, et celui de continuité d'activité (PCA).
- **NIST SP 800-82** ; « Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)». Ce guide décrit le contexte des systèmes industriels de contrôle face au changement d'environnement actuel décrit dans la section 1 ; il définit les menaces et vulnérabilités, identifie les bonnes pratiques dans un principe d'application de la défense en profondeur.
- **NIST SP 800-53** ; « Recommended Security Controls for Federal Information Systems and Organizations » ; ce guide offre une panoplie de mesures de sécurité adaptées à la classification des systèmes considérés, obtenus par l'application des **FIPS 199** « Standards for Security Categorization of Federal Information and Information Systems » et **FIPS 200** « Minimum Security Requirements for Federal Information and Information Systems ».
- **NEI 08-09** ; « *Cyber Security Plan for Nuclear Power Reactor* ». Ce document a été développé pour servir de guide permettant de répondre aux exigences du « *Code for Federal Regulations* » définies par le référentiel 10, Part 73, Section

73.54 de la NRC[6]. Ce référentiel décrit les exigences générales pour la « Protection des systèmes informatiques et des réseaux et systèmes de communication[7] » pour le contexte des installations nucléaires civiles. L'exigence principale de la NRC[8] est l'établissement et la soumission aux autorités d'un « Cyber Security Plan ».

- **IAEA NSS 17** « *IAEA Nuclear Security Series #17, reference manual- Computer security at nuclear facilities*": Les manuels de référence sont au rang le plus bas de la pyramide documentaire de la série « Sécurité » de l'AIEA. De plus, contrairement à la série des standards « Sûreté », ces documents n'ont pas de caractère prescriptif, les États étant souverains en termes de sécurité. Cependant, étant donné le paysage actuellement vierge en termes de références internationales sur la sécurité informatique des installations nucléaires, et la crédibilité de l'AIEA auprès des États et de leur autorités de régulation, ce document fait référence.
- **IEC 62351-6 «** *Data and communications security* » [5] : Le périmètre de cette série de standard IEC est la sécurité de l'information pour les opérations de contrôle des systèmes électriques (de puissance). Tel que décrit dans la norme en anglais : « *The primary objective is to* "*Undertake the development of standards for security of the communication protocols defined by IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. Undertake the development of standards and/or technical reports on end-to-end security issues* ».

5.2 Les standards en construction

Pour le domaine nucléaire, la future **norme IEC 62645** a été lancée en avril 2009 par un projet de norme internationale sur la sécurité informatique des centrales nucléaires. Elle vise à préciser les exigences à respecter pour établir un « programme » de sécurité informatique (ensemble de mesures) adapté aux systèmes critiques.

Le référentiel **IEC 62443** constitue également un ensemble de documents en construction, relatif à la « cyber sécurité des processus industriels de mesure et de contrôle ». A noter que le référentiel « CEI 62443 » est principalement issu du groupe de travail ISA99 et du standard ISA associé.

6 Panorama des certifications applicables au domaine industriel

6.1 Les certifications répondant aux exigences « Critères Communs »

La norme **ISO/CEI 15408** ou ***Common Criteria*** (*Common Criteria for Information Technology Security Evaluation*) définit les critères communs pour l'évaluation de la sécurité des technologies de l'information [22]. Dans le domaine des produits, systèmes informatiques, solutions et services à valeur ajoutée, les Critères Communs

[6] *United States Nuclear Regulatory Commission*
[7] *Protection of digital computer and communication systems and networks*
[8] *Nuclear Regulatory Commission*

constituent un référentiel complexe, difficile à appréhender, mais ayant démontré une réelle efficacité, et possédant de nombreux atouts. Ce référentiel [22] présente les qualités suivantes :

- Il est générique dans ses applications à tout type de produit ou système (logiciels, matériels, systèmes, réseaux, solutions complexes à haute valeur ajoutée), mais souvent fustigé pour sa complexité et les difficultés d'appréhension que cela engendre.
- Il garantit la confiance dans les résultats à travers le recours à des organismes dont la compétence et l'indépendance sont reconnus.
- Il est normalisé à l'échelle mondiale.
- Il fait l'objet d'une reconnaissance internationale des certificats. Un certificat émis dans un pays a la même valeur dans tous les pays au monde signataires des accords.

Le document [7] décrit précisément les principes de l'évaluation des produits sur la base des critères communs définis par la norme. L'extrait figure 2 en montre le concept.

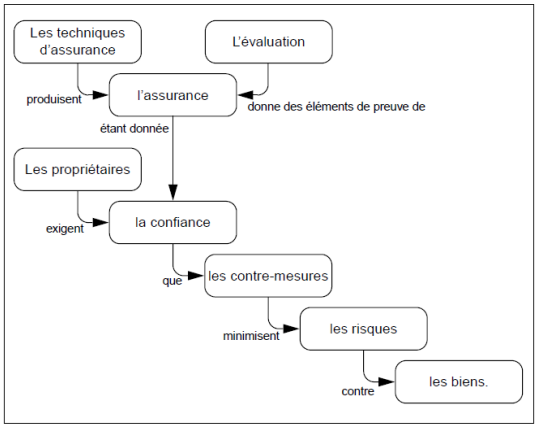


Fig. 2. Concept de l'évaluation Critères Communs (source [7])

6.2 Les Certifications ACHILLES

Les certifications « Achilles » de la société ***Wurldtech*** portent sur deux volets différents :

- La certification de produits,
- La certification des processus des entreprises fabricants des produits de contrôle industriel (par exemple Schneider-Electric).

Commençons par une description rapide du second processus : le ***Achilles Practices Certification*** (APC) [8].

A l'origine de cette certification on trouve une association de clients de produits de contrôle industriel. Ensuite, le *International Instrument Users Association* (WIB) va

s'appuyer sur un ensemble d'exigences de sécurité [9], qu'il est possible d'obtenir sur http://www.wib.nl/download.html en se déclarant nominativement. Le niveau de certification est en fait attribué en fonction du niveau de maturité atteint dans la gestion des processus organisationnels, du niveau des exigences générales sur les produits fabriqués (durcissement, authentification, etc.) et enfin sur les exigences mises en œuvre durant les phases de mise en service et de maintenance. Le processus formel s'appuie sur le modèle de maturité SSE-CMM décrit à la référence [10]. Des acteurs importants comme **Emerson, Honeywell, Sensus** et plus récemment **Siemens et Yokogawa** disposent de cette certification.

Le ***« Achilles Communication Certification »*** (ACC) [11]_est la certification industrielle la plus répandue. Elle s'appuie sur les exigences de l'ISA 99 et sur une batterie de tests mise en œuvre par un outillage développé par Wurldtech, permettant de faire des tests de vulnérabilités sur les protocoles (vulnérabilités connues), d'erreurs d'implémentation (permettant par exemple l'exécution de *buffer over flow*), de dénis de services (attaques DoS) sur les CPU et mémoires par l'envoi de très nombreux paquets de données.

Le processus s'appuie sur une plate-forme de test propriétaire (Achilles Test Platform – *figure 13*) permettant d'exécuter les tests de robustesse. Les tests sont réalisés à partir d'algorithmes de type Fuzzing propriétaires Wurldtech et de tests de vulnérabilités.

Fig. 3. : Plateforme de test ATP (Achilles Test Platform) [source Achilles]

6.3 Les Certifications ISASecure

Le programme de certification ISASecure [12] a été développé par un consortium industriel dénommé « ISA Security Compliance Institute » (ISCI) dans le but d'accélérer une large amélioration de la cybersécurité des IACS[9]. La certification ISASecure EDSA[10] a pour objectif de remplir ce rôle en offrant une assurance et une reconnaissance des produits pour leur réponse aux exigences de sécurité demandé par le consortium. Elle s'apparente aux niveaux de certification SIL (*Security Integrity Level*) définis par la norme ISO/IEC 61508 relative à la sureté de fonctionnement. Tel que défini dans [13], ce programme concerne potentiellement tous les matériels embarquant du logiciel permettant de superviser, de contrôler ou d'agir sur un process industriel, incluant directement les matériels suivants :

[9] *Industrial Automation and Control Systems*
[10] *Embedded Device Security Assurance*

- PLC (Programmable Logical Controller),
- Capteurs/Actionneurs,
- SIS Controller (Safety Instrumented System Controller),
- DCS Controller (Distributed Control System Controller).

Le programme fournit trois niveaux de certification offrant une assurance croissante. Le socle *Communication Robustness Testing* (CRT) défini par les spécifications [14] reste commun aux trois niveaux. Les exigences augmentent pour les niveaux 2 et 3 selon les spécifications techniques définies pour le « *Functional Security Assessment* » [15] et pour le « *Software Development Security Assessment* » [16]. La *figure 4* positionne ces niveaux.

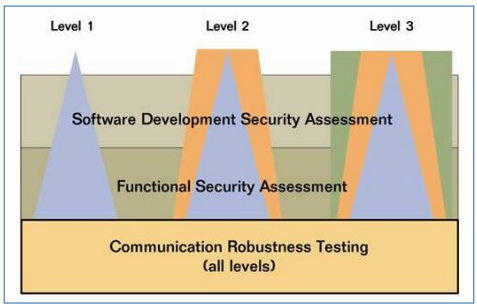


Fig. 4. Niveaux de certification ISASecure EDSA (source ISASecure.org)

Le schéma de certification est basé sur les référentiels énumérés figure 3. Il est bâti sur :

- Des spécifications techniques suivant les principes de l'ISA-99 TR-04.01,
- Des exigences d'accréditations pour les laboratoires et centres d'évaluation,
- Des références normatives (ISO/IEC 62443, ISO/IEC 17025, etc.).

Le niveau de certification obtenu dépendra de la réponse aux exigences des référentiels [15] et [16]. Les exigences du FSA [15] portent sur la mise en œuvre de mesures sur les items suivants qui se basent en grande partie sur les propositions du ***NIST SP 800-53*** *:*

- Contrôle d'accès,
- Protection, mesures d'audit,
- Intégrité des données,
- Confidentialité des données,
- Restriction des flux,
- Réponse sur incidents,
- Disponibilité des ressources réseau.

Les exigences du SDSA [16] portent quant à elles sur la mise en œuvre de mesures sur les items suivants (relatifs au développement des logiciels) et se basent sur des

exigences de sureté de fonctionnement probabilistes (IEC 61508) et sur des exigences Critères Communs (ISO/IEC 15408) :

- Process de management de la sécurité dans les logiciels,
- Spécifications des exigences de sécurité,
- Intégration de la sécurité dans la conception du logiciel,
- Modélisation des menaces et évaluation des risques,
- Meilleures pratiques de développement,
- Production de guide d'usage pour les utilisateurs,
- Développement et implémentation sûre des codes,
- Tests d'intégration de la sécurité (*fuzzing*, test de pénétration),
- Plan de réponse à la découverte de vulnérabilités ou de problèmes de sécurité,
- Confirmation que toutes les exigences ont été mises en œuvre et vérifiées,

A ce jour encore peu de matériels ont reçu une certification **ISASecure**, ils sont publiés sur le site de l'ISA[11].

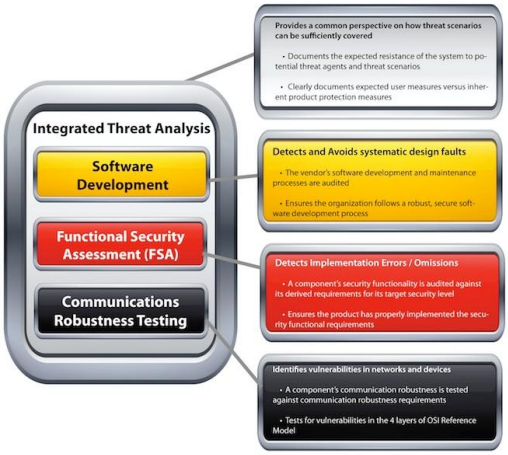


Fig. 5. : Processus de certification ISASecure EDSA (source ISASecure.org)

6.4 Certification FIPS du NIST

Le standard américain « Federal Information Processing Standards - FIPS 140-2 définit un ensemble d'exigences de sécurité applicables aux modules cryptographiques. Le National Institute of Standards and Technology (NIST) des États-Unis et le Communications Security Establishment (CSE) du Canada ont agi en qualité d'autorités de certification pour la norme FIPS 140-2. Les modules certifiés sont acceptés par les agences fédérales des deux pays aux fins de la protection d'informations sensibles, et d'autres gouvernements et entreprises du monde entier exigent la norme FIPS 140-2 sur les produits qu'ils emploient.

[11] *International Society of Automation disponible à www.isasecure.org*

6.5 Les certifications TUV : focus sur la « Sécurité Fonctionnelle »

Les normes IEC 61508 et IEC 61511 sont de véritables outils normatifs de la « sécurité fonctionnelle ». Ils permettent, à partir du cycle de vie des systèmes instrumentés de sûreté, d'analyser et de réaliser toutes les phases indispensables à leur conception, leur mise en œuvre et leur exploitation. Des organismes certificateurs comme les TUV [17] sont spécialisés dans les produits et installations industriels et s'appuient sur ces standards pour délivrer des certifications, y compris sur les développements de codes de sûreté ou des composants tels que des FPGA.

Par exemple, TUV-SUD Automotive a certifié conforme aux standards IEC 61508 l'analyseur de code source « QA-C » de *Programming Research* QA pour le domaine des logiciels critiques de sûreté [18]. Le problème de ces certifications de « sûreté » est qu'elles excluent les défaillances dites de « causes communes », ce qui est acceptable dans un contexte de tolérance aux fautes et aux pannes, mais qu'il est difficile de totalement évacuer dans le contexte de la malveillance !

6.6 Certifications de sécurité informatique en France

L'agence nationale de la sécurité des systèmes d'information, Autorité nationale en matière de sécurité des systèmes d'information, est chargée d'organiser la délivrance, voire de délivrer, au nom du Premier ministre, des labels de sécurité à des produits et à des prestataires de services de confiance. Elle délivre des certifications « produits » et « prestataires :

- Labels délivrés aux produits des technologies de l'information :
  - la certification Critères Communs (CC) selon la norme CEI 15408 [6] ;
  - la certification de sécurité de premier niveau (CSPN) ;
  - la qualification d'un produit ;
  - l'agrément (label réservé aux produits destinés à protéger les informations relevant de la défense et de la sécurité nationale).
- Labels délivrés aux prestataires de services de confiance :
  - la qualification d'un prestataire.

Les certificats émis par l'ANSSI, attestent que les produits certifiés sont conformes à une spécification technique appelée « cible de sécurité ». Cette cible de sécurité peut elle-même être certifiée conforme à un cahier des charges appelé « profil de protection ». Le profil de protection permet d'exprimer des exigences de haut niveau et peut-être partagée par une communauté d'intérêts telle que la communauté bancaire, celle de la santé ou du transport, etc.

Les produits ou systèmes certifiés peuvent arborer la marque " Certification Sécurité TI " ci-après :

Cette certification s'appuie sur des critères, une méthodologie et un processus élaborés par l'ANSSI. La documentation sur l'ensemble de ces points est disponible sur le site de l'Agence.

Le principe général de la CSPN est de proposer une évaluation en charge et délai contraints pouvant mener à une certification. Les évaluations sont réalisées par des centres d'évaluation agréés par l'ANSSI. Ces centres sont plus communément appelés CESTI

Il est toutefois important de noter qu'il n'existe pas pour le moment de protocole ou de méthodologie pour faire l'évaluation de matériels dits « industriels » tels que des automates industriels ou des systèmes programmés au sens de la norme CEI 61508 et des normes qui en découlent par secteur.

7 Les avis d'experts et spécialistes du domaine

De nombreux acteurs (institutionnels, presse spécialisée, industriels, etc.) peuvent prôner que le principe de certification des produits trouve parfaitement sa place dans l'application du principe de défense en profondeur. **Angela Godwin** de la revue « ***WaterWorld*** », décrit par exemple dans son article « *Water and Wastewater Cyber Security: Strengthening the Chain* » [19], que l'évaluation des systèmes industriels et la détection de leurs faiblesses est un pré-requis à la mise en place de mesures de sécurité. Elle évoque l'utilisation d'ISASecure et des outils d'évaluation du DHS tels que CSET[12] [20]. On pourrait donc légitimement penser que le marché de la certification est promis, compte tenu des enjeux, à un bel avenir. Toutefois, la prise en compte de la sécurité à tous les niveaux dans les organisations est le réel challenge. La reconnaissance de l'intérêt des démarches de certification passe par une élévation du niveau de maturité des organisations.

Dans un récent article datant de juin 2012, **S.J. Murdoch** [21] décrit les faiblesses des certifications et tire certaines leçons de l'histoire des certifications de sécurité, notamment par l'étude détaillée et les prévisions du rapport « Ware » [22] établi dès 1970 ! Il aborde notamment largement la difficulté de certifier un système dans la durée, d'un coté parce que les coûts et investissement en temps sont conséquents, et de l'autre parce que la certification répond à une cible de sécurité identifiée à un instant (t), dans un environnement où les menaces sont en perpétuelle évolution. Les auteurs de l'article prennent l'exemple de terminaux de paiement pour cartes assujettis et bénéficiant de certification Critères Communs avec un Profil de Protection adapté et démontre comment l'objectif de protection du secret du code PIN peut être facilement détourné. Par ailleurs, la chasse aux fabricants se targuant de disposer de certifications alors que ce n'est pas (ou plus) le cas (sur l'ensemble des produits) n'est que rarement mise en œuvre et les sanctions restent visiblement très peu contraignantes.

Les certifications coutent cher, mais elles sont aussi souvent attribuées à une partie seulement des composants des produits ou des systèmes. L'exemple des clés USB « Stealth MXP » est probant [23] : ces clés ont été certifiés FIPS-140 par leur implémentation de l'algorithme de chiffrement AES-256, toutefois des vulnérabilités dans d'autres fonctions ont permis le vol des mots de passe. Le produit se base par ailleurs sur une authentification multi-facteurs avec notamment l'utilisation d'une empreinte digitale comme élément secret. Par ailleurs, bien qu'ayant mis en œuvre correctement

[12] *Cyber Security Evaluation Tool*

l'algorithme AES, plusieurs failles de conception du logiciel de pilotage pour le déverrouillage de la clé ont été mises en évidence ; elles permettent assez facilement l'obtention des mots de passe « hashés » avec l'algorithme SHA-1, dont il est aisé de retrouver le « clair » à l'aide de « *rainbow table* » [23].

Pareillement, **K.M. Goertzel** [24] note que « la sécurité logicielle est une propriété dynamique, les logiciels qui sont sécurisés (« au sens sûrs ») dans un environnement particulier au sein d'un périmètre de menace défini, ne le resteront pas longtemps si l'environnement change ou si le logiciel lui-même connait des modifications ». Ce qui indique qu'une certification de sécurité significative doit concerner un produit ou un système dans son environnement final d'utilisation, incluant les processus organisationnels et opérationnels. La même analyse est faite par **R. Schierholz** de chez ABB dans un document [25] publié par le DHS13, où il explique qu'un produit certifié un jour contre telle malveillance devrait être régulièrement inspecté au vue du nombre croissant « d'*Exploits* » ou de vulnérabilités découvertes. Par ailleurs il décrit une faille dans les schémas de certifications eux-mêmes, qui veut que les organismes certificateurs ne soient pas responsables des implémentations faites avec les produits certifiés ; R. Schierholz remet ensuite l'accent sur le fait qu'un faux message peut être transmis au marché et aux acheteurs ou opérateurs de produits certifiés, laissant penser que parce que le produit acheté est certifié, la mission est remplie. Comme nous l'avons déjà évoqué, la sécurité peut dépendre de la qualité des matériels mais aussi et surtout de la façon dont ils sont mis en œuvre et sont exploités. L'auteur encourage donc plutôt les acteurs industriels (fabricants/vendeurs, acheteurs/ utilisateurs) à profiter de leurs relations clients/fournisseurs historiques pour faire avancer conjointement les réponses aux problèmes de sécurité et à développer des exigences communes.

D'après **R. Anderson** dans son article coécrit avec **S. Fuloria** [26], imposer des certifications de type Critères Communs dans le domaine des systèmes industriels de contrôle serait une hérésie. La notion de « Profile de Protection » n'est selon lui pas adaptée au domaine industriel et n'aurait d'ailleurs pas fait ses preuves dans le domaine de l'IT pour les raisons que nous avons évoquées plus haut. Les opérateurs de ces systèmes devraient par conséquent être au centre des expressions des besoins de sécurité, de par leurs responsabilités et par leur connaissance des environnements d'exploitation et de production. Par ailleurs, ces auteurs sont plutôt favorables à l'émergence de certifications comme ISASecure et Achilles.

8 Conclusion

Déjà décrit au STICC 2007 par **C. Damour** [2] : « à l'heure de la mondialisation et de la dématérialisation des échanges, la sécurité des systèmes d'information se doit de mettre en œuvre une approche globale, qui ne soit plus fondée sur une approche purement technologique, comme nous pouvons parfois être amenés à le croire. S'agissant de sécurité, la résistance d'une chaîne est souvent celle du maillon le plus faible (même une fois toutes les précautions prises, une seule faille ou combinaison de failles suffit au pirate à pénétrer un système) ».

[13] *Department of Homeland Security*

La mesure de l'assurance que peut apporter une certification n'est pas une chose simple. En effet, de quoi parle-t-on vraiment en matière de certification ? D'exigences portées sur un système complet, sur certaines parties d'un système, de ses composants, de certains de ses composants, de certaines de ses fonctionnalités, de certaines briques logicielles ou matérielles mises en œuvre par ces fonctionnalités ? Même si le périmètre de la certification est précisé, tient-on vraiment compte de l'environnement dans lequel le système est installé et surtout de l'assurance qui est apportée par les autres éléments installés dans l'environnement du système lui-même ? Autant de questions à réponses multiples.

Quel degré de confiance accorder dans ces conditions à un système certifié ? N'est-ce pas une manière de s'affranchir de certaines responsabilités pour les fournisseurs, ou pour un propriétaire ou opérateur de système industriel de se fourvoyer quant au réel apport de la certification ? Quelle pérennité en matière de garanties apportées dans un secteur où nous savons pertinemment que les risques évalués à un instant ou une période donnée vont forcément changer (plus ou moins rapidement) en fonction de l'évolution des menaces !

Les certifications, si elles peuvent paraitre intéressantes, ne doivent pas masquer les effets de bords possibles par la mise en place d'une confiance trop importante dans les composants certifiés. Un système industriel est constitué de multiples éléments interconnectés mais aussi d'éléments redondés « diversifiés » (selon les secteurs d'activité) pour remplir les fonctions essentielles.

Les certifications de type Critères Communs ou FIPS sont des certifications de conception. Il est désormais communément admis que le panorama des menaces est en perpétuelle évolution et que les systèmes cibles doivent réagir à ce changement ; Un exemple probant est le nombre de chercheurs découvrant des vulnérabilités, forçant les éditeurs ou fabricants à mettre à disposition ou à installer des mises à jour ; Ces modifications pourraient invalider les certifications et par conséquent de nouveaux tests devraient être réalisés. Cela pose évidemment aussi problème aux propriétaires et exploitants de ces matériels.

La certification des produits, systèmes et environnements informatisés a certains avantages que nous avons pu exposer dans cette note, toutefois, les leçons du rapport Ware de 1970 [22] nous enseignent clairement que l'arbre ne doit pas cacher la forêt et que certification ne doit surtout pas rimer avec illusion :

"Thus, the security problem of specific computer systems must, at this point in time, be solved on a case-by-case basis, employing the best judgement of a team consisting of system programmers, technical hardware and communications specialists, and security experts".

9 Références

[1] COFRAC, « Comité Français d'Accréditation », disponible à http://www.cofrac.fr/

[2] Christian Damour, « Démarches de sécurité & certification : atouts, limitations et avenir », STICC 2007.

[3] Ministère de l'Economie, des Finances et de l'Industrie, « La certification des produits industriels et des services en 7 questions », 2004.

[4] “CIP” disponible à http://www.nerc.com/pa/stand/Pages/default.aspx
[5] CEI/TS 62351 part 6, « *Power system management and associated information exchange – Data and Communication Security* », 2007
[6] ISO/CEI 15408:2005, Technologies de l'information - Techniques de sécurité - critères d'évaluation pour la sécurité TI, ISO IEC, 2006
[7] « Critères Communs pour l’évaluation de la sécurité des technologies de l’Information », Aout 1999, version 2.1, CCIMB-99-031.
[8] Achilles Practice Certification disponible à http://www.wurldtech.com/product_services/certify_educate/achilles_practices_certification/
[9] International Instrument Users’ Association WIB, « Process Control Domain – Security Requirements for Vendors », Report M2784-X10, Mars 2010.
[10] CMU, "*Systems Security Engineering Capability Maturity Model (SSE-CMM) V3.0," Carnegie Mellon University - Software Engineering Institute*, 2003.
[11] Achilles Communication Certification disponible à http://www.wurldtech.com/product_services/certify_educate/achilles_communication_certification/
[12] Programme ISASecure, disponible à http://www.isasecure.org/ISASecure-Program.aspx
[13] ISASecure EDSA-206, « *Embedded Device Security Assurance – ISASecure EDSA CRT laboratory operations and accreditation* »
[14] ISASecure EDSA-310, « *Common Requirements for Communication Robustness Testing (CRT)* »
[15] ISASecure EDSA-311, « *Functional Security Assessment (FSA)* »
[16] ISASecure EDSA-312, « *Software Development Security Assessment (SDSA)* »
[17] Conditions générales TUV Rheinland http://www.tuv.com/media/france/cofrac/conditions_generales_de_certification_201108.pdf
[18] John McConnell, « QA·C certified by TÜV SÜD for ISO 26262 and IEC 61508 compliance», disponible à http://www.programmingresearch.com/press-releases/2011/prqa-qa-c-certified-by-tuv-sud-for-iso-26262-and-iec-61508-compliance/
[19] Angela Godwin, « Water and Wastewater Cyber Security: Strengthening the Chain », disponible à http://dpwsd.waterworld.com/index/display/article-display/0535730141/articles/waterworld/volume-28/issue-4/editorial-features/water-and-wastewater-cyber-security-strengthening-the-chain.html
[20] ICS-CERT, « *Control System Assessment* », disponible à http://www.us-cert.gov/control_systems/satool.html
[21] Steven J. Murdoch, Mike Bond, Ross Anderson, « *How Certification Systems Fail: Lessons from the Ware Report* », 2012
[22] Willis H. Ware, « *Security controls for computer systems: Report of defense science board task force on computer security* », Report R-609-1, RAND Corporation, January 1970. Reissued October 1979.
[23] Philippe Oechslin, « *Screwing up security*», disponible à http://www.h-online.com/security/features/USB-stick-with-hardware-AES-encryption-has-been-cracked-746215.html, 2008.
[24] K.M. Goertzel « Introduction to Software Security) » disponible à https://buildsecurityin.us-cert.gov/introduction-software-security
[25] Ragnar Schierholz, Kevin McGrath, « Security Certification –A critical review », ABB Corporate Research, 2010
[26] Ross Anderson, Shailendra Fuloria, « Certification and Evaluation : A security Economics Perspective », disponible à « http://www.cl.cam.ac.uk/~rja14/Papers/certi_eval.pdf »

Security requirements in procurement for Electric Power Utilities

Dennis Holstein, Pascal Sitbon

holsteindk@ocg2u.com, psitbon@epri.com

Keywords: cybersecurity procurement requirements, electric power utility

Abstract. In practice it is often difficult to implement common security techniques in electric power utility's control systems because of field constraints like real-time and available resources. One other essential issue is the contractual one. For example the owner/operator is not free to choose what techniques it could implement without the explicit agreement by the solution provider. For that matter, all organizations in the supply chain are not sufficiently mature in their practice of well recognized security policies. Cybersecurity procurement requirements must address the full life cycle of the solution, beginning with design, unit testing, factory acceptance testing, site acceptance testing, maintenance and support, and decommissioning and disposal.

Because rapid developments in the threat landscape outpace the development and deployment of mitigation technologies, the procurement requirements must be "future proof." Future proofing procurement requirements requires the full attention of all stakeholders with a vested interest in solution development, integration, operation, support services, regulatory enforcement. This paper will present and discuss different inputs like the procurement language developed by US Department of Homeland Security (DHS) and Department of Energy (DOE), or ISO/IEC 27036. Also the paper includes the framework for grading criteria that can be used to compare the security maturity offered in tenders responding to request for proposals.

1 Cybersecurity standards are available, but!

There is not a lack of cybersecurity standards. Standards, guidelines and best practices address to a great extent cybersecurity requirements for an electric power utility (EPU) operator to design a strong cybersecurity program, efficiently operate the program, and specify technical security controls to mitigate known threats. These requirements commonly address access control (identification and authentication), use control, data confidentiality and integrity, restricting data flow, timely reporting of events, and ensuring communication network resource availability. They are more and more taking into account the specifics of industrial systems such as safety first, primacy of availability and integrity over confidentiality, architecture and system

constraints, etc. Examples include IEC 62443, NISTIR 7628, ISO/IEC 27019, and the NERC CIP.

Some standards (like IEC 62351) include security interoperability requirements for selected communication protocols. Other standards address legacy systems using serial communication protocols (IEEE 1711). And, the list goes on.

Procurement language guidelines such those developed by US Department of Homeland Security (DHS) and Department of Energy (DOE), or ISO/IEC 27036 lay an excellent foundation to help EPU to integrate security into the procurement cycle, but they do not include any grading criteria to compare and rate the security maturity offered in a proposed solution.

A major weakness is the lack of "future proofing" requirements and procurement language to adequately respond to the volatile threat landscape and to take timely advantage of the technical advances to improve the capability to minimize the impact of a previously unknown cyber-attack.

2 Future proofing procurement security requirements

Future proofing procurement security requirements must address five categories:

1. organizational requirements for the contractor's policies and procedures to ensure alignment with EPU's security objectives,
2. system capability requirements for security functions designed into the contractor's system,
3. system testing and commissioning requirements to demonstrate effective security implementation including interoperability of security functions,
4. maintenance and support requirements to demonstrate due diligence in tracking threats to their system and responding with system patches to mitigate the impact of these threats, and
5. decommissioning and disposal requirements to demonstrate secure retirement of components and sensitive data.

To date we have discovered 37 security control objectives that address the five categories shown above. For example:

- contractor organizational requirements focus on the need to prepare and inform contractor personnel to be aware of security vulnerabilities in their products and services,
- examples of system security capability requirements focus on hardening the system, protecting the system from malware and viruses, securing wireless and remote access connections, and protecting sensitive data such as cryptographic keys for encrypted communications to external substation interfaces,
- testing and commissioning security requirements focus on demonstration of security capabilities by including the phrase "the contractor's system shall demonstrate" as part of the requirement,
- maintenance and support security requirements also focus on the demonstration of diligent maintenance of security functions as part of the EPU's normal maintenance cycles, and

- decommissioning and disposal security requirements focus on the contractor's policies and procedures to securely archive or destroy sensitive data.

EPUs recognize that effective security capabilities designed into the contractor's systems and services comes with a cost, which can be significant. In response to the cost implications we devised a simple grading scheme to prioritize the procurement security requirements. Based on a consensus of EPU subject matter experts (SMEs) an initial grade was assigned to each requirement. However, this assignment is only a guideline which requires each EPU to carefully tailor the assignment for their solicitation.

We examined several grading schemes such as Carnegie-Mellon's CMMI technique. A prototype of the CMMI scheme was tested by Wurldtech Security Technologies using the WIB-based security technologies modified for EPU applications. The test contractors and EPU found the multi-dimensional CMMI scheme too complex. As a result a simple three-level grading scheme was synthesized. Bronze, Silver and Gold assignments were developed to discriminate increasing contractor security maturity practices and implementation. We further refined this grading scheme for EPU's to compare contractor offers in response to the EPU's solicitation for systems and services.

We tested the simple grading scheme using an example procurement of a security enabled electric power delivery substation gateway. For this example we selected from the categories described above the applicable security requirements. Analysis of these requirements suggested procurement language. Examples include the following.

> ***[Contractor]*** *shall ensure that all substation gateway equipment (hardware and software) and support services delivered shall have networking protocols enabled with the purpose or intent to connect to* ***[EPU's]*** *operational TCP/IP wide area network (WAN) which provides the interface to the utility enterprise providing centralized services for identity management, engineering applications, supervisory control and data acquisition, and asset monitoring. The WAN interface is declared untrusted; therefore, the substation gateway shall provide the necessary security protection.*
>
> ***[Contractor]*** *shall ensure that all substation gateway equipment (hardware and software) and support services delivered shall have networking protocols enabled with the purpose or intent to connect to* ***[EPU's]*** *substation internal TCP/IP local area network (LAN) which provides the interface to the local stationary substation user interface workstation; portable configuration, maintenance, and testing tools; Global Positioning System (GPS) time synch; monitoring IEDs; and protection and control IEDs (including remote terminal units for SCADA). The LAN interface to GPS is trusted; all other LAN interfaces are untrusted.*
>
> *Substation gateway security requirements and requirement enhancements qualified by the* ***[Contractor]*** *as preplanned product improvements (P3I) shall be accepted by the* ***[EPU]*** *only if the qualification is supported by a well-defined, and approved, resource plan and milestone implementation plan.*

*To demonstrate compliance of the substation gateway equipment, software and services, the **[Contractor]** shall provide to the **[EPU],** on acceptance of order at no cost to **[EPU]**, certificate of security compliance issued by a recognized and approved authority – Bronze is required, Silver is desired, Gold receives special contractor selection consideration.*

Based on discussions with SMEs, the term "recognized and approved authority" required further clarification. Specifically, the recognized and approved authority may be the contractor's self-audit authority; an energy sector recognized authority, or an authority specified by local laws and regulations which have been tailored for specific power authorities or for EU/country authorities.

3 EPU's preference for contract types

Historically, EPUs prefer to use firm-fixed-price contracting to procure their power delivery system solutions. While this works well for well understood control system functionality, it doesn't seem to properly incentivize contractors to build security into their products and services. Such an incentive needs to be in the form of fixed-price for the initial delivery of the solution with a performance based incentive contract option for maintenance and support. How to structure the procurement language and incentive program will depend on the maturity level of the security standards to be enforced and the maturity level of the contractor's security policies and practices.

This paper considered types of contracts by comparing their advantages and disadvantages and the order which trade-offs will be made. We begin with the comparisons shown in Table 1.

Cost-reimbursable contracts are generally labor intensive and require additional scrutiny in regards to the contractor's cost accounting system. Under a cost-reimbursable contract, the contractor agrees to provide its best effort to complete the required contract effort. Cost-reimbursement contracts provide the payment of allowable incurred costs, to the extent prescribed in the contract. These contracts include an estimate of total cost for the purpose of obligating funds and establishing a ceiling that the contractor cannot exceed (except at its own risk) without approval of the contracting officer.

Table 1 Comparison of three basic contract types

Comparison criteria	Firm-fixed-price	Cost-reimbursable	Time & materials
Product delivery	The contractor is required to deliver the product and/or perform the services requires as specified in the statement of work.	The contractor is only required to deliver "best effort" to provide the specified product or service.	The contractor is only required to deliver "best effort" to provide the specified product or service.
Commercial items	This type of contract may be used for the acquisition of commercial product or services.	This type of contract is ill-advised for the acquisition of commercial items.	This type of contract may be used for the acquisition of commercial services.
Risk	The contractor accepts more responsibility for performance costs and resulting profits or losses.	The client accepts more responsibility for performance costs and resulting fee.	The client accepts more responsibility for performance costs. There is minimal incentive for the contractor to perform efficiently and control costs.
Level of security maturity	Requires well-defined security standards and supporting profiles (implementation agreements) and properly vetted contractor enforcement of security policies and practices.	The maturity level for standards (implementation agreements) and vetted contractor enforcement of security policies and practices is relaxed to a negotiated level.	The maturity level for standards (implementation agreements) and vetted contractor enforcement of security policies and practices is relaxed to a negotiated level.
Payment	Generally made after inspection and acceptance of the final product or service.	Payment made for reasonable, allowable, and allocable costs, typically on a monthly basis are incurred.	Payment made typically on a monthly basis based on the hourly rate multiplied by the hours worked, plus appropriate material costs.
Administrative burden	Generally low administrative burden on the client, requiring minimal oversight of the contractor	High administrative burden on the client, requiring heavy oversight of the contractor.	High administrative burden on the client, requiring heavy oversight of the contractor.

EPU's tend to push-back from cost reimbursable and time and material contract types. For this reason, we next compared fixed price contract types. Our observations are described in Table 2.

Table 2 Comparison of fixed-price contract types

Comparison criteria	**Firm** fixed **price**	**Fixed price performance price adjustment**	**Fixed price incentive firm**	**Fixed price award fee**
Principal risk to be mitigated	None. The contractor assumes all cost risk	Unstable or rapidly changing security threat environment	Moderately uncertain contract labor or material requirements to respond to the evolving security threat environment	Risk that the client (user) will not be fully satisfied because of judgmental criteria
Use when	• The security requirements are well defined • Contractors are experienced in meeting it • Security threats are stable • Financial risks are otherwise insignificant	The security threats at risk are severable and significant. The risk stems from industry-wide contingencies beyond the contractor's control. The cost at risk outweighs the administrative burden to manage the contract.	A ceiling price can be established that covers the most probable risks inherent in the nature of the security threat environment. The proposed profit sharing formula would motivate the contractor to control costs to and meet other objectives	Judgmental standards can be fairly applied by an award-fee panel The potential fee is large enough to both: • Provide a meaningful incentive • Justify related administrative burdens
Elements	A firm fixed price for each line item or one or more groupings of line items	A fixed price ceiling on upward adjustment, and a formula for adjusting the price up or down based on: • Established prices • Actual labor or material costs • Labor or material indices	• A ceiling price • Target cost • Target profit • Delivery, quality of security mitigation capabilities, and/or other security performance targets • Profit sharing formula	• A firm fixed price • Standards for evaluation performance • Procedures for calculating a fee based on performance against standards
Contractor is obliged to	Provide an acceptable deliverable at the time, place and price specified in the contract	Provide an acceptable deliverable at the time, place and price specified in the contract at an adjusted price	Provide an acceptable deliverable at the time, place and price specified in the contract at or below the ceiling price	Perform at the time, place and the price fixed in the contract
Contractor	Generally	Generally real-	Realizes a	Generally real-

Comparison criteria	Firm fixed price	Fixed price performance price adjustment	Fixed price incentive firm	Fixed price award fee
incentive (other than maximizing goodwill)	realizes an addition profit for reduced costs	izes an addition profit for reduced costs	higher profit by completing the work below the ceiling price and/or by meeting objective security performance targets	izes an additional profit for reduced costs; earns an additional fee for satisfying the security performance standard
Typical applications	Commercial supplies and services	Long-term contracts for commercial supplies during a period of dynamic threat activity	Production of a secure system based on a prototype	Security-performance based service contracts
Principal limitations	Generally not appropriate products and services that require significant research and development	Must be justified	Must be justified. Must be negotiated. Contractor must have an adequate accounting system related to security policies and procedures. Cost data must support security targets.	Must be negotiated
Variants	Firm fixed price level of effort		Successive targets	

4 Preliminary conclusion

This paper describes a work-in-progress. To date we have drawn some preliminary conclusions. In the future experiments need to be performed to refine the requirements, grading scheme, and procurement language.

- All five categories of procurement security requirements need to be articulated in EPU's procurement specifications.
- A simple grading scheme framework provides the EPU a starting point to tailor the grades for their procurement.
- The procurement security requirements and grading scheme needs to be codified as an energy sector "profile" which can be used by the EPUs to judge contractor's security maturity responding to EPU's solicitation.

- The most attractive contract type is a firm fixed price (FFP) with a fixed price incentive (or award) fee option. This contract strategy offers incentives for the contractor to maintain a high degree of security vigilance to identify threats and system vulnerabilities, and to provide patches and other updates in a timely manner. I does require the EPU to exercise an extensive prequalification of potential contractors to evaluate organizational capabilities and technical security capabilities.

Monitoring Advanced Metering Infrastructures with Amilyzer

Robin Berthier and William H. Sanders

Information Trust Institute and Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
{rgb,whs}@illinois.edu

Abstract. Advanced metering infrastructures (AMIs) enable two-way communications between smart meters and utility control centers. They are a key component of the smart grid initiative as they encompass a large number of devices and technologies and provide important applications that improve energy consumption and grid reliability. They could also attract diverse cyber-physical threats, and thus they require efficient monitoring solutions to ensure the detection of known and unknown abnormal activities. This paper presents Amilyzer, a specification-based intrusion detection system (IDS) that leverages tight control over authorized AMI protocol operations to provide a practical network situational awareness solution for AMI operators.

1 Introduction

The progressive replacement of traditional power meters with smart meters over the past few years was made possible through the deployment of important communication infrastructures by energy utilities. Those infrastructures, called *advanced metering infrastructures* (AMIs), consist of sets of wide-area networks (WANs) and neighborhood-area networks (NANs) that enable utilities to exchange information with meters in near real-time. That capability saves utilities from having to send human meter readers every month and allows new applications to improve grid reliability, energy savings, and consumer awareness. As an example of an AMI-enabled application, demand/response programs give consumers the ability to participate in load reduction during times of peak load, thanks to price signals sent by utilities. Those signals, received by meters, are used to automatically control home appliances that can accept delayed starts or slower running cycles, such as heating, ventilation, and air conditioning.

The communication capabilities of AMI also mean that utilities and parts of the distribution grid could be exposed to the risk of cyber intrusions. Motivations for malicious actions include access to large networks and an important number of low-computational devices, as well as access to consumption data and consumer information. Moreover, disruptions of grid operations through an AMI might have high visibility and high impact.

As a result, important efforts have been made by vendors, utilities, and regulators to ensure the resiliency of AMIs. In particular, strong encryption and authentication mechanisms are part of communication standards such as the ANSI

C12.22. While those protective measures are crucial to preventing attacks, they do not replace the need for efficient monitoring solutions. Indeed, the rapid evolution of attack techniques means that some protections might become obsolete, and successful intrusions should be promptly mitigated through an adequate combination of detection and response systems. The application of traditional information technology (IT) security solutions offers mixed results, and research and development efforts are still required to meet the needs of utilities [3].

This paper focuses on the detection aspect of the resiliency equation. Over the past two decades, various techniques for efficiently detecting intrusions in IT environments have been developed and evaluated. Through the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) research center[1], we studied how the unique characteristics of AMI compared to traditional IT networks could be leveraged in order to design highly efficient and practical intrusion detection systems (IDSes) [4,11]. In this paper, we present a sensor called *Amilyzer* that implements a specification-based approach to white-list the behavior of thousands of identical meters by observing and validating their network communications against protocol standards and a security policy.

The paper is organized as follows. Section 2 describes the scope of Amilyzer and the categories of threats that it monitors. Section 3 presents the internal architecture of Amilyzer and discusses deployment options. Section 4 describes our approach to define a sound security policy through the study of failure scenarios. Section 5 reports on lessons learned during the evaluation of Amilyzer in a testbed environment and in an AMI of more than 10,000 meters. Finally, Section 7 concludes the paper and discusses future work.

2 Threat Model and Failure Scenarios

Unlike a traditional IT network, AMI networks carry traffic for a limited set of applications using a single communication protocol, and smart meters are all designed to behave similarly. This tight control over devices and communications means that precise specification of expected traffic characteristics becomes a tractable problem; the control also opens up the possibility of implementing efficient white-listing technologies.

The scope of Amilyzer is to monitor network traffic and to focus on malicious behaviors that are visible in network activities. Thus, intrusions that reside entirely system-side, such as firmware compromise or penetrations into the collection engine application, are excluded from our scope. They could be detected by Amilyzer if they impact the network or if an attack vector is transferred through the network. Additionally, Amilyzer assumes complete visibility over payloads, which means that encrypted packets or packet captures that are incomplete because of sampling are currently not supported. We reviewed techniques to support encryption in [2], and improvement of Amilyzer so that it can be integrated into an IDS-friendly encrypted network environment is part of our future work.

[1] http://www.tcipg.org

To understand the types of malicious activities that Amilyzer should detect, we partnered with the Electric Power Research Institute (EPRI) and leveraged the work of the National Electric Sector Cybersecurity Organization Resource (NESCOR). NESCOR produced a report on possible failure scenarios for the different domains of the smart grid [18]. This report includes a threat model that consists of 4 categories of threat agents: criminals (economic, malicious, or recreational), activist groups, terrorists, and hazards. Insider threats such as disgruntled or careless employees are also included. This model helped us understand possible intents, threat characteristics, and risk prioritization. After studying failure scenarios for AMIs, we extracted 12 categories of failures that affect network activity. Those categories are presented in Table 1.

1	Adversary Issues Invalid Mass Remote Disconnect
2	Adversary Manipulates Meter Data Management System to Over/Under Charge
3	Mass Meter Rekeying Required when Common Key Compromised
4	One Compromised Meter in a Mesh Wireless Network Blocks Others
5	False Meter Alarms Overwhelm AMI and Mask Real Alarms
6	Unauthorized Pricing Information Impacts Utility Revenue
7	Spoofed Meter "Last Gasp" Messages Cause Fake Outage
8	Breach of Cellular Provider's Network Exposes AMI Access
9	Out of Sync Time-stamping Causes Discard of Legitimate Commands
10	Stolen Field Service Tools Expose AMI Infrastructure
11	Threat Agent Performs Unauthorized Firmware Alteration
12	Rogue Firmware Enables Unauthorized Mass Remote Disconnect

Table 1. Categories of network-related AMI failures extracted from the NESCOR report on failure scenarios

Each category in Table 1 groups one or several failure scenarios that we translated into security policy rules (detailed in Section 4). We then proceeded to extract the information needed for the successful detection of rule violations. First, Amilyzer has to access source and destination information, as well as identifiers for calling and called devices, from the network and application layers. That makes it possible to uniquely identify devices and to monitor security policy rules, such as "remote disconnects can only be issued from the collection engine." Second, Amilyzer has to understand the requests and responses issued by AMI devices so that security policy rules, such as "price updates should respect a given price window," can be supported. That means that headers and payloads from the application layer have to be captured and parsed. Finally, Amilyzer has

to be able to track the behavior of devices over time in order to monitor rules, such as "remote disconnects cannot be sent to more than N meters in less than M minutes." That means that the detection operations should be stateful.

3 Architecture

To achieve the objective of monitoring network activity and applying constraints from the specifications of valid behaviors, Amilyzer uses a modular architecture that is shown in Figure 1. The application was developed in Python and consists of about 2,300 lines of code. We describe the different modules in the next subsections.

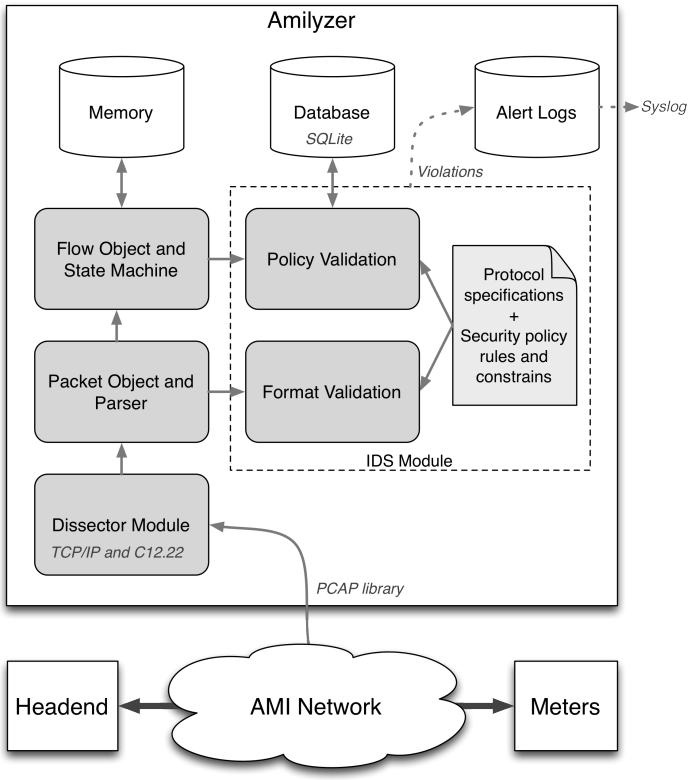


Fig. 1. Internal components and architecture of Amilyzer

3.1 Dissector

The application captures AMI traffic using the PCAP library and sends network packets to the dissector. The dissector includes parsers for TCP/IP, ANSI C12.22, and ANSI C12.19. A packet structure is instantianted for each new packet received, and information from the network, transport, and application layers are stored. At the application layer, the C12.22 header consists of an application security context element (ASCE) from which calling and called identifiers are extracted, an extended protocol specification for electric metering (EPSEM) header, and optional C12.19 data elements. The most important information extracted by the dissector is the information on EPSEM services that define the operations being requested. For instance, issuing of a remote disconnect involves sending of a *write* operation to update a specific register on the meter. An example of a dissected C12.22 packet representing a *full read* request and captured in the TCIPG testbed is provided below. The first line shows the timestamp, source IP address, and destination IP address. The next two lines show the raw bytes captured at the application layer. The first byte "60" indicates the beginning of a C12.22 frame. This frame has an ASCE header and an ESPEM section for which the different fields are detailed.

```
10:10.45.899059 10.9.0.1 > 10.9.2.6
app-layer:          60 15 a4 03 02 01 00 a8 03 02 01 00
        be 09 28 07 81 05 80 03 30 00 00
  --Decoding C12.22------- 21 bytes
  ACSE section:
       Called AP-invocation-identifier = 2.1.0
       Calling AP-invocation-identifier = 2.1.0
       User Information Element
       User Information External (length: 7)
       User Information Octet String (length: 5)
  EPSEM section: User Information Element (length: 5)
      EPSEM control: 128 10000000
       security: cleartext
       response_control: always respond
       --EPSEM request-response 1--
        Service length: 3
        Service: Full read
        Data: 00 00
```

3.2 State Machine

Once a packet structure has been created, Amilyzer tries to match it with an existing flow. Flows are defined as C12.22 sessions in which calling and called identifiers match and the flow is still active. Flows are expired after a couple of minutes of inactivity. If no flow is found, a new flow is created. Otherwise, the existing flow structure is updated. Each flow maintains a state machine for the caller and the called device. The state machine is built from the working state

of the device, which can be *in use*, *failed*, or *offline*, and the C12.22 protocol state, which can be *idle*, *sessionless processing*, *session idle*, or *session processing*. That state machine has been described and illustrated in [4]. A violation is reported to the intrusion detection module when an invalid transition is attempted. In addition, the sequence of EPSEM services requested and responded to is stored to allow the intrusion detection module to validate the flow against the specifications of known AMI operations.

3.3 Intrusion Detection System

Once a flow structure has been created or updated, the intrusion detection module analyzes the source and destination of the flow as well as the ordered sequence of requests and responses. Three types of checking operations are conducted. First, if a protocol violation has been recorded by the parser or by the state machine, an alert is logged. Second, the tuple {source, destination, sequence} is matched against a database of known valid flows. If the tuple has never been seen before, an alert is also, logged and an operator will have to approve the newly discovered flow or escalate the alert to create an incident. An approach to initial population of the database consists of running Amilyzer for a few days in *learning mode* before switching the system to *checking mode*. Third, the tuple is checked against a set of constraints. Those constraints are defined according to the security policy rules that are described in the next section. Five fields can be defined for each constraint: 1) a sequence pattern, which can be defined using a regular expression over the sequence of EPSEM services sent and received; 2) a source address or calling identifier; 3) a destination address or called identifier; 4) a condition, which can be expressed through functions such as *maximum rate per hour* or *scheduled time of validity*; and 5) an action, which might trigger a low-, medium-, or high-level alert. An example of a constraint is provided below for the security policy rule "*Allow only scheduled remote disconnect commands during authorized time windows.*"

```
– Pattern:      remote_disconnect
– Source:       any
– Destination:  any
– Condition:    NOT(9am–5pm)
– Action:       alert_high
```

An important feature of the intrusion detection module that improves the practicality of Amilyzer is the lookup mechanism. It enables operators to label caller ID, called ID, or C12.22 sequences of requests and responses with human-readable names. As shown in the example constraint above, the keyword *remote_disconnect* in the pattern field actually represents the sequence {*Logon; Full read; Partial write table 7; Logoff*}.

4 Security Policy

As mentioned in Section 2, we used the report on failure scenarios produced by NESCOR [18] to define a security policy for AMIs. A first step in writing the policy was to produce a human-readable set of rules that were extracted from the different scenarios that relate to network activity. The scope of those rules is to define what activities are allowed and prohibited in an AMI, and under which conditions. Conditions include timing, user roles, and system state requirements. A second step has been to translate the security policy rules into constraints that can be understood by Amilyzer.

A total of 23 rules were identified. For each rule, 6 fields were defined: 1) action to perform when a violation occurs; 2) best practice to prevent violations of the rule; 3) follow-up response actions after a violation occurred and an alert has been issued; 4) optimal sensor location to monitor the information required by the rule; 5) optimal location to issue response actions; and 6) information required for a successful detection. The 23 rules and 4 of the 6 fields are detailed in Table 2.

The optimal location to monitor the security policy rules depends on the information required. For instance, threats local to a neigborhood area network would not be visible at the headend. The Amilyzer sensor has been designed to be lightweight and to support flexible deployment schemes. Sensors can be deployed either centrally at the headend, or distributed in the field within access points, meters, or dedicated monitoring field devices. The central approach offers the advantages of low deployment cost, reliable alerting, and simple configuration. However, the central location lacks visibility over the edge of the network and can suffer from scalability issues in the case of a large AMI with hundreds of thousands of meters. In [6], we introduced a framework to assist utilities in selecting the right deployment strategy based on the characteristics of their AMIs.

5 Evaluation

The evaluation of Amilyzer was first conducted in a testbed environment. The TCIPG research center has a metering lab [21] that we used to capture normal meter operations and to test detection capabilities by injecting malicious traffic. The testbed consists of 20 meters deployed on 3 floors of a building. Each floor represents a NAN and has a wireless access point. The 3 access points are communicating using C12.22 over TCP/IP to a collection engine. An Amilyzer sensor was deployed on a switched port analyzer (SPAN) of a switch that connects the collection engine to the access points. The collection engine was configured to periodically send meter reading queries to meters. We then proceeded to inject the following attacks: 1) a remote disconnect from the collection engine towards a single meter at an unauthorized time; 2) a set of remote disconnects from the collection engine towards 10 meters at once; 3) a remote disconnect from a rogue IP address towards a single meter; 4) a burst of read requests from a rogue IP

Policy Rule	Prevention	Location	Information Required	Alert
Allow remote disconnect only from authorized headend	authentication; access control	headend	network access (app layer); Authorized headend	high
Allow remote disconnect to be issued only by employees with sensitive function credentials	least privileges	headend	network traffic (app layer); Employee ID	high
Remote disconnect commands affecting more than N1 meters require 2-person authentication	prevent command from reaching meter	headend	network traffic (app layer); N1 threshold	high
No remote disconnect command affecting more than N2 meters in less than M1 minutes should be authorized	prevent command from reaching meter	headend	network traffic (app layer); N2, M1 thresholds	high
Remote disconnect commands affecting more than N3 meters in less than M2 minutes require 2-person authentication	prevent command from reaching meter	headend	network traffic (app layer); N3, M2 thresholds	high
Allow scheduled remote disconnect commands only during authorized time windows	defining tight time windows	headend	network traffic (app layer); authorized time period	high
Pricing information must be flowing from the head end to meters	traffic control	headend; field	network traffic (app layer)	moderate
Only authorized system components can access the metering servers	device authentication; network access control lists	headend; field	network traffic (app layer) authorized devices ID	moderate
Cryptographic keys must never be transmitted in clear on the network	use cryptographic module	headend; field	network traffic; cryptographic key format	moderate
Allow software/firmware upgrades only from authorized headend systems or authorized field devices	authorization and privileges	headend; field	headend and device ID	moderate
Meters should respond to communication requests in less than S seconds	network health	headend; field	meter response time	low
Allow authorized operations to be sent to and received only from meters	white-listed network	headend; field	network traffic (app layer); list of authorized operations	moderate
Allow meter alarms to be issued only by registered meters	authentication, message authenticity, non-repudiation	headend; field	network traffic (app layer); list of authorized operations	moderate
Time-of-use price updates should fit between minimum and maximum acceptable values	authentication; data integrity	headend; field	network traffic (net + app layer); minimum and max pricing values	moderate
Time-of-use price updates should be executed by 2 persons	authentication	headend	authentication logs network traffic (app layer)	moderate
Meters in last-gasp state should have limited functionalities	up to date database of registered meter statuses	headend; field	network traffic (app layer); limited functionality definition	low
Traffic should be encrypted on leased networks	communication confidentiality	leased networks	network traffic (app layer); perimeter definition for leased networks	moderate
Traffic on leased networks must be isolated per utility	communication confidentiality; network configuration	leased networks	network traffic (app layer); perimeter definition for leased networks	moderate
Allow time synchronization updates to be issued only by authorized time servers	authentication of time servers	headend; field	network traffic (app layer); list of authorized time servers	low
Allow only correctly time synchronized communication messages	time synchronization process; communication integrity	headend; field	network traffic (app layer); correctly time synchronized: maximum of X milliseconds	low
Allow access to AMI only from authorized and authenticated field service equipment	authentication and authorization	headend; field	network traffic (net + app layer); list of authorized devices	low
Allow authorized operations only from field service equipment	authentication; authorization; privileges	headend; field	network traffic (net + app layer); list of authorized devices	moderate
Allow firmware upgrade only from valid firmware signature	authorization; privileges	headend; field	network traffic (net + app layer); firmware signature	high

Table 2. Security policy rules defined based on failure scenarios

address towards a single meter. Amilyzer was configured to accept remote disconnects only if they occur during an authorized time window, towards less than 2 meters per hour, and if they were issued from the collection engine. We verified that alerts were correctly triggered for each of the attack injected.

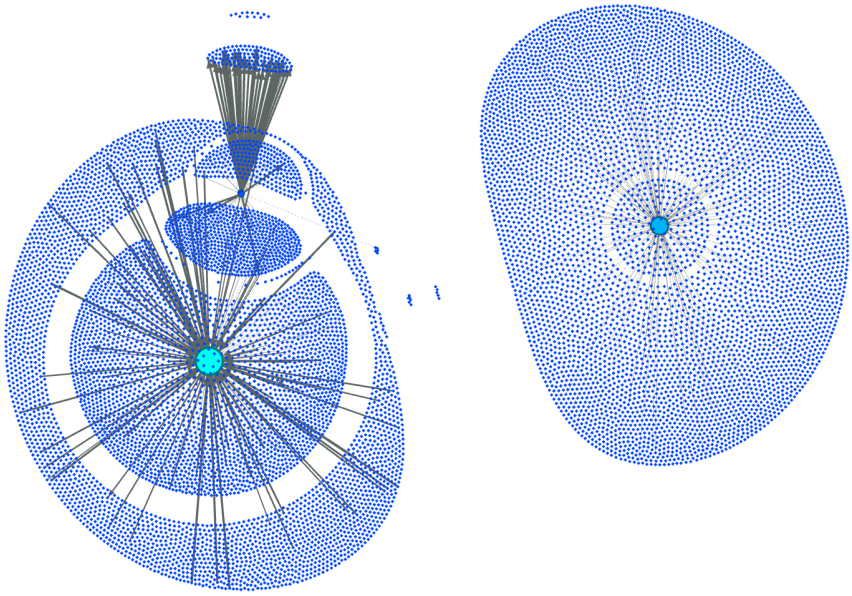
Once Amilyzer successfully passed accuracy and performance tests in the lab, we partnered with a large utility in the United States to deploy a sensor at the headend of a real AMI. The number of meters in this AMI grew from 6,000 at the beginning of the deployment in December 2012, up to 32,000 meters in October 2013. This large-scale deployment enabled us to identify and fix performance bottlenecks, as well as to tune the security policy and better understand the situational awareness needs of AMI operators. A total of 10 versions of the application were deployed over the past 10 months to take into account crash reports and data logged. Three types of instabilities were reported: 1) frequent crashes of the C12.22 dissector module; 2) large number of packets that could not be parsed; and 3) intrusion detection module too slow to keep up with the rate at which packets were captured. We solved the first issue by improving exception handling in the dissector. The second issue was due to many packets being segmented at the application layer. We completed the implementation of the dissector to handle reassembly of C12.22 segments. Finally, we replaced the file-based input/output system used by the intrusion detection module with an SQLite database. The database significantly improved the speed at which search and save queries could be handled. As an example, for one week of traffic collected in October 2013, the average traffic rate measured has been 593 packets per minute (ppm), with a minimum of 17 ppm and a maximum of 2942 ppm. At the end of those 7 days, Amilyzer was maintaining a database of 29 MB that consisted of half a million flow processed, 144,175 unique flows identified, and 234 unique sequences of C12.22 operations. During that week, C12.22 operations recorded included 9,084 meter registration requests, 988,607 identification requests, and 2,791 write requests.

Figure 2 is a screenshot of a visualization application that represents the network topology from the logs produced by Amilyzer. It also allows us to filter the traffic monitored by type of requests and responses. Each dot in Figure 2 represents a smart meter and arrows represent directed traffic captured between the meters and one of the 3 collection engines (larger circles at the center of the clusters). In this screenshot, only response errors are shown, indicating areas of the AMI in which errors occur more frequently. (The thickness of arrows indicates traffic volume.) That representation is used by operators to identify misconfigurations and security issues.

6 Related Work

IDSes for critical infrastructures have been the focus of an increasing number of studies over the past few years. A first category of work has looked at supervisory control and data acquisition (SCADA) protocols. [7] leverages the regular traffic patterns of SCADA networks to develop a model-based IDS. The approach mon-

Fig. 2. Visualization of response errors sent by meters to a collection engine for an AMI of 12,000 meters. Meters are clustered around 3 collection engines and edges represent network flows for a specific C12.22 operation.



itors Modbus protocol fields to update models of the protocol. Rules to detect violations of the critical characteristics of those models have been implemented in Snort. MHINDS [12] extended that approach by specifying additional temporal and spatial model characteristics using a Petri net implementation. The authors of [10] also introduced a state-based network intrusion detection system. They focused on the detection of complex multi-step attacks targeting systems that use the DNP3 or the Modbus protocols. At the core of this approach is a rule language that allows operators to describe critical device states for which alerts should be triggered. [14] implemented a complete parser for DNP3 in the open source Bro IDS, along with a set of rules to detect violations of the protocol semantic. Those rules enable the detection of both errors within a given DNP3 packet, and of state-based issues across a sequence of DNP3 operations. [20] proposed a model-based sensor working on top of the WirelessHART protocol to monitor and protect wireless process control systems. The architecture consists of a central component that collects information periodically from a set of sensors distributed in the field. On the side of host-based IDSes, [16] presents a probability model based on stochastic Petri nets to specify the behavior of a cyber physical system (CPS). A contribution of that work is a framework that can be dynamically adjusted to tune detection parameters of IDS sensors in order to better monitor and respond to attackers. [8] looked at the specific issue of supply-chain threats that target critical-infrastructure embedded systems. The

hardware-based IDS monitors the analog signal response of a resistor-capacitor circuit to identify the presence of hardware Trojans.

A second category of work has investigated the specific domain of AMIs. Detection of and protection against firmware compromises has been studied in [13], where an architecture called the *cumulative attestation kernel* enables utilities to remotely audit firmware updates in smart meters. Another host-based IDS is described in [9], which proposed to instrument meters, data concentrators, and the headend with sensors that can apply data-mining techniques on the continuous stream of data exchanged. Finally, [19] studied how to instrument a trusted meter device with an anomaly-based IDS. Closer to our approach, a few network-based IDSes for AMI have been recently introduced. [15] presented BRIDS, a behavior-rule based IDS that can translate rules about the expected behavior of AMI components into state machines. States are defined according to the combined values of predicates expressed in normal form. [17,1] described an anomaly-based IDS for NAN that uses a combination of central and distributed sensors to support monitoring of encrypted traffic.

Our present work builds upon [5], which explained the motivation for using specification-based IDSes in the context of an AMI, and [4], which leveraged a modeling technique and a theorem-proving framework to formally verify that a detection operation correctly implements the security policy. Our contributions in this paper are the following. First, the complete design of Amilyzer is presented and grounded in a review of realistic AMI failure scenarios. Second, a comprehensive security policy for AMI is introduced. Third, lessons learned after evaluating Amilyzer in a large AMI for 9 months are presented.

7 Conclusions and Next Steps

Amilyzer is a specification-based intrusion detection sensor designed to monitor AMI communications. This paper presented the threat model covered by Amilyzer, as well as the modular architecture of the sensor. A unique aspect of this project is that it leverages an industry-established set of realistic failure scenarios to define a comprehensive security policy. The policy, which consists of 23 rules, was described and translated into machine-checkable constraints. Several months of deployment of Amilyzer at the headend of a large AMI enabled us to improve the scalability and reliability of the IDS. Amilyzer has reached a development phase at which it is starting to address the pressing need for an efficient and practical monitoring solution for AMIs.

Amilyzer is still a prototype, and there are still important research challenges to investigate as part of future work. First, Amilyzer does not support encrypted traffic. We are looking into IDS-friendly key-sharing mechanisms to increase the visibility of the sensor over meter communications in the field. Second, Amilyzer currently works as an individual sensor, but we believe that the efficiency of the intrusion detection approach could gain from being distributed and coordinated across multiple sensors. Finally, we are looking at how to improve the resiliency of the monitoring infrastructure against attacks that target IDS sensors.

Acknowledgments

This material is based upon work supported in part by the Department of Energy under Award Number DE-OE0000097 and by the Electric Power Research Institute. The opinions expressed are those of the authors alone. The authors would like to thank Annabelle Lee for her input and insightful feedback on the security policy and Jenny Applequist for her editorial assistance.

References

1. Nasim Beigi Mohammadi, Jelena Mišić, Vojislav B Mišić, and Hamzeh Khazaei. A framework for intrusion detection system in advanced metering infrastructure. *Security and Communication Networks*, 2012.
2. Robin Berthier, Jorjeta G Jetcheva, Daisuke Mashima, Jun Ho Huh, David Grochocki, Rakesh B Bobba, Alvaro A Cárdenas, and William H Sanders. Reconciling security protection and monitoring requirements in advanced metering infrastructures. In *Smart Grid Communications (SmartGridComm), Conference on*. IEEE, 2013. To appear.
3. Robin Berthier and Galen Rasche. Intrusion detection system for advanced metering infrastructure. Technical report, EPRI, 2012. http://www.energycollection.us/Energy-Metering/Intrustion-Detection-System.pdf.
4. Robin Berthier and William H Sanders. Specification-based intrusion detection for advanced metering infrastructures. In *Dependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on*, pages 184–193. IEEE, 2011.
5. Robin Berthier, William H Sanders, and Himanshu Khurana. Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 350–355. IEEE, 2010.
6. Alvaro A Cárdenas, Robin Berthier, Rakesh B Bobba, Jun Ho Huh, Jorjeta G Jetcheva, David Grochocki, and William H Sanders. A framework for evaluating intrusion detection architectures in advanced metering infrastructures. *Smart Grid, IEEE Transactions on*, 2013. To appear.
7. Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner, and Alfonso Valdes. Using model-based intrusion detection for SCADA networks. In *Proceedings of the SCADA Security Scientific Symposium*, pages 1–12, 2007.
8. Nathan J. Edwards. Hardware intrusion detection for supply-chain threats to critical infrastructure embedded systems. Master's thesis, University of Illinois at Urbana-Champaign, 2012.
9. Mustafa Amir Faisal, Zeyar Aung, John R Williams, and Abel Sanchez. Securing advanced metering infrastructure using intrusion detection system with data stream mining. In *Intelligence and Security Informatics*, pages 96–111. Springer, 2012.
10. Igor Nai Fovino, Andrea Carcano, T De Lacheze Murel, Alberto Trombetta, and Marcelo Masera. Modbus/DNP3 state-based intrusion detection system. In *Advanced Information Networking and Applications (AINA), International Conference on*, pages 729–736. IEEE, 2010.
11. David Grochocki, Jun Ho Huh, Robin Berthier, Rakesh Bobba, William H Sanders, Alvaro A Cárdenas, and Jorjeta G Jetcheva. AMI threats, intrusion detection

requirements and deployment recommendations. In *Smart Grid Communications (SmartGridComm), International Conference on*, pages 395–400. IEEE, 2012.
12. Adam Hahn. *Cyber security of the smart grid: Attack exposure analysis, detection algorithms, and testbed evaluation.* PhD thesis, 2013.
13. Michael LeMay and Carl A Gunter. Cumulative attestation kernels for embedded systems. *Smart Grid, IEEE Transactions on*, 3(2):744–760, 2012.
14. Hui Lin, Adam Slagell, Catello Di Martino, Zbigniew Kalbarczyk, and Ravishankar K Iyer. Adapting Bro into SCADA: building a specification-based intrusion detection system for the DNP3 protocol. In *Annual Cyber Security and Information Intelligence Research Workshop*, page 5. ACM, 2013.
15. Robert Mitchell and Ing-Ray Chen. Behavior-rule based intrusion detection systems for safety critical smart grid applications. 4(3):1254–1263, September 2013.
16. Robert R Mitchell III. *Design and Analysis of Intrusion Detection Protocols in Cyber Physical Systems.* PhD thesis, Virginia Polytechnic Institute and State University, 2013.
17. Nasim Beigi Mohammadi. An intrusion detection system for smart grid neighborhood area network. *Journal on Information Technology and Applications*, 2(1):7–13, 2012.
18. National Electric Sector Cybersecurity Organization Resource (NESCOR). Electric sector failure scenarios and impact analyses. Technical report, EPRI, 2012. http://www.smartgrid.epri.com/doc/NESCOR_10_25_12.pdf.
19. Massimiliano Raciti and Simin Nadjm-Tehrani. Embedded cyber-physical anomaly detection in smart meters. In *Critical Information Infrastructure Security (CRITIS12), International Conference on*, 2012. To appear.
20. Tanya Roosta, Dennis K Nilsson, Ulf Lindqvist, and Alfonso Valdes. An intrusion detection system for wireless process control systems. In *Mobile Ad Hoc and Sensor Systems, International Conference on*, pages 866–872. IEEE, 2008.
21. Tim Yardley, Robin Berthier, David Nicol, and William H Sanders. Smart grid protocol testing through cyber-physical testbeds. In *Innovative Smart Grid Technologies (ISGT)*, pages 1–6. IEEE, 2013.