Ministère de la Transition écologique et solidaire



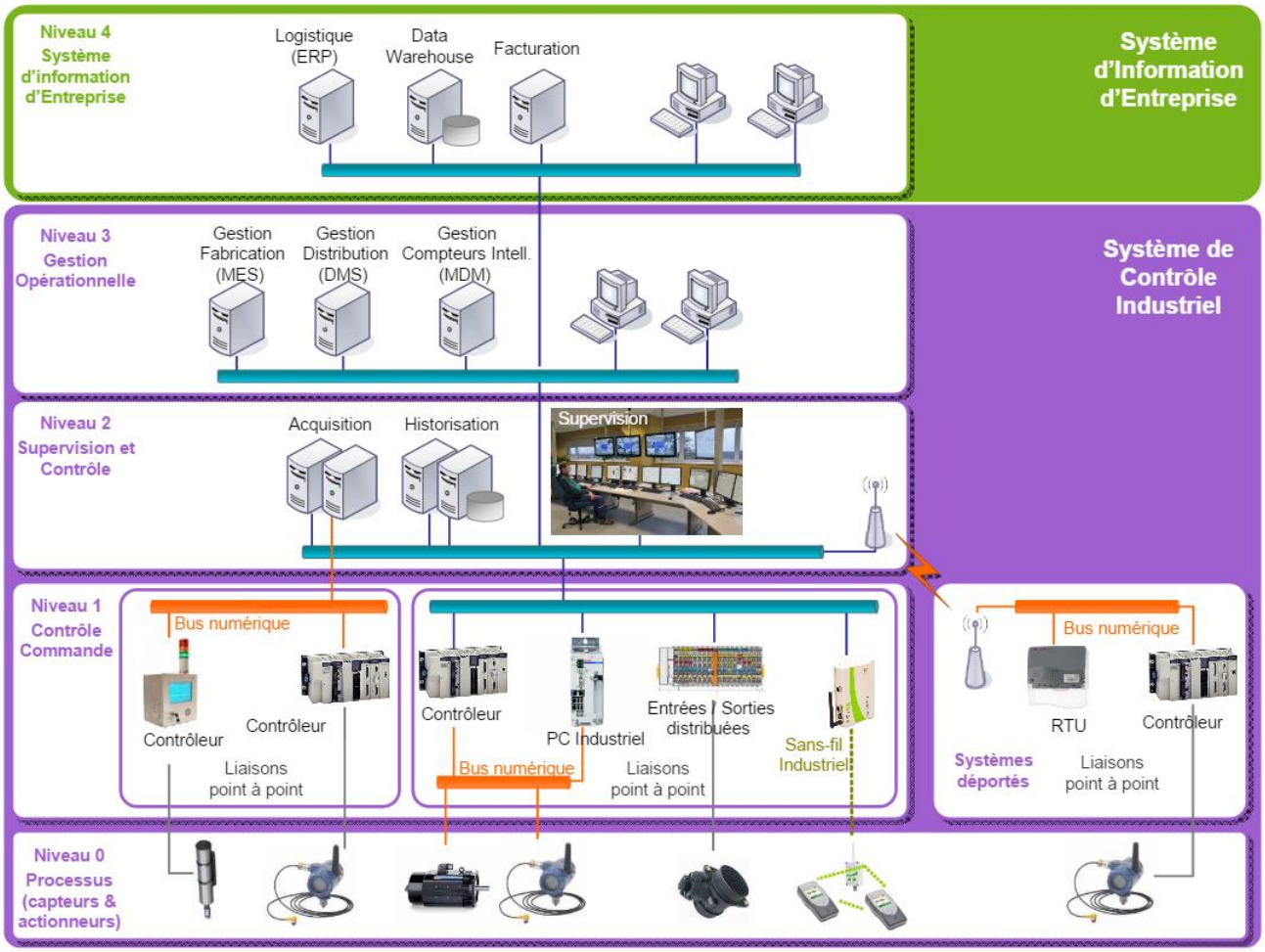
Cybersécurité dans l'industrie

ARIA
dgpr srt barpi

____Sommaire____

INTRODUCTION

Un système informatique pilotant une unité industrielle peut se décomposer schématiquement de la façon suivante :



Ce système présente la particularité d'être isolé dans le meilleur des cas par un pare feu des systèmes informatiques classiques de l'entreprise (bureautique, vidéosurveillance…). Comme indiqué, Il est généralement composé de plusieurs sous dispositifs servant à:

- **piloter les équipements industriels**, par exemple l'ouverture des vannes d'alimentation d'un réacteur chimique. Des « automates programmables industriels » (API) ou en anglais programmable logic controler (PLC), ainsi que des terminaux de contrôle (RTU) assurent cette fonctionnalité ;
- **centraliser les données puis piloter le processus industriel en salle de contrôle avec un système SCADA** (système d'acquisition et de contrôle des données) reposant généralement sur une interface homme machine et des serveurs informatiques ;
- **transmettre les informations via des ondes électromagnétiques** (signal Wifi, GSM, centrale d'alarme) ou **des réseaux câblés** suivant un protocole précis (ethernet, profibus/profinet entre plusieurs centrales automates, ASi).

Un dysfonctionnement de ces systèmes informatiques (SI) peut être à l'origine d'événements accidentels. A titre d'exemple, la défaillance et l'indisponibilité d'un système SCADA pilotant un pipeline sont en partie responsables de l'accident de Belligham aux Etats-Unis en 1999 (ARIA n°15621). Plus récemment, lors de l'accident de la plateforme pétrolière Deepwater horizon en 2010 (ARIA 38145), des articles de la presse américaine font état sur la base de témoignages d'employés, de nombreux écrans bleus (blue screen of death) signifiant des problèmes informatiques avant l'accident (http://www.examiner.com/article/did-bsods-on-the-deepwater-horizon-contribute-to-the-gulf-oil-disaster).

Par ailleurs, dans un contexte soutenu de menaces terroristes, de nombreux logiciels malveillants (malware) ont vu dernièrement le jour rendant les SI davantage vulnérables. C'est ainsi qu'une coupure d'électricité affectant près de 1,4 millions d'abonnés ukrainiens le 23 décembre 2015 serait liée à une attaque informatique.

Pour suivre la structure d'un système de contrôle industriel (SCI ou ICS : industrial control system en anglais), les événements étudiés dans la présente note sont répartis suivant qu'ils impliquent des :

- automates ;
- capteurs ;
- centres de traitement (SCADA) ;
- protocoles de transmission de l'information.

Par ailleurs, les systèmes de climatisation des salles de contrôle peuvent introduire des dysfonctionnements ou des indisponibilités des SI. Un point spécifique leur est ainsi consacré.

Le présent document s'attache à étudier les événements recensés dans ARIA à travers le prisme de la cybersécurité. Ainsi, les accidents n'impliquent pas nécessairement un acte de malveillance d'une personne externe ou interne à l'entreprise. Ils résultent pour certain d'erreur humaine ou organisationnelle dont les leçons peuvent utilement être transposées au cas de la malveillance informatique. En effet, la frontière entre un acte malveillant et une erreur humaine se caractérise par la volonté de nuire à une institution, soit pour des raisons idéologiques, financières ou affectives.

Les automates programmables (PLC (US)/ API (FR))

Exemples de matériels :

Siemens

Allen Bradley

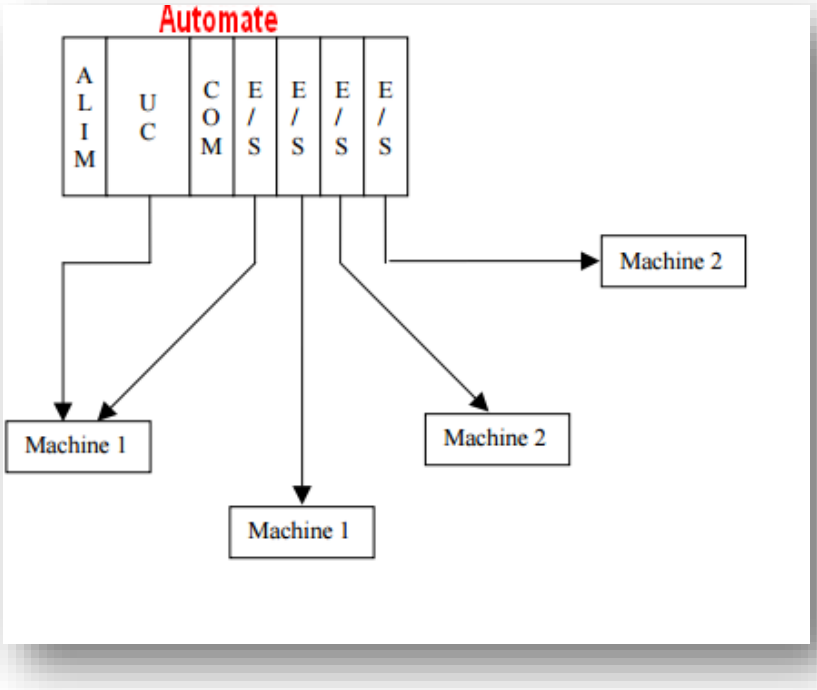
Principe de fonctionnement :

Un automate programmable industriel est un composant électronique qui assure 2 fonctions, l'une dénommée partie opérative (PO) qui actionne les moteurs électriques, vérins pneumatiques et/ou hydrauliques de l'unité, l'autre appelée partie commande (PC) qui coordonne ces différentes actions. Ces composants sont programmés par des automaticiens à l'aide de logiciels spécifiques (langage de programmation répondant à la norme CEI 61131-3) ou de console de programmation propriétaire. Les automaticiens se connectent avec leur ordinateur sur une prise dédiée comme indiqué sur le schéma ci-dessous :

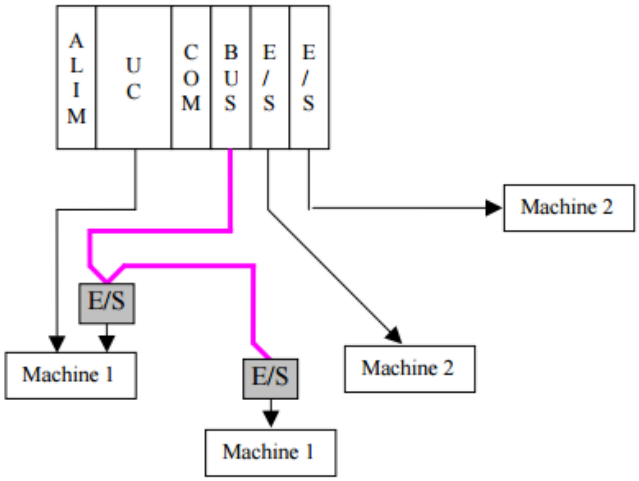
Ces automates sont constitués de cartes d'entrée/sortie au nombre de 4, 8, 16 ou 32 qui assurent la transformation et l'adaptation des signaux électriques venant des capteurs ou des boutons-poussoirs (entrées) vers l'automate, et dans l'autre sens, des signaux allant de l'automate vers les contacteurs, voyants, électrovannes, etc.

Types de montages possibles :

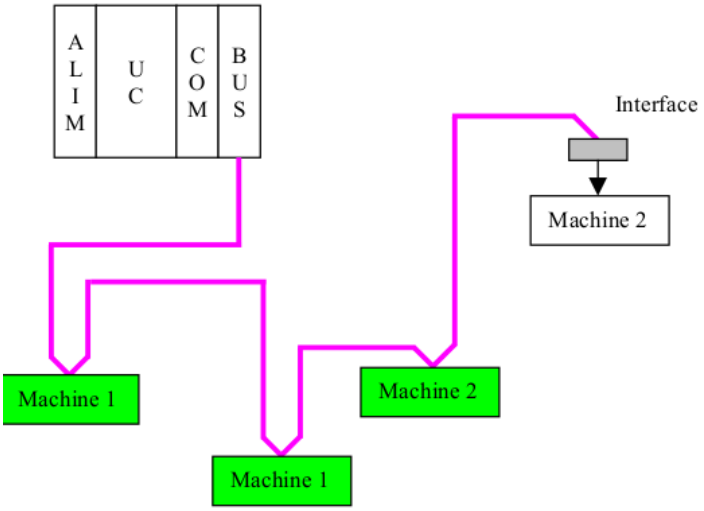
Chaque carte entrée/sortie est reliée à une machine, ce montage nécessite une grande longueur de câble :



Les évolutions de la technologie ont conduit à des montages conduisant petit à petit à l'installation des cartes d'entrée/sortie au plus près des capteurs/machines, puis au multiplexage des équipements comme l'indiquent les schémas ci-après à travers des bus de communication :



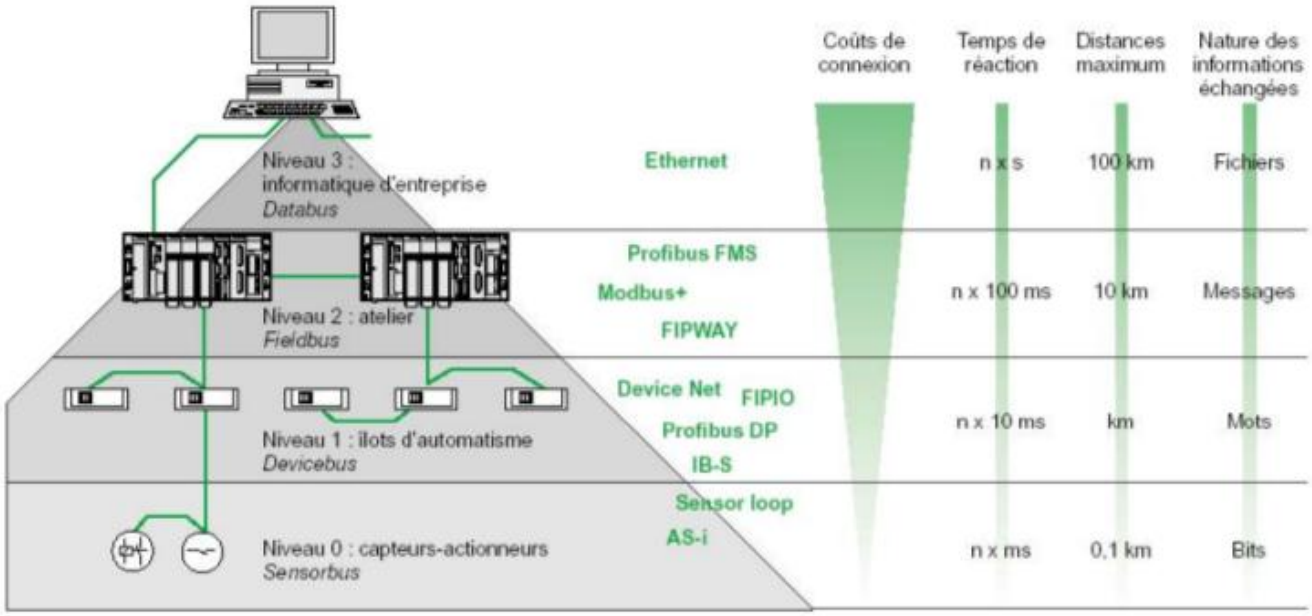
Carte d'entrée sortie au plus prés des machines



Multiplexage des machines

Le bus ASi (Actuators Sensors interface) permet de raccorder 31 esclaves (capteurs ou préactionneurs) sur un câble spécifique (deux fils) transportant les données et la puissance.
Ce bus est totalement standardisé et permet d'utiliser des technologies de plusieurs constructeurs (interopérabilité). L'automate est pour cela doté d'un coupleur ASi.

La nécessité de communication entre cellules (communication entre automates) a permis de voir apparaître de nombreuses normes de communication (Profibus, Fip ...).



La tendance actuelle est à l'introduction des réseaux Ethernet au plus près des automatismes (exemple : norme Profinet).

Sécurité :

L'automate doit résister à des :

- Contraintes extérieures du monde industriel et fait l'objet de nombreux tests normalisés (tenue aux vibrations, compatibilité électromagnétique, température…) ;
- Coupures d'alimentation : l'automate est conçu pour supporter les coupures d'alimentation et permet d'assurer un fonctionnement correct lors de la réalimentation (reprises à froid ou à chaud) ;

- Mode marche/arrêt : seule une personne habilitée peut mettre en marche ou arrêter un automate. La remise en marche se fait par une procédure d'initialisation (programmée).

Il existe enfin des automates dits de sécurité (APIdS) qui intègrent des fonctions de surveillance et de redondance accrues.

L'ANSSI qualifie par ailleurs du matériel au titre de la sécurité informatique. La liste des équipements certifiés est disponible à l'adresse suivante :

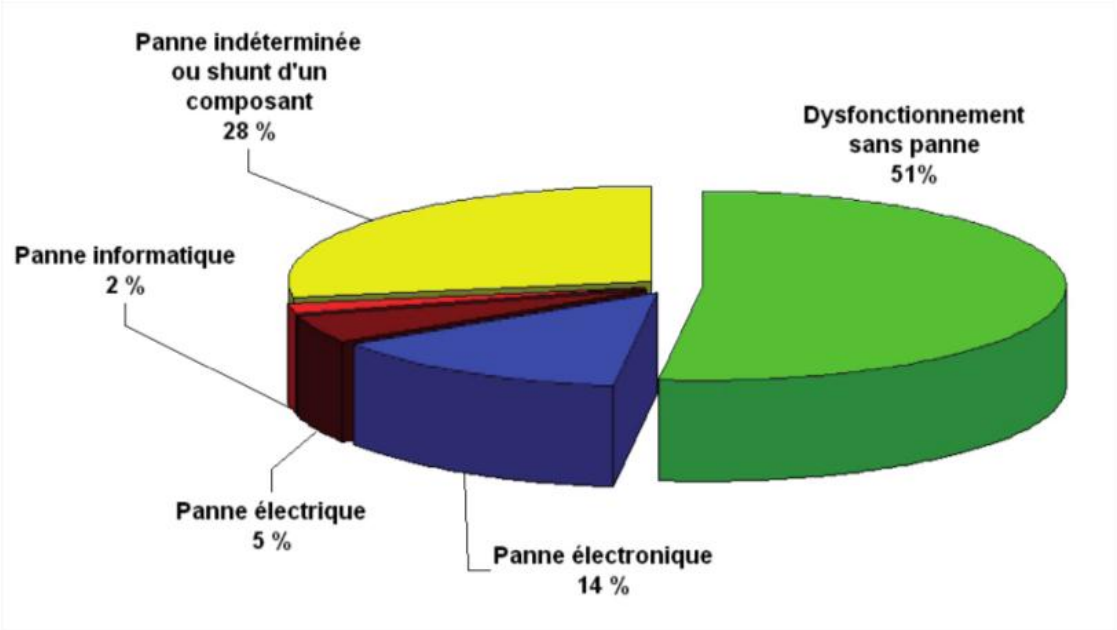
http://www.ssi.gouv.fr/administration/qualifications/produits-recommandes-par-lanssi/les-produits/ rubrique équipement industriel pour les automates.

Les accidents recensés dans ARIA :

L'accidentologie des automatismes industriels et notamment leur partie traitement a fait l'objet d'une étude par le BARPI en 2014. L'étude est téléchargeable sur internet à partir l'adresse suivante : https://www.aria.developpement-durable.gouv.fr/synthese/syntheses/accidentologie-des-automatismes-industriels-la-fonction-traitement/.

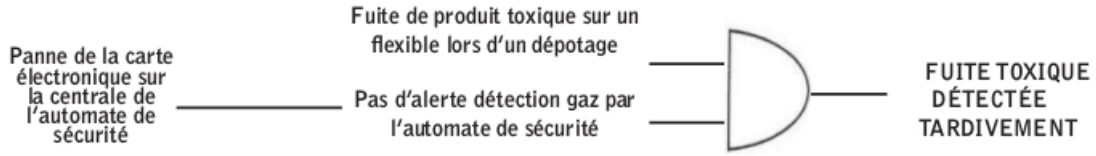
Parmi les éléments d'analyse qui ressortent :

- L'examen de 275 accidents impliquant des défaillances de composants de la fonction traitement fait apparaître l'implication de la partie matérielle (calculateur, carte électronique) dans 49 % des accidents ;
- Les composants liés à la transmission d'information au sein de l'automate (bus de données, relais) sont impliqués dans 14 % des cas ;
- Les défaillances matérielles représentent la première cause directe des défaillances de la fonction traitement (102 cas), elles se répartissent de la façon suivante :



Exemples d'accidents :

PANNE DE CARTE ÉLECTRONIQUE (ARIA 42931) 02/05/2012



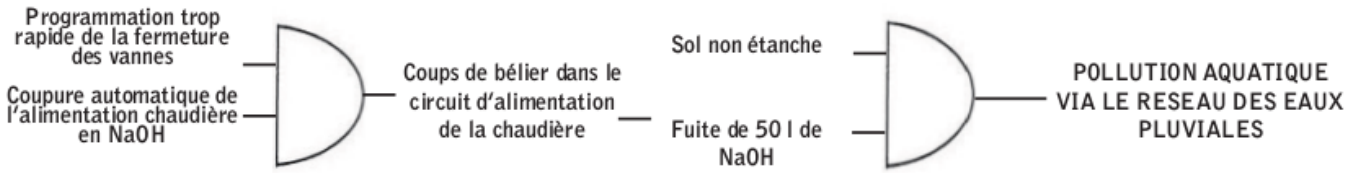
Lors d'une livraison de méthoxyméthane (DME) dans une usine de produits cosmétiques, un flexible de transfert gonfle au niveau du raccord vers l'installation fixe et fuit en raison d'une incompatibilité entre le matériau du flexible et le produit livré. L'opératrice constate la fuite et alerte le chauffeur qui ferme la vanne de fond de cuve et coupe le moteur du camion. Le bouton d'arrêt d'urgence est actionné pour déclencher la mise en sécurité du poste de dépotage et l'évacuation de l'usine par précaution durant 20 min. **L'accident met en évidence une détection gaz qui s'est révélée inopérante à cause d'un défaut matériel des cartes électroniques de la centrale de traitement (cartes datant de 2001)**. Les capteurs, rapidement saturés, sont passés en signal « hors échelle » ; signal qui a été traité comme « défaut de capteur » sans action particulière (alors que le « hors échelle » doit normalement déclencher les procédures de sécurité).
Le fabricant de la carte aurait identifié le risque potentiel de dysfonctionnement depuis 2008 et remédié à la situation (par changement des cartes et mise à jour du logiciel). Toutefois, l'ensemble des cartes concernées n'avaient pas été rappelées ou mises à jour. L'exploitant de l'usine chimique remplace l'ensemble de ses cartes.

VOIR AUSSI Aria 3536, 7172, 10064, 21466, 27060, 32624, 39321, 43437

L'analyse des causes profondes des événements rappelle également toute l'importance du soin à apporter à **la programmation des automates**. L'accidentologie comporte en effet, de nombreux cas de **programmation incomplète, inadaptée, voire accidentogène** de ces derniers (Cf ARIA 36437, 21994, 28911...).

Exemples d'accidents :

PROGRAMMATION ACCIDENTOGÈNE (ARIA 28911) 21/09/2004



Une fuite de 50 l de soude (NaOH) se produit sur l'alimentation de l'unité de déminéralisation d'une chaudière dans une usine de fabrication de colles. Le sol détérioré sous les colonnes de déminéralisation facilite l'écoulement des eaux de lavage chargées de soude dans un ancien réseau pluvial se rejetant dans la SORGUE. L'élévation du pH provoque la précipitation du carbonate de calcium, entraînant un important trouble blanchâtre de la rivière. Ce dernier disparaît 1 h plus tard. **L'entreprise prévoit** la réfection et l'étanchéification du sol de l'unité, la réparation de la tuyauterie, **la modification du programme de l'automate pour éviter les coups de bélier lors de la fermeture des vannes et une réduction de la temporisation de discordance.**

VOIR AUSSI Aria 5989, 16072, 28911, 30417, 32109, 31691, 40522, 41736, 42038, 42921

Attaques informatiques d'automates

La base ARIA ne comporte pas d'accidents impliquant une attaque informatique au sens classique (voir annexe) d'automates de contrôle.
Toutefois, des vidéos circulent sur internet montrant que les automates sont sensibles aux attaques par déni de service (https://www.youtube.com/watch?v=Uu0bB3ptUvo) lorsqu'ils ne sont pas protégés derrière un pare feu. Ces attaques semblent provoquer un code erreur et l'arrêt du système.

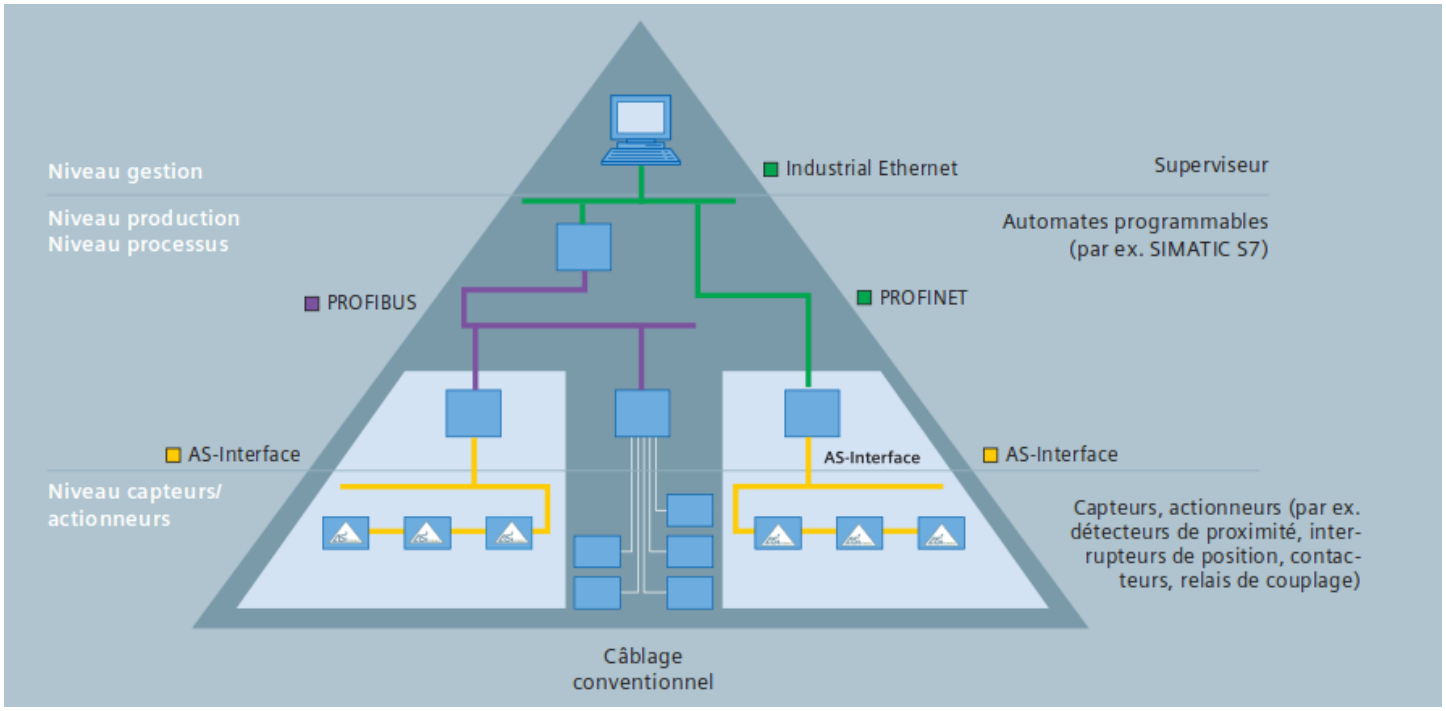
Les capteurs

Principe de fonctionnement :

Le rôle principal du capteur est de transformer la grandeur analogique à mesurer en un signal compréhensible par le système de commande.

Branchement sur le Système de Contrôle Industriel :

Comme évoqué plus haut, les capteurs étaient avant connectés directement en parallèle sur un bus. La tendance actuelle est plutôt au multiplexage avec la norme AS-i comme l'indique l'extrait d'une documentation du constructeur Siemens :



Les accidents recensés dans ARIA :

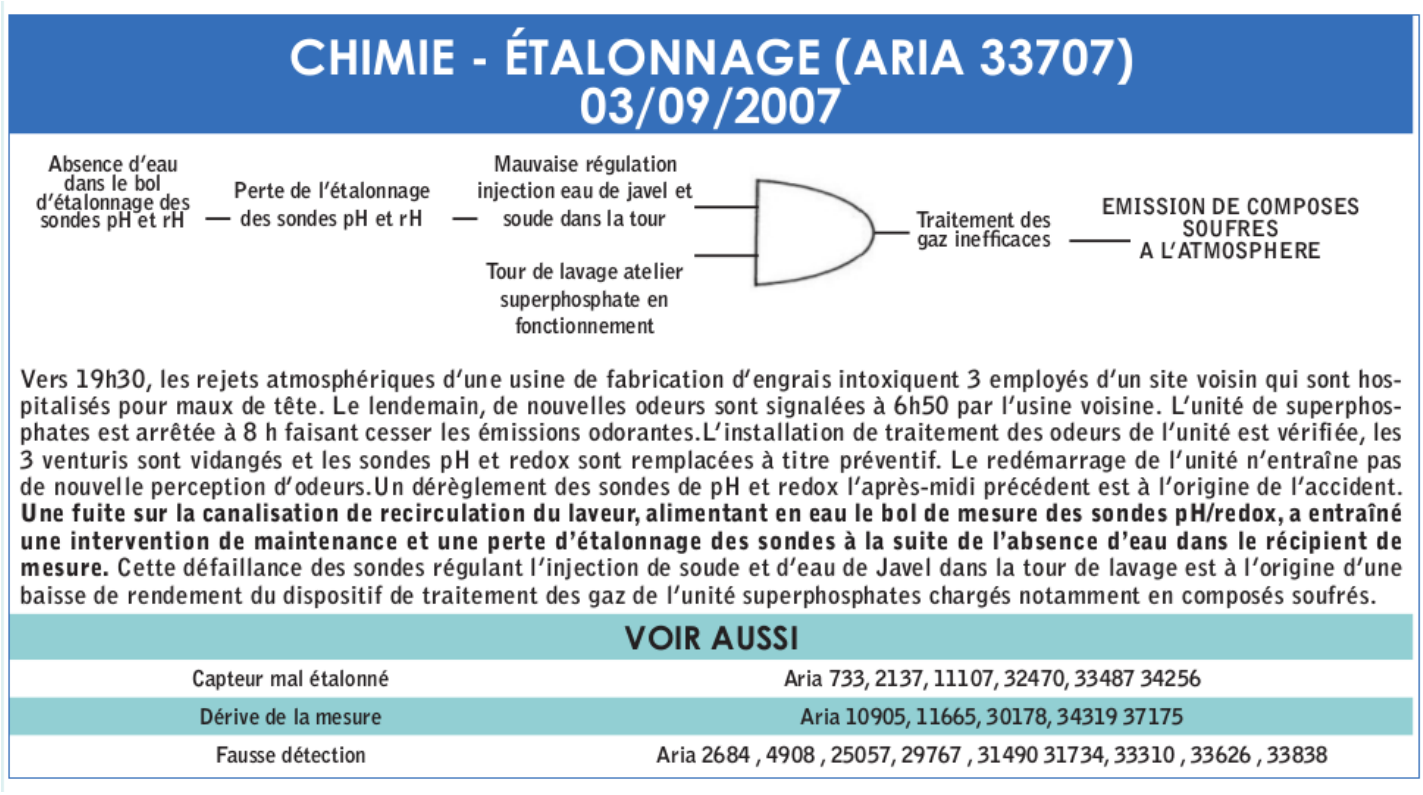
L'accidentologie des capteurs a fait l'objet d'une étude par le BARPI en 2012. L'étude est téléchargeable sur internet à partir de l'adresse suivante : https://www.aria.developpement-durable.gouv.fr/synthese/syntheses/accidentologie-des-automatismes-industriels-le-capteur/.

Parmi les enseignements tirés de cette analyse, nous pouvons noter que :

- Les accidents impliquant des capteurs ne représentent qu'une faible partie des accidents de la base ARIA (3 % des accidents), et ceux causés par des défaillances critiques de capteur moins de 2% ;
- L'implication des capteurs dans l'accidentologie est plus marquée en dehors des phases d'exploitation normale des installations : redémarrage, arrêt ou mise à l'arrêt ;
- Plus d'un accident capteur sur deux est dû à une panne, les deux tiers des causes identifiables relèvent d'une erreur humaine ou d'une organisation inadaptée : manque d'entretien, mauvais branchement, défaut de nettoyage…
- Pour les secteurs les plus équipés en capteurs, la fausse détection est à l'origine de plus de 20 % des accidents impliquant des capteurs défaillants. Elle découle en général d'une dérive de la mesure ou d'un défaut d'étalonnage ;

- Bien qu'ils soient moins répandus que les capteurs de température et de pression, les capteurs de niveau sont impliqués dans plus de 20 % des accidents étudiés, quel que soit le secteur d'activité. Leurs mécanismes les rendraient plus facilement sujets au blocage et au colmatage.

Exemples d'accidents :



Attaques informatiques de capteurs

La base ARIA ne comporte pas d'accidents impliquant une attaque informatique au sens classique de capteurs.

Les attaques semblent plutôt concernés les capteurs sans fil qui véhiculent via des ondes électromagnétiques des informations. Le cryptage des informations émises mérite ainsi une attention particulière (http://www.lemondeinformatique.fr/actualites/lire-les-capteurs-industriels-vulnerables-a-des-attaques-par-ondes-radio-54532.html).

Dans le cas d'un capteur sans fil, il convient également d'étudier la façon dont transitent les informations entre le centre de contrôle et le capteur. Est-ce le système SCADA qui envoie une requête au bout d'un certain laps de temps pour questionner le capteur, ou est-ce le capteur qui envoie sa télémesure ? Cette latence dans le traitement de l'information doit être mise en parallèle avec une éventuelle nécessité de traitement en temps réel des informations.

Les systèmes SCADA

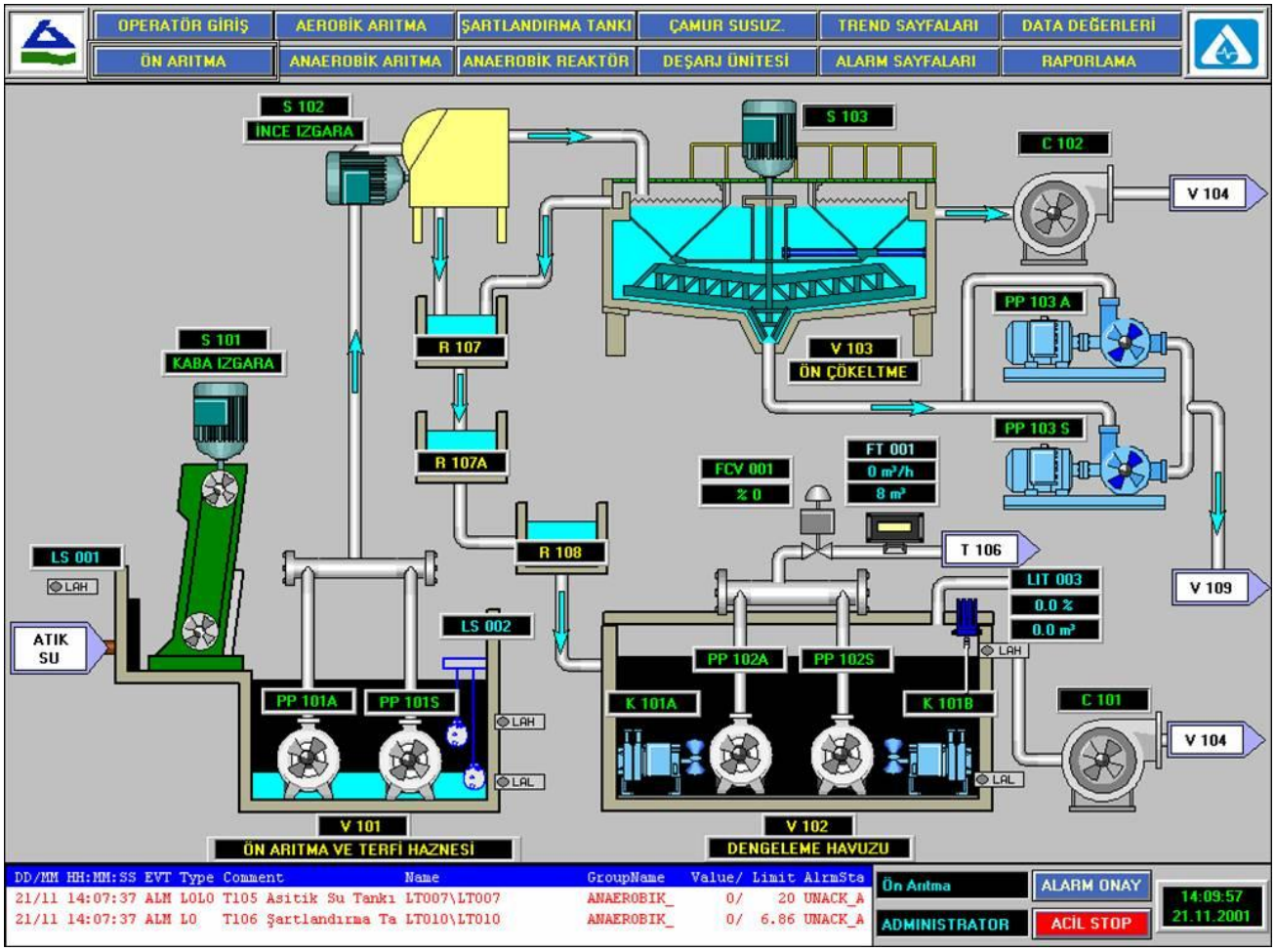
Définition :

Un système de contrôle et d'acquisition de données (SCADA en anglais) **gère et traite en temps réel** un grand nombre de télémesures. Il **contrôle** également à distance les installations techniques. Il s'agit en quelque sorte du cerveau du système de contrôle industriel. Le système **alerte** par ailleurs les opérateurs en salle de contrôle via des alarmes en cas de dépassement des paramètres physiques du procédé industriel.

Un SCADA comporte entre autre des contrôleurs, une base de données, un logiciel de gestion d'entrées-sorties et une interface homme machine. Les informations du dispositif SCADA sont centralisées sur une unité centrale. Celle-ci permet

à l'opérateur de commander tout ou partie des actionneurs d'une installation souvent très étendue (usine, réseau de distribution...). Le contrôle sur le terrain est réalisé par des terminaux distants (*RTU- Remote Terminal Units – confer schéma de la page 2*) ou par des automates programmables.

Exemple d'interface homme machine :



Accidentologie :

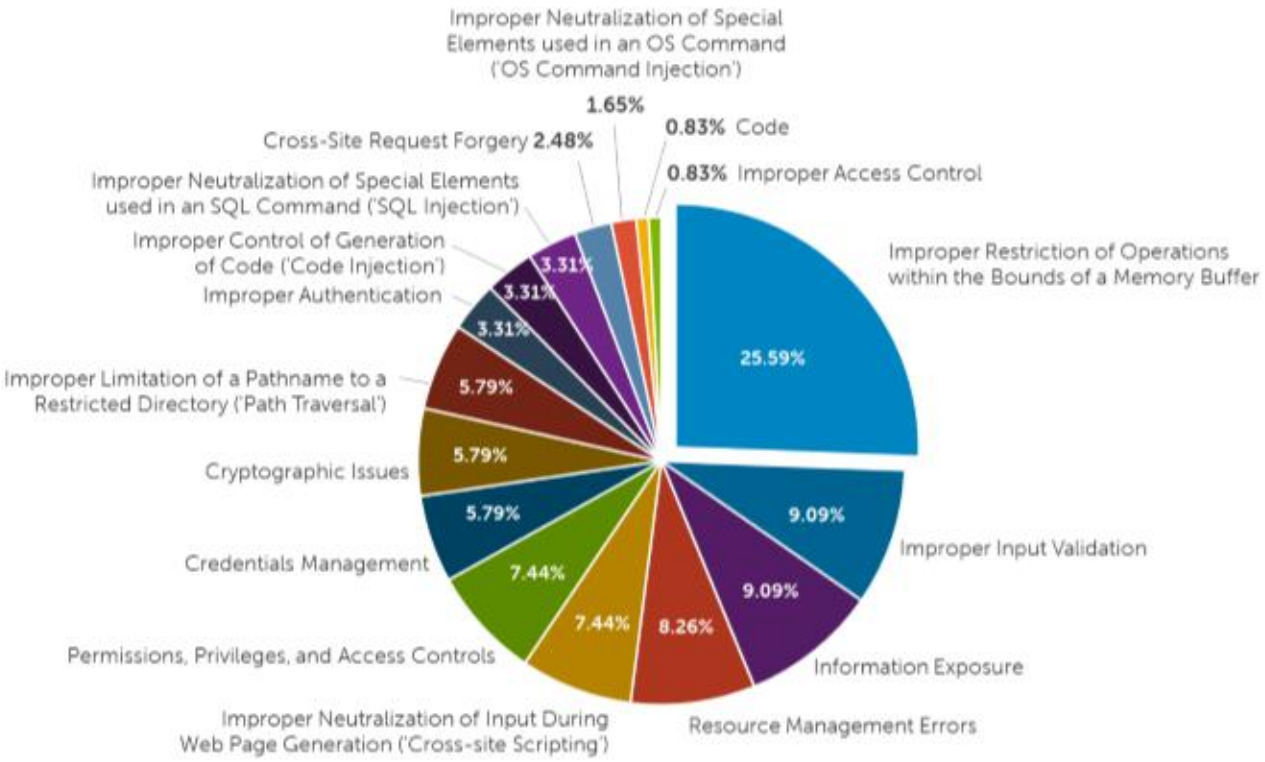
Hormis l'accident de Belligham aux Etats-Unis (ARIA 15621), la base ARIA ne répertorie pas d'accident où le mot « SCADA » est explicitement mentionné dans le résumé d'accident. Sans nul doute, ces systèmes ont été impliqués dans davantage d'événements, mais l'analyse des causes profondes n'a malheureusement pas été menée avec une vision sécurité informatique.

Néanmoins, certains enseignements peuvent être tirés de façon plus large sur l'ergonomie des interfaces homme machine, confer accidentologie de la partie traitement éditée en 2014 par le Barpi où il est noté que : « Si les défauts d'ergonomie concernent majoritairement des erreurs de perception en raison de paramètres importants non visibles par l'opérateur, elles sont aussi la source d'erreurs d'interprétation et de décision et parfois même d'exécution. »

Attaques informatiques :

Constitués de serveurs informatiques, les systèmes SCADA sont sensibles aux attaques informatiques telles que décrites dans les annexes de ce document. Ainsi, le constructeur américain de matériels informatiques Dell a observé plus de 91 000 attaques visant les Scada en janvier 2012, puis plus de 163 000 un an plus tard, et enfin plus de 675 000 en janvier 2014. Le groupe précise que la majorité de ces attaques ont visé des installations en Finlande, au Royaume-Uni et aux Etats-Unis, « probablement parce que les systèmes Scada sont plus répandus dans ces régions et plus susceptibles d'être connectés à Internet ». Ainsi, en 2014, près de 70 000 attaques ont visé les systèmes Scada outre-Manche. Ces chiffres

sont basés à partir du matériel que le constructeur a installé chez ces clients pour se prémunir d'éventuelles attaques. La répartition des différentes attaques observées est la suivante :



Dans plus de 25 % des cas, les attaques consistent à chercher et à exploiter des débordements de mémoire tampon. Par ailleurs, dans plus de 9 % des cas, les vulnérabilités visées concernent la validation des données en entrée. C'est sans compter avec l'injection SQL dans plus de 3 % des cas, ou encore l'injection de code, (3 %). Ce qui souligne tout l'intérêt à porter à la programmation des logiciels.

Viennent ensuite les vulnérabilités que l'on pourrait imputer à la mise en œuvre des systèmes concernés, ou à leur exploitation : vulnérabilités de chiffrement, gestion des identifiants, ou encore contrôle des accès et des droits (7,44 %).

La firme américaine recommande à ces clients de :

- s'assurer que les systèmes Scada et leurs logiciels sont à jours ;
- contrôler que le réseau n'accepte que des connexions d'adresses IP « approuvées » ;
- bloquer les ports USB et les interfaces Bluetooth lorsqu'ils ne sont pas nécessaire ;
- partager les informations sur les attaques informatiques.

Les protocoles de communication

Une grande variété de protocoles de communication est utilisée dans les systèmes de contrôle industriel (confer le schéma de la page 5). Une recherche par mots clés « profibus, profinet, ASI, etc … » a permis de mettre en évidence un événement impliquant le protocole ethernet dans une usine de plasturgie en France. Des paramètres de contrôle ont été gardés en mémoire au niveau d'un serveur à la suite d'une micro-coupure de la liaison ethernet, conduisant à une émission de chlrore :

N°43639 - 03/04/2013 - FRANCE - 57 - MORHANGE

C22.21 - Fabrication de plaques, feuilles, tubes et profilés en matières plastiques

Une surchauffe se produit vers 14h10 dans un mélangeur contenant 400 kg de PVC dans une usine de plasturgie. Une odeur de chlore est sentie par le personnel qui est évacué. Les installations sont mises hors-service. Des mesures de chlore sont effectuées et se révèlent négatives. Les pompiers, secondés par des employés sous protection respiratoire vidangent le mélangeur. L'intervention s'achève à 16h15. La gendarmerie s'est rendue sur place.Le mélangeur est géré par une unité centrale (CPU) reliée elle-même à un serveur permettant la programmation, le suivi et l'enregistrement des paramètres de production. Chacun des 3 mélangeurs possède sa CPU mais le serveur est commun. Une micro-coupure de la liaison Ethernet s'est produite entre la CPU du mélangeur incriminé et le serveur, générant un "effet de mémoire" vers le serveur qui indiquait des valeurs de production normales, même après arrêt effectif. Ce dernier n'a donc pas déclenché la mise à l'arrêt automatique du mélangeur. Même sans lien avec le serveur, la CPU est capable de mener le mélange à son terme. Après analyse avec le fournisseur, la raison de la défaillance de la CPU n'a pas pu être éclaircie, de même que la raison de la micro-coupure, le câble ne présentant aucune détérioration.L'exploitant prévoit d'équiper le mélangeur d'une boucle de sécurité supplémentaire indépendante de la CPU et du serveur, permettant l'évacuation automatique du mélange vers la cuve de refroidissement en cas de dépassement d'une température donnée. Le mélangeur sera arrêté et une alarme se déclenchera dans les 15 sec qui suivent. Il prévoit d'insérer cette même boucle au programme du serveur. Le programme de l'automate sera également modifié pour ajouter un paramètre de suivi prenant en compte la durée du mélange et permettant son arrêt en cas de dépassement. Ces modifications ont été réalisées début juillet et la remise en service du mélangeur est conditionnée à la réalisation de tests de fonctionnement positifs. Enfin, l'exploitant prévoit des actions complémentaires, telles que le changement de tous les câbles dits "sensibles" (connexions digitales et analogiques). En lien avec le fournisseur, il vérifiera la possibilité de modifier le programme de l'automate afin d'éviter le figeage des valeurs en cas de rupture de la liaison Ethernet, ainsi que le bon fonctionnement du programme dans le cas de diverses ruptures de connexions envisageables et la possibilité d'intégrer des boucles de sécurité supplémentaires pour ces différents cas. Toutes les actions définies pour ce mélangeur seront étendues aux deux autres.

Les systèmes de climatisation

Deux événements impliquant des systèmes de climatisation et ayant affecté des centres de traitement informatique sont recensés dans la base ARIA :

N°43506 - 19/02/2013 - FRANCE - 33 - SAINT-MEDARD-EN-JALLES

O84.11 - Administration publique générale

Dans la salle informatique du bâtiment administratif d'un centre d'études techniques, une soupape de sécurité "saute" vers 11h30 sur un climatiseur en cours de maintenance. Tout le frigorigène chloro-fluoré mis en oeuvre dans l'installation s'échappe à l'atmosphère, le jet sous pression endommage et disperse dans l'air le flocage contenant de l'amiante. Le brouillard déclenche la détection incendie et l'extinction automatique. Les 100 employés évacuent le bâtiment.En défaut à la suite d'une fuite de frigorigène observée depuis plusieurs mois, le climatiseur est réparé par une société spécialisée. La détection incendie fonctionne normalement. Des extincteurs supplémentaires sont installés dans le local, les bouteilles du système d'extinction ne pouvant être remplacées que 15 jours plus tard. Tant que la climatisation ne peut être remise en service (remplacement de la soupape), le fonctionnement du centre serveur est fragilisé en raison de la présence d'un seul groupe froid non secouru électriquement.

N°5132 - 30/03/1994 - FRANCE - 92 - COURBEVOIE

D35.30 - Production et distribution de vapeur et d'air conditionné

Une explosion se produit à 1h30 dans une chaufferie urbaine (500 MW, 6 000 m²), l'énergie dissipée dans le sol est estimée à l'équivalent d'une charge de 50 kg de TNT. Mise en service en 1987, cette chaufferie comporte 5 chaudières (2 au charbon, 2 mixtes charbon/gaz et 1 au gaz). Au cours du poste précédent, plusieurs tentatives de démarrage d'une chaudière mixte échouent. Ne parvenant toujours pas à la redémarrer et les manomètres d'arrivée de gaz indiquant une pression nulle, le chef de quart de l'équipe de nuit donne l'instruction d'ouvrir les 2 vannes quart de tour de sectionnement de l'arrivée de gaz sur le circuit principal. La pression indiquée restant nulle, il demande alors au conducteur de chaudière d'ouvrir un obturateur guillotine puis une vanne papillon pour permettre l'alimentation de la chaudière mixte en gaz. Cette opération entraîne une fuite importante de gaz. Une chaudière au gaz est arrêtée d'urgence et 2 opérateurs sortent pour couper l'alimentation générale au poste de détente, à 110 m du bâtiment, lorsque l'explosion survient.L'un des 5 employés est tué. Une fillette de 10 ans habitant à 40 m de l'usine décèdera 4 jours plus tard des suites de ses blessures ; 59 autres riverains sont blessés. L'installation est ravagée. Les quartiers voisins subissent d'importants dommages, 600 personnes sont en chômage technique et 250 riverains sont à reloger. En attendant leur connexion sur des réseaux voisins 140 000 usagers et 2,2 Mm³ de bureaux sont privés de chauffage et d'eau chaude. Le fonctionnement de grands réseaux informatiques climatisés par la centrale est perturbé. Les dommages sont évalués à 544 MF (83 M.euro). Selon les résultats de l'enquête, 3750 Nm3 de gaz auraient été relâchés jusqu'à ce que le service du gaz coupe l'alimentation 30 min après l'explosion. Les manomètres défaillants auraient pu avoir été endommagés par une surpression antérieure à l'accident. Les interventions du chef de quart ne devaient être réalisées que par le service de maintenance ; en cas d'urgence, les opérateurs de la centrale devaient demander l'intervention du service du gaz. L'obturateur n'était pas conçu pour être manipulé sous pression et la vanne papillon en amont de l'obturateur guillotine aurait été manipulée par le conducteur de chaudière alors que l'obturateur était resté en position intermédiaire, position dans laquelle il n'est plus étanche car les brides sont légèrement écartées. Le nuage de gaz s'est alors enflammé au contact de la chaudière à charbon en service au moment du sinistre. Par ailleurs, aucun scénario de fuite et d'explosion de gaz n'était évoqué dans l'étude de dangers du site. Les risques liés aux poussières de charbon n'y étaient pas non plus abordés. Le comportement des poussières a probablement contribué à la violence de l'explosion.Le 5 mai 2004, le juge d'instruction de la Cour d'appel de Versailles conclut à un non-lieu.

Points de réflexion pour évaluer la sécurité informatique d'une usine

En conclusion, plusieurs enseignements semblent se dégager de la présente analyse et de l'étude de l'accidentologie. Les principaux items méritant d'être analysés lors d'un audit d'un système informatique dans une usine seraient relatifs à/au :

- **L'organisation de l'entreprise :**
  - Existe-t-il un référent sûreté ? A-t-il des compétences en matière de cybersécurité ? Si non, qui s'occupe de ces aspects ? Y-a-t-il une coordination entre les deux personnes ?
  - Règle de clôture des comptes informatiques lorsque quelqu'un part ?
  - Existe-t-il une politique d'attribution des droits reposant sur deux grands principes : n'attribuer que les droits strictement nécessaires, et n'utiliser que les droits strictement nécessaires (en d'autres termes, une personne ayant des droits d'administrateur sur un système informatique doit se connecter avec un autre compte, ayant des droits réduits, lorsqu'il n'effectue pas des tâches d'administration) ;
  - Comment sont gérés les mots de passe ? Existe-t-il une politique de gestion locale ? Est-elle régulièrement contrôlée y compris pour les mots de passe de systèmes théoriquement non connectés ?
  - Les armoires techniques où se trouvent les automates sont-elles sécurisées ?
  - La salle des serveurs informatiques est-elle à accès restreint ? Des procédures de sauvegarde existent-t-elles ? Se faire préciser le niveau (sauvegarde au niveau des serveurs du système SCADA ? des programmes gérant les automates ? …) ;

- **La sécurité informatique :**
  - Le système informatique est-il indépendant de celui lié à la gestion/ télésurveillance de l'entreprise ? Se faire préciser la nature de la protection (pare feu) et les personnes habilités à y avoir accès ? L'exploitant dispose t'il d'un schéma conceptuel de son réseau avec les différents protocoles utilisés (éthernet, profibus)? Le schéma englobe t'il toute la chaîne des différents réseaux informatiques de l'entreprise (bureautique, téléalarme, etc) au SCADA jusqu'au capteur, en passant par les accès VPN et VNC ?
  - Que se passe-t-il en cas de perte de la connexion ethernet ? Le réseau est-il redondant ?
  - Les protocoles de communication à l'intérieur du réseau sont-il sécurisés (pas de transmission d'information par http, Ftp, telnet…) ;
  - Des sondes d'analyse du trafic TCP/IP sont-elles installées ? Fréquence et nature des contrôles ? Que se passe-t'il en cas de détection d'anomalie ?
  - L'industriel connaît-il l'Anssi et ses guides (par exemple le guide d'hygiène informatique) ? Sont-ils appliqués en totalité (mot de passe, sensibilisation du personnel sur la cybersécurité) ? Utilise-t-il du matériel certifié par l'Anssi ? Pourquoi ?

Les guides de l'ANSSI sont librement téléchargeables sur internet à l'adresse suivante :
http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

  - L'exploitant utilise-t-il un système SNMP (Simple Network Management Protocole) pour mettre à jour l'ensemble du matériel informatique de son parc ? Est-il à jour ? Comment s'assure-t-il que des mises à jour ne sont pas potentiellement dangereuses ? Comment est réalisée l'identification des sources de fichiers ?
  - le système d'exploitation utilisé fait-il toujours l'objet de mise à jour de la part du constructeur (Windows 2000, NT, XP?)
  - Le système informatique de l'entreprise a t'il fait l'objet d'un audit par une société spécialisée ? Est-ce que les éventuelles non-conformités sont soldées ? Possibilité de voir le dernier compte rendu d'audit ? Vérifier quelle partie du système a été auditée (le système SCADA, les modules de transmission qui sont déportés, les routeurs ou switch, etc) ;
  - Certains modules d'entrée/sortie au niveau des automates acceptent des cartes SD (par exemple Siemens ET200S, comment ces cartes sont gérées en interne ?
  - Des logiciels de contrôle à distance du système sont-ils installés ? Leur sécurité a-t-elle été évaluée ?

- De la maintenance ou de la surveillance est-elle réalisée à l'aide de logiciels téléchargés sur le Google playstore ou l'Apple market ? Le risque lié à leur utilisation est-il évalué ?
- Gestion des changements sur le réseau ou au niveau des automatismes ? Une analyse de risques est-elle réalisée ?
- Une phase de repli sûr des procédés industriels utilisés sur le site est-elle définie ? En cas de perte de l'informatique, l'exploitant est-il en mesure de maîtriser les procédés en cours sur son site, peut-il piloter manuellement ses installations ?

- **Partage de l'information / veille informatique** :
  - Les événements jugés anomaux sont-ils consignés ? Sont-ils déclarés à l'Anssi et à l'inspection des installations classées dès lors qu'ils sont susceptibles de conduire à un scénario de risques accidentels ?

Le formulaire de transmission d'information à l'Anssi en cas d'accident est téléchargeable à l'adresse suivante :
https://www.ssi.gouv.fr/uploads/2016/04/formulaire-declaration-incident-lpm_anssi.pdf

  - Comment l'exploitant effectue sa veille en matière de cybersécurité (veille sur des sites internet spécialisés, lesquels ?, suivi des failles informatiques et des mises à jour des composants constituant les automates notamment leur firmware (logiciel interne servant à leur fonctionnement) ?…)

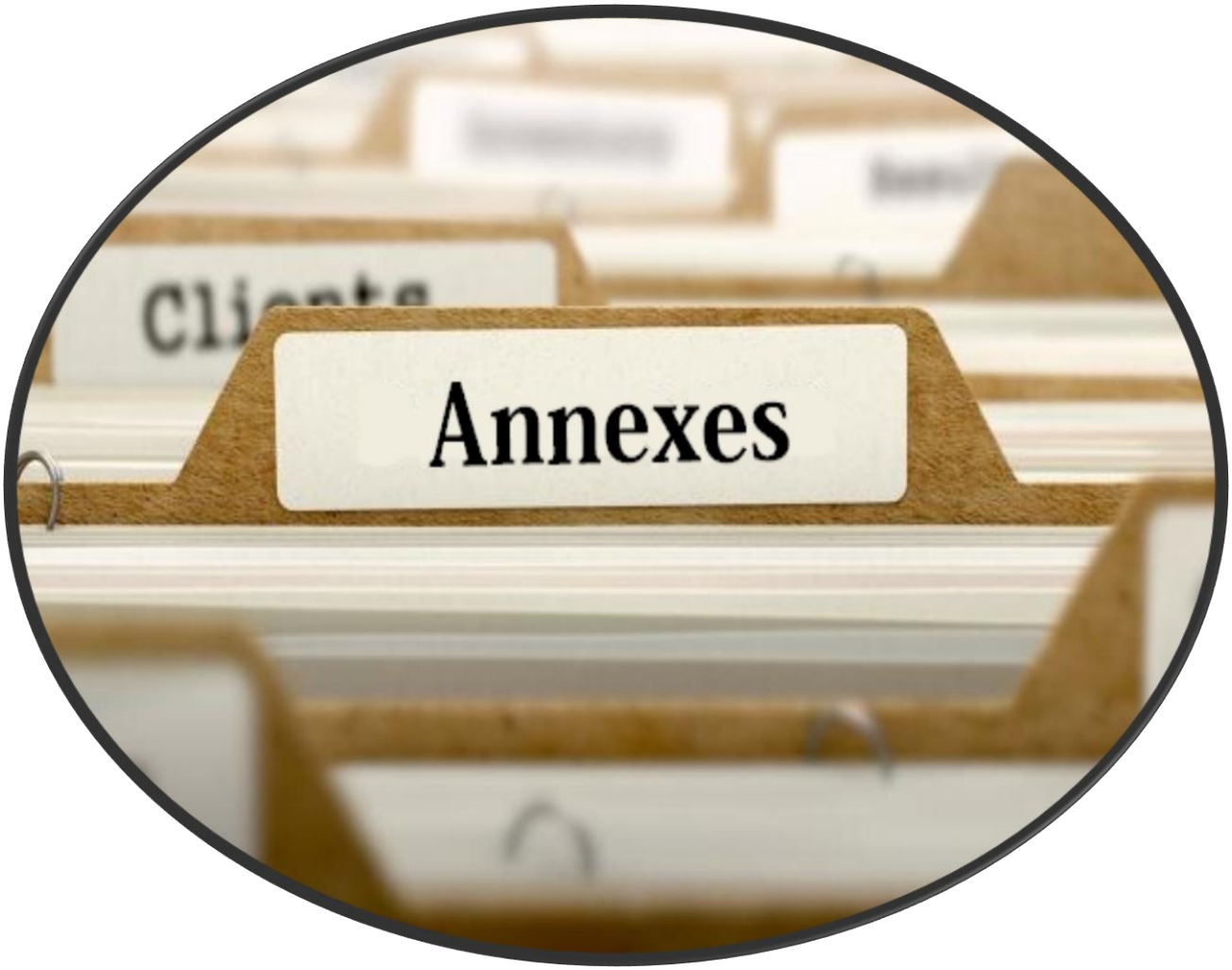
- **La fiabilité des moyens de mesure :**
  - Reposent-ils uniquement sur des capteurs reliés au SCI ? Existent-ils des moyens de mesures physiques indépendants du SCI (plus difficilement piratable) ?
  - Les capteurs sont-ils correctement entretenus (risque d'encrassage / corrosion)? Par qui ?
  - Les préconisations du constructeur en termes d'étalonnage sont-elles respectées ? Justifier les cas de dérogation aux préconisations du constructeur ?
  - Les capteurs sont-ils bien placés aux bons endroits (capteur de niveau) ?
  - Des relevés des mesures physiques sont-ils prévus ? Historique des relevés ?
  - Que se passe-t-il en cas de décalage de mesure ?
  - Les problèmes de sécurité liés à la télétransmission d'informations par des capteurs sans fil ont-ils bien été pris en compte ? Risque de brouillage des transmissions ?

- **La confidentialité des informations :**
  - Existe-t-il dans l'entreprise une politique de protections des données (informatique, process industriel,...) ?
  - Les informations concernant la résistance des équipements sous pression (PMS, pression de rupture, pression de tarrage des soupapes) sont-elles en libre accès sur internet ?
  - Les informations disponibles sur internet ne sont pas de nature à faciliter la compréhension du process industriel de l'entreprise par un pirate informatique ?

- **La sous-traitance :**
  - Sur quelles parties du SCI un sous-traitant peut intervenir ?
  - Est-ce que le sous-traitant est audité et habilité pour les interventions qu'il a à réaliser (qualité de la programmation / connaissance du process industriel et des installations) ?
  - Peut-il intervenir rapidement en cas d'accident ou nécessité de reprogrammer un automate ?
  - Le matériel (PC portable) utilisé pour la programmation des automates est-il fiable (mise à jour du système d'exploitation, protection anti-virus ...)? Une bonne pratique consiste à ne pas autoriser l'admission de PC étrangers (utilisation de PC "prisonniers du site" pour les mises à jour) ;
  - Le prestataire dispose-t-il de toutes les informations (mots de passe) concernant le système de contrôle industriel ou uniquement celles nécessaires à sa mission ?
  - L'exploitant est-il en mesure d'intervenir sur son réseau ou fait-il systématiquement appel à un prestataire externe ?

- **Système de climatisation :**
  - La défaillance du système de climatisation est-elle envisagée ? l'exploitant dispose-t-il d'un système de secours ?
  - La maintenance et le suivi réglementaire des groupes froids au titre de la réglementation des équipements sous pression sont-ils correctement réalisés ?
  - Dans le cas d'audit de chaufferies urbaines fournissant du « froid » à d'autres entreprises, il convient de regarder les conséquences sur ces établissements, notamment les data-center (cloud computing).

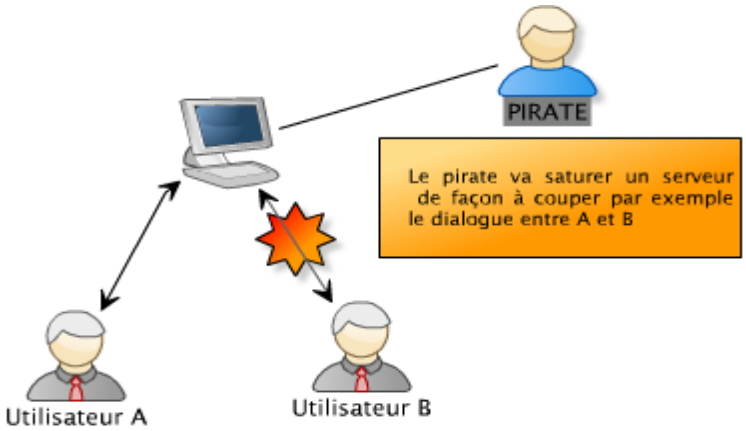
- **Fiabilité des communications :**
  - Y-a-t-il une redondance au niveau de la liaison internet avec des opérateurs téléphoniques différents ?
  - Les nœuds de raccordement ou points de mutualisation de zone optique sont-ils distants des nœuds de raccordement des abonnés (RTC) ? Leur accès est-il sécurisé ?


Annexes

LES DIFFÉRENTES TECHNIQUES D'ATTAQUES INFORMATIQUES

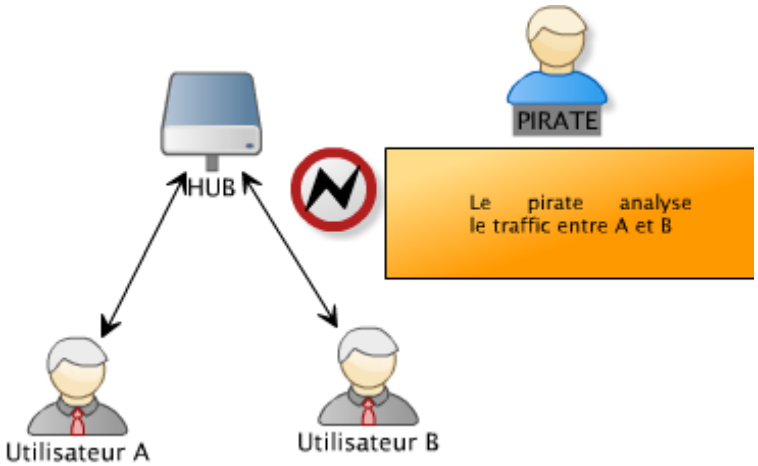
Les attaques les plus couramment réalisées, évoquées ci-dessous, peuvent être uniques, ou se combiner entre elles, pour former selon le terme consacré, "une chaîne d'exploits". Les pirates informatiques sont en général compétents et n'agissent pas par hasard. Les finalités des attaques informatiques sont diverses : acte de malveillance interne ou externe à l'entreprise, terrorisme, espionnage industriel, guerre numérique afin de paralyser son ennemi à moindre frais, chantage...

- Le **déni de service** (en anglais Denial of service) : la victime se voit dans l'incapacité de communiquer (courriels, serveur de fichiers, site web indisponible…). L'inondation d'un serveur par des requêtes informatiques peut en être la cause.



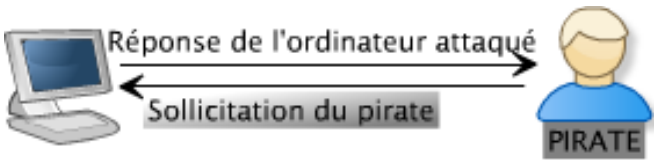
Objectifs cherchés par le pirate : chantage économique (payer pour que j'arrête), paralyser un site web, tremplin pour utiliser une autre technique d'attaque.
Moyen de protection : être à jour des correctifs logiciels sur son système d'exploitation.

- Le **reniflage** (en anglais Sniffing) : le pirate analyse le trafic de données entre 2 ordinateurs afin de découvrir des données sensibles (noms d'utilisateurs et mots de passe, clé sécurisée du signal Wifi)



Objectifs cherchés par le pirate : pénétrer un système dans le but de voler des données ou de prendre l'identité numérique de quelqu'un.
Moyens de protection : utiliser de préférence un switch (commutateur) plutôt qu'un hub ; utiliser des protocoles chiffrés pour les informations sensibles comme les mots de passe.

- Le **scanning** : un appareil (scanner) balaye les ports de communication d'une machine afin de déterminer ceux qui sont ouverts ou fermés. Cette technique permet de déterminer le système d'exploitation de la machine attaquée ainsi que les applications associées à chaque port. Un administrateur système peut recourir à cette méthode dans le cadre de son travail. Il faut donc être capable de distinguer un pirate d'une personne habilitée.



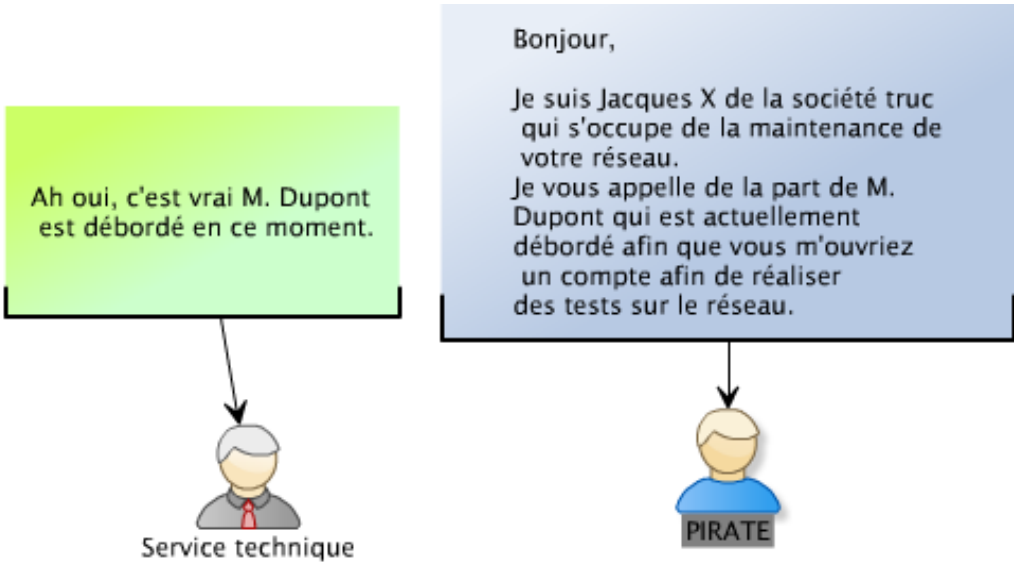
A partir des réponses de l'ordinateur à certains types de sollicitations, le pirate détermine les failles de sécurité du système.

Objectif cherché par le pirate : identifier les cibles potentielles
pour réaliser une attaque par déni de service par la suite.
Moyens de protection : faire un inventaire régulier des ports ouverts sur sa machine ;
utiliser un firewall ou des détecteurs d'intrusion.

Comment connaître les ports ouverts sur son ordinateur ?

Il y a différentes façons de faire, la plus simple étant de se mettre en ligne de commande. La commande est ***netstat -an***. Les ports ouverts sont indiqués par la mention "listening".

- L'**ingénierie sociale** : elle repose sur l'art de manipuler les personnes à travers les informations trouvées sur les réseaux sociaux ("facebook", "copains d'avant", etc). Elle ne nécessite pas de connaissance particulière en informatique.



Objectifs cherchés par le pirate : abus de confiance, essayer de deviner un mot de passe
(date et lieu de naissance) dans l'espoir d'usurper par la suite l'identité de la victime (compte de messagerie).
La victime est parfois placée dans un état de stress intense (demande urgente) dans l'optique qu'elle donne des informations ou qu'elle réalise des actions, qu'elle n'aurait jamais données ou réalisées en temps normal.
Moyens de protection : le bon sens et une organisation adaptée au sein de l'entreprise
pour faire face à ce type de situation.

- Le **crackage des mots de passe**, pour cela les pirates utilisent plusieurs techniques :

- les attaques par dictionnaire : cette méthode teste tous les mots d'un dictionnaire car beaucoup d'utilisateurs utilisent des mots existants comme mots de passe ;
- les attaques hybrides : cette méthode essaie des combinaisons de mots et de chiffres par exemple "enveloppe01" ;
- les attaques par force brute : toutes les combinaisons de chiffres et de lettres sont testées. L'attaque aboutit toujours, en revanche les temps de calcul sont plus ou moins longs suivant le mot de passe et les moyens dont dispose le pirate informatique ;
- une veille sur internet permet de savoir les mots de passe utilisés par défaut lors de la livraison des équipements. Ces derniers ne sont pas toujours changés en phase d'exploitation. Ceci nécessite toutefois une reconnaissance des lieux pour connaître le type de matériel utilisé par l'industriel (voir rubrique d'usurpation physique d'identité) ;
- les logiciels de type keylogger permettent d'enregistrer les informations que tape un utilisateur sur son clavier.

Objectifs cherchés par le pirate : prendre le contrôle d'un système (droit administrateur), vol de données, prendre le contrôle d'un compte de messagerie...
Moyens de protection : utiliser des mots de passe mnémotechniques, recourir à la double identification (taper son mot de passe puis envoi d'un SMS avec un code sur son portable)
Note : pour les courriels et toute communication : utiliser un logiciel de chiffrement des données.

- L**'usurpation informatique d'identité** :
  - prendre l'adresse IP ou MAC de l'ordinateur (en anglais IP ou MAC spoofing) que l'on souhaite attaquer. Ces données sont parfois en libre accès sur internet via des moteurs de recherche spécialisés (le site shodan.io est le "google" des objets connectés) ;
  - prendre l'adresse courriel d'une personne ;
  - utiliser le Phishing : par exemple envoi d'un courriel reproduisant la charte graphique d'un organisme bancaire.

Objectifs cherchés par le pirate : obtenir des informations, faire télécharger un logiciel malveillant à quelqu'un...
Moyens de protection : Se méfier des messages reçus et ne pas hésiter à prendre contact avec l'expéditeur par téléphone ou autre moyen pour bien confirmer la demande.

- L**'usurpation physique d'identité** :
  - l'utilisation de scanner RFID pour copier les badges d'accès à des bâtiments sécurisés. Ces équipements sont en vente libre sur amazon pour une soixantaine d'euros (confer bibliographie).

Objectifs cherchés par le pirate : installer dans les locaux du matériel infecté type clé USB, logiciel de keylogger. Trouver des mots de passe (post-it sur les écrans ou sous les claviers). Trouver un PC avec une session ouverte pour pouvoir envoyer un courriel, fouiller les poubelles.
Moyens de protection : Le gardiennage. La vidéosurveillance avec une gestion stricte du personnel interne et externe au site. Politique de destruction des documents confidentiels.

- Les **erreurs d'exécution ou le dépassement de tampon** (Buffer over Flow) : il s'agit d'introduire une chaîne de caractères particulière afin d'initier ou de provoquer une erreur d'exécution (failles SQL ou javascript pour les bases de données).

Objectif cherché par le pirate : prendre le contrôle d'un site internet ou d'un système informatique.
Moyens de protection : Cette technique utilise les défauts ou anomalie de programmation d'un logiciel (bugs). Il convient de se tenir au courant des failles de sécurité de son système informatique.
Remarque : les failles de sécurité les plus connues sont recensées sur le site http://www.cert.ssi.gouv.fr/site/index.html

- Les **attaques par logiciels de rançon (Locky) après une usurpation d'identité (par exemple factures Free mobile) : l'utilisateur reçoit un logiciel malveillant via un fichier word contenant des macros qui vont crypter le contenu du disque dur de sa machine la rendant ainsi inutilisable.** Le retour à la normale ne peut se faire qu'à travers le paiement d'une somme d'argent. Cette menace est assez répandue en France (confer bulletin d'alerte n°CERTFR-2016-ALE-001 de l'ANSSI du mois de mars 2016).
  L'ordinateur pilotant une hydrolienne dans le Finistère (29) a par exemple été piraté de cette façon (ARIA 48048). L'hydrolienne n'a pas produit d'électricité pendant 15 jours.

Objectif cherché par le pirate : gagner de l'argent.
Moyens de protection : Désactiver par défaut les macros des suites offices Microsoft ou Libre Office.
Mettre à jour son logiciel antivirus.

Certaines **attaques** ne nécessitent **pas de connaissances pointues en informatique**, mais juste une **veille sur internet** (attaque par ingénierie sociale ou par exploitation des failles de sécurité par exemple).

QUELQUES ATTAQUES INFORMATIQUES MEDIATIQUES

1- Stuxnet

Généralités : Ce virus informatique a été découvert en 2010. Il avait pour but de s'attaquer au programme nucléaire iranien. Le logiciel modifiait la vitesse des moteurs des centrifugeuses dont le rôle est de séparer physiquement les isotopes de l'uranium pour fabriquer un combustible nucléaire hautement enrichi. Environ 1 000 centrifugeuses auraient été endommagées.

Principe de l'attaque : Le virus s'attaque aux systèmes Windows en utilisant leurs failles de sécurité et vise les systèmes utilisant des logiciels SCADA. Le virus est inoculé à l'aide d'une clé USB. Il contamine ensuite d'autres ordinateurs du réseau. Une fois dans le système, il utilise les mots de passe par défaut pour faire des requêtes. La complexité du ver est inhabituelle pour un malware : l'attaque demande à la fois **des connaissances en procédés industriels** et en informatique (**failles du système Windows)**.

2- Attaque informatique dans une aciérie en Allemagne

Généralités : Au cours de l'année 2014, un haut fourneau allemand est endommagé faute d'avoir été mis en sécurité à temps.

Principe de l'attaque : en utilisant une attaque par **ingénierie sociale**, les pirates se sont d'abord infiltrés dans le système informatique de la partie administrative de l'entreprise, puis ils se sont ensuite introduits dans celui pilotant la production. L'attaque a provoqué la **défaillance de plusieurs composants** qui ont **empêché l'arrêt contrôlé du haut fourneau**, l'endommageant. Selon le rapport de l'organisme d'état allemand (voir référence en annexe), les hackers disposaient de capacités techniques "très avancées". Ils **maîtrisaient également les processus de production industriels**.

3- Dragonfly

Généralités : En 2014, un groupe de Hackers dénommé "dragonfly" aurait pénétré les systèmes informatiques de grandes sociétés du secteur de l'énergie (électricité, gaz, opérateurs de pipeline, fournisseurs d'équipements). Selon la société Symantec (éditrice de logiciels anti-virus), la majorité des victimes se trouveraient aux États-Unis, ainsi qu'en Europe (Espagne, France, Italie, Allemagne). C'est **le second cas avéré de piratage de systèmes SCADA**, après le virus Stuxnet. Toutefois, le but de cette attaque informatique semblerait être l'**espionnage industriel**.

Principe de l'attaque : Le groupe Dragonfly utilise des campagnes d'envoi massif de courriels avec des pièces jointes infectées (PDF) auprès d'organismes et de personnes cibles (dirigeants et cadres supérieurs d'entreprises fournisseurs de service auprès d'industriels). Cette campagne de publipostage est par ailleurs renforcée par un phishing. L'utilisateur est ainsi réorienté sur un site internet pour télécharger des logiciels malveillants.

Une fois l'ordinateur cible atteint, un dispositif de porte dérobée (type malware Havex) est installé sur l'ordinateur pour en prendre le contrôle. Les données du carnet d'adresses d'Outlook et les fichiers de configuration VPN sont également extraites. Celles-ci sont ensuite écrites dans un fichier crypté avant d'être transmise au pirate.

Le groupe de pirates informatiques réussit ainsi à atteindre par étapes l'ordinateur cible (du fournisseur à l'industriel).

Parmi les entreprises ayant propagé l'infection figurent en particulier :

- l'Allemand MB Connect Line (contrôles pour éolienne et usines de biogaz) ;
- le Belge eWon (accès VPN).

4- BlackEnergy

Généralités : A la fin de l'année 2015, plus d'un million d'abonnés ukrainiens sont privés d'électricité. Selon plusieurs cabinets d'experts en sécurité informatique, un **malware** aurait infecté le réseau du fournisseur d'électricité Prykarpattya Oblenergo, dans l'ouest du pays. Cet événement constituerait le plus grand "blackout" informatique d'un système d'utilité publique. Une société de transport ferroviaire ainsi qu'une industrie minière ukrainienne auraient également été affectées.

Principe de l'attaque : Le logiciel malveillant se propagerait à l'aide d'une simple macro contenue dans un tableur. Pour flouer les destinataires, le courriel paraissait provenir d'un organisme d'état et contenait un message encourageant à ouvrir le document vérolé.

BlackEnergy offre la possibilité de créer une porte dérobée sur l'ordinateur afin de le contrôler à distance. Le malware intègre également un module d'accès aux systèmes de contrôle et d'acquisition de données (SCADA) de l'industriel.

La majorité des attaques étudiées semblent reposer sur le téléchargement de logiciels espions par un employé d'une entreprise. La vigilance de la personne lisant le courriel devrait être la meilleure arme contre la propagation de ce genre de menace.
Toutefois, les pirates via les techniques d'ingénierie sociale savent être convaincants dans leur demande. Ils peuvent ainsi se faire passer pour un simple fournisseur et transmettre une facture sous la forme d'un fichier PDF ou Excel infecté. La seule barrière est alors le logiciel anti-virus du poste du receveur. Toutefois, l'anti-virus devra avoir dans sa base de données les caractéristiques du malware transmis ; ce qui n'est pas évident en cas de nouveau virus polymorphe.
Une autre caractéristique commune des attaques étudiées est la connaissance des procédés et installations industrielles par les hackers. L'attaque vise en effet des systèmes qui sont au cœur de procédés industriels parfois complexes. Cet élément laisse penser que ces attaques sont menées par des personnes disposant d'une très forte culture informatique et industrielle.
En outre, un "air gap" '(absence d'interconnexion de SI) n'est pas une garantie contre une attaque, car cela se contourne souvent facilement si on dispose d'un appui interne (pose d'une clef wifi par exemple).

Sites internet et guides étrangers de bonnes pratiques :

Europe

Angleterre :

https://www.cert.gov.uk/

Suède :

https://www.msb.se/en/Prevention/Information-security/Publications/

Guide de sécurité des systèmes de contrôle industriels avec des recommandations :

https://www.msb.se/RibData/Filer/pdf/26118.pdf

Allemage :

https://www.bsi.bund.de/DE/Home/home_node.html

Espagne :

https://www.osi.es/

Hors Europe :

Etats-Unis :

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

https://www.us-cert.gov/

Chine :

中国信息安全测评中心
China Information Technology Security Evaluation Center

http://www.itsec.gov.cn/

ACCIDENTS TECHNOLOGIQUES EN LIGNE

Sécurité et transparence sont deux exigences légitimes de notre société. Aussi, depuis juin 2001 le site www.aria.developpement-durable.gouv.fr du Ministère de la Transition écologique et solidaire, propose-t-il aux professionnels et au public des enseignements tirés de l'analyse d'accidents technologiques. Les principales rubriques du site sont présentées en français et en anglais.
Sous les rubriques générales, l'internaute peut, par exemple, s'informer sur l'action de l'Etat, disposer de larges extraits de la base de données ARIA, découvrir la présentation de l'échelle européenne des accidents, prendre connaissance de l'indice relatif aux matières dangereuses relâchées pour compléter la « communication à chaud » en cas d'accident ou d'incident.

La description des accidents, matière première de toute démarche de retour d'expérience, constitue une part importante des ressources du site : déroulement de l'événement, conséquences, origines, circonstances, causes avérées ou présumées, suites données et enseignements tirés.

Une centaine de fiches techniques détaillées et illustrées présente des accidents sélectionnés pour l'intérêt particulier de leurs enseignements. De nombreuses analyses par thème ou par secteur industriel sont également disponibles. La rubrique consacrée aux recommandations techniques développe différents thèmes : chimie fine, pyrotechnie, traitement de surface, silos, dépôts de pneumatiques, permis de feu, traitement des déchets, manutention...

Une recherche multicritères permet d'accéder à l'information sur des accidents survenus en France ou à l'étranger.

Le site www.aria.developpement-durable.gouv.fr s'enrichit continuellement. Actuellement, près de 50 000 accidents sont en ligne et de nouvelles analyses thématiques verront régulièrement le jour.

Les résumés des évènements présentés sont disponibles sur le site :

www.aria.developpement-durable.gouv.fr

Bureau d'analyse des risques et pollutions industriels
5 place Jules Ferry
69006 Lyon
Téléphone : 04 26 28 62 00

Service des risques technologiques
Direction générale de la Prévention des risques
Ministère de l'Environnement, de l'Énergie et de la Mer
Tour Sequoia
92055 La Défense cedex
Téléphone : 01 40 81 21 22

Coordination :
Annie NORMAND, Christian VEIDIG

Rédaction :
Jean-Francois MICHEL

Crédits photos : hhdgomez

Date de rédaction du document : juillet 2016

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE