Chapitre XV

Zoom sur la norme internationale IEC 62443 pour la cybersécurité des systèmes numériques industriels

Pierre KOBES (Siemens)

Dans le domaine de l'informatique de gestion il existe des standards couramment utilisés par les entreprises pour la mise en place de mesures pour protéger les informations contre les manipulations ou le vol. La série de normes ISO/IEC 27000 constitue un référentiel largement accepté. Pour la cybersécurité appliquée aux installations industrielles, l'évolution a été beaucoup plus récente. Les initiatives isolées de divers pays ou organisations semblent cependant se consolider dans la norme internationale IEC 62443 qui est spécialement dédiée aux installations industrielles. Bien que tous les documents de cette norme ne se soient pas encore achevés, il semble que son adoption s'étende aux divers domaines industriels. Il est à noter que l'administration américaine FDA *(Food and Drug Administration)* a référencé cette norme en devenir pour les systèmes informatiques en milieu médical. Un signe supplémentaire qui justifie que l'on s'y intéresse de près.

1. Champ d'application de l'IEC 62443

La norme IEC 62443 est dédiée à la sécurité informatique des IACS *(Industrial Automation and Control Systems)*. Elle couvre les systèmes utilisés dans les installations de production de l'industrie manufacturière et des procédés continus, les automatisations de bâtiments, les sites dispersés géographiquement comme les réseaux de distribution (eau, gaz, électricité, pipelines, etc.), ainsi que d'autres industries et applications comme les réseaux de transport mettant en œuvre des équipements automatisés.

Le terme IACS inclut tout ce qui est nécessaire pour régir ou influencer le contrôle des processus industriels de manière sûre, sécurisée et fiable. L'IACS a une composante technique, la solution d'automatisation incluant :

– les SCI (systèmes de contrôle industriels) et leurs réseaux de communication englobant entre autres les systèmes numériques de contrôle-commande,

les systèmes SCADA *(Supervisory, Control and Data Acquisition)*, les automates programmables, les terminaux distants, les équipements électroniques intelligents, etc. Les SCI peuvent avoir un BPCS *(Basic Process Control System)*, dont la fonction est le contrôle du processus de production ainsi qu'un SIS *(Safety Instrumented System)* qui est destiné à la protection des biens et des personnes contre un dysfonctionnement du BPCS. Les deux systèmes peuvent être intégrés ou dissociés.

- les systèmes associés de niveau trois ou inférieurs du modèle de Purdue, comme par exemple des optimiseurs en temps réel, des équipements spécifiques de surveillance, des visualisations graphiques, des historiens, des MES *(Manufacturing Execution System)*, ou des systèmes de gestion de l'énergie.
- les interfaces homme-machine, les réseaux et les logiciels des équipements utilisés pour le contrôle de la production.

D'autre part l'IACS a une composante organisationnelle englobant toutes les gouvernances mises en œuvre par l'entité responsable pour l'exploitation du site de production. Celles-ci englobent en particulier :

- les directives qui spécifient ou régulent la façon de protéger les ressources système sensibles ou critiques. Elles doivent être obligatoires et pouvoir être auditées ;
- les chaînes de responsabilité internes et les procédures d'escalade ;
- les procédures qui définissent en détail les étapes à respecter pour chaque mesure de sécurité ;
- les mesures de formation du personnel pour la mise en place et le maintien du niveau de compétences requis.

Pour cerner le champ d'application de l'IEC 62443 on peut définir l'activité associée à l'utilisation des systèmes concernés par la norme :

- une exploitation prévisible de la production ;
- la sûreté du personnel et de la production ;
- la fiabilité et la disponibilité de la production ;
- l'efficacité de la production ;
- la qualité de la production ;
- la protection de l'environnement ;
- la conformité à la réglementation.

Une autre approche se base sur les équipements mis en œuvre qui doivent réaliser au moins un des critères suivants pour entrer dans le périmètre de l'IEC 62443 :

- l'équipement a une valeur économique pour un processus de production ;
- l'équipement accomplit une fonction nécessaire au processus de production ;
- l'équipement représente une propriété intellectuelle pour le processus de production ;
- l'équipement est nécessaire pour la protection du personnel, des sous-traitants et des visiteurs impliqués dans le processus de production ;

- l'équipement est nécessaire pour la protection de l'environnement et du public des effets du processus de production ;
- l'équipement est une obligation légale en particulier pour des raisons de sécurité du processus de production ;
- l'équipement est nécessaire pour la reconstruction en cas de catastrophe ;
- l'équipement est nécessaire pour l'enregistrement d'événements de sécurité.

Pour la compréhension de l'IEC 62443 il est important de définir les trois rôles de base qui sont impliqués dans la protection des installations contre les attaques informatiques : le fournisseur PS *(Product Supplier)*, l'intégrateur SI *(System Integrator)* et l'exploitant AO *(Asset Owner)*. Le PS est responsable du développement, de la commercialisation et de la maintenance des équipements utilisés dans la solution d'automatisation. Le SI est responsable de la conception et de la mise en œuvre de la solution d'automatisation. L'AO est responsable de l'exploitation, de la maintenance et éventuellement du démantèlement de solution d'automatisation.

La dénomination *Asset Owner* utilisée dans l'IEC 62443 veut dire littéralement « propriétaire », on a admis que très souvent le propriétaire est également chargé de l'exploitation. Nous avons ici choisi d'utiliser le terme « exploitant » et de garder l'abréviation AO correspondant au terme original. Il faut souligner qu'il s'agit ici de rôles. On a choisi dans l'IEC 62443 de nommer ces rôles par l'entité qui remplit le plus souvent les activités correspondant au rôle. Chaque situation est particulière et bien souvent le rôle est rempli par une entité différente. Par exemple le propriétaire peut déléguer la responsabilité de l'exploitation et / ou de la maintenance à des prestataires extérieurs. Il se peut également que le propriétaire de l'installation ait des services qui conçoivent et mettent en œuvre les solutions d'automatisation, activités correspondant au rôle SI.

Responsabilité	Rôle
Développement, commercialisation et maintenance des équipements utilisés dans l'IACS	Fournisseur, PS
Conception et mise œuvre de la solution d'automatisation	Intégrateur, SI
Exploitation, maintenance et démantèlement de la solution d'automatisation	Exploitant, AO

Tab. 1 – *Rôles et responsabilités des acteurs de l' IACS.*

Il est à noter que les équipements utilisés sont généralement développés indépendamment d'une application particulière. Les activités du SI et de l'AO sont définies dans le cadre d'un projet d'automatisation avec les contraintes et l'environnement spécifique de l'application.

Pour prendre l'exemple des automates programmables, ceux-ci sont intégrés dans un grand nombre de solutions qui peuvent être très différentes, allant de l'automatisation d'une machine-outil à des systèmes très complexes comme on en trouve dans l'industrie pétrolière.

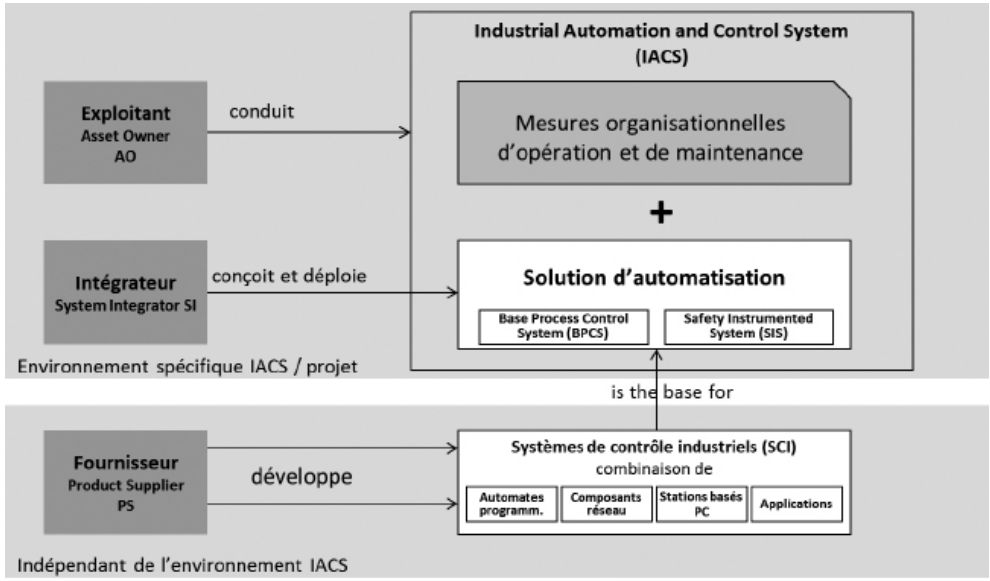

Fig. 1 –*Champ d' application de l' IEC 62443*

2. Structure de l'IEC 62443

La norme IEC 62443 se répartit en quatre parties, chacune d'entre elles regroupant plusieurs documents. La partie 1 regroupe les documents destinés aux concepts généraux, à la terminologie et aux méthodes. Il est également prévu de décrire des métriques de conformité, bien que ce sujet ne soit pas encore résolu.

La partie 2 spécifie uniquement des mesures organisationnelles. Elle s'adresse principalement aux entités responsables de l'exploitation et de la maintenance de solutions d'automatisation (rôle AO) et de l'intégration d'équipements dans des solutions d'automatisation (rôle SI). La partie 2 contient également des recommandations dans le cadre des corrections et mises à jour (*patch management*).

La partie 3 a un contenu beaucoup plus technique. D'une part elle s'adresse aux fournisseurs de systèmes de contrôles industriels (rôle PS) avec des exigences fonctionnelles pour les systèmes. Celles-ci sont étagées en fonction de leur sévérité en quatre niveaux de sécurité *(Security Level, SL)*. Une discussion du concept des SL fait l'objet de la Section 1.3.4. Un document de la partie 3 décrit la méthode et les moyens pour structurer l'architecture de la solution en zones et canaux de communication (*conduits*). Cette segmentation est une mesure importante pour la protection contre les attaques informatiques et pour contrecarrer leur propagation à l'intérieur de la solution. Elle doit se faire en étroite collaboration entre l'exploitant (AO) et l'intégrateur (SI). Il s'agit de définir des niveaux de sécurité cible *(Target SL)* pour chaque zone et chaque canal de communication, voir Section 1.3.4. Enfin la partie 3 contient un rapport technique qui donne un résumé de l'état de l'art des techniques de protection contre les attaques informatiques.

La partie 4 est spécifiquement destinée aux équipements faisant partie de systèmes de contrôle industriels, comme les automates programmables, les stations opérateur ou d'ingénierie, les composants réseau tels que firewalls ou passerelles et les logiciels applicatifs. D'une part on distingue les exigences fonctionnelles, dérivées des exigences fonctionnelles pour les systèmes spécifiées dans la partie 3, d'autre part un document est consacré aux exigences pour le processus de développement des produits. Ce document a pour objet des minimiser les risques de créer des vulnérabilités pendant la conception et le développement, par exemple par une architecture faible ou des faiblesses de codage du logiciel.

Il est à noter qu'au moment où nous écrivons cet ouvrage[1] la norme IEC 62443 n'a pas encore été adoptée dans son ensemble. En particulier le concept de niveau de sécurité qui fait l'objet d'une discussion dans la Section suivante devra être affiné et complété pour tenir compte des aspects qui ne sont pas encore intégrés actuellement. Nous considérons cependant que la norme peut d'ores et déjà être appliquée, car le contenu des documents les plus importants pour la protection des installations industrielles est déjà suffisamment stable :

- ISO/IEC 63443-3-3, *System Security Requirements and Security Levels*. Spécifie les exigences fonctionnelles pour les systèmes de contrôle industriels (rôle PS). Le document a été adopté en 2013 ;
- IEC 62443-2-4, *Requirements for IACS solution suppliers*. Spécifie les mesures organisationnelles de l'intégrateur (rôle SI) et de la maintenance (rôle AO). L'adoption de ce document est attendue fin 2014 ;
- IEC 62443-2-1, *Requirements for an IACS security management system*. Spécifie les mesures organisationnelles de l'exploitant (rôle AO). Le document actuel est un profil de la norme ISO/IEC 27001/27002 qui est largement appliquée pour les systèmes d'information de gestion. L'adoption est attendue en 2015, il n'y a pas de grandes modifications du contenu actuel à attendre.

3. Concepts de l'IEC 62443

La norme IEC 62443 repose sur quelques concepts fondamentaux. Ceux-ci sont en partie adressés dans le document IEC 62443-1-1. On trouvera ci-après une discussion de ces concepts.

1. Avril 2014.

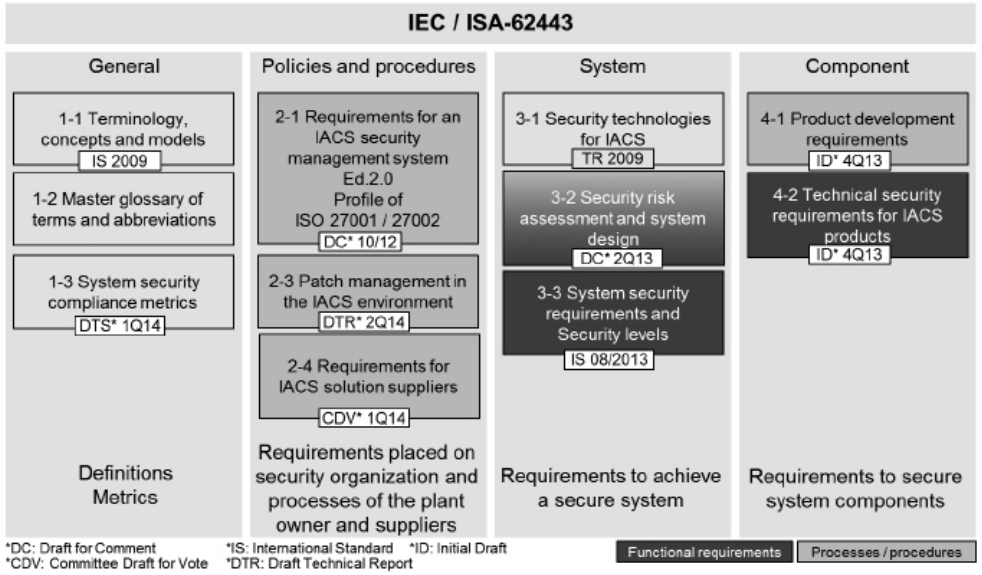

Fig. 2 – *Structure de l' IEC 62443*

3.1 Défense en profondeur

Une notion importante dans la protection des installations industrielles contre les attaques informatiques est basée sur le fait qu'elle requiert la participation de tous les acteurs : l'exploitant, l'intégrateur et le fournisseur. En général une seule mesure ne sera pas suffisante pour atteindre un certain niveau de protection. Il est nécessaire de mettre en œuvre plusieurs mesures coordonnées qui représenteront autant de barrières, de lignes de défense contre l'attaquant. Cette stratégie, appelée défense en profondeur *(Defense in Depth)* a été appliquée dans le domaine militaire depuis très longtemps. On la retrouve par exemple dans la conception des châteaux forts avec comme ultime rempart la porte renforcée de la chambre du seigneur tout en haut du donjon. La norme IEC 62443 adresse tous les aspects d'une stratégie de défense en profondeur.

Les premières lignes de défense se trouvent chez l'exploitant. On constitue déjà une première barrière en sensibilisant les personnels aux menaces des attaques informatiques, en mettant en place un plan de formation et en définissant clairement les processus et l'organisation de la sécurité. D'autres mesures sont par exemple le cloisonnement et le contrôle d'accès aux locaux, la vérification de la fiabilité du personnel, la définition des droits et devoirs des utilisateurs ou la mise en place d'un plan de continuité de l'activité en cas d'attaque.

D'autres couches de la défense en profondeurs sont à trouver dans le déploiement de la solution d'automatisation, par exemple par la segmentation de l'architecture du réseau en zones avec des protections par firewall, la protection de l'accès avec des mots de passe ou la réduction des actions possibles de chaque utilisateur au minimum

nécessaire à sa fonction. Ces mesures sont mises en général en place par l'intégrateur sur la base des capacités fonctionnelles des systèmes et composants utilisés.

Les couches intérieures de défense sont réalisées par les fonctionnalités de sécurité des produits offerts par les fournisseurs. Ce sont par exemple des protections contre des logiciels malveillants par des anti-virus ou des listes blanches *(White Listing)*, la protection des logiciels contre les modifications en utilisant de la cryptographie ou du hachage, la signature des logiciels téléchargés ou la mise en œuvre de retards pour contrecarrer les attaques d'estimation de mot de passe.

D'autres contributions sont apportées par les processus de mise en œuvre et de maintenance de la solution, comme par exemple l'effacement ciblé de tous les comptes provisoires, la modification des mots de passe de tous les comptes système ou par défauts ou l'actualisation systématique de toutes les protections contre les logiciels malveillants. Par ailleurs les fournisseurs peuvent réduire le nombre de vulnérabilités dans les produits en mettant en place un processus de développement rigoureux tenant compte des impératifs de la sécurité.

La cybersécurité doit protéger les installations pendant leur phase d'exploitation. Pour cela tous les acteurs doivent apporter leur contribution. Les systèmes et composants doivent proposer des fonctionnalités de sécurité apportant une sécurité intégrée et permettant la mise en œuvre de solutions sécurisées. L'intégrateur doit concevoir des solutions d'automatisation mettant en jeu les fonctionnalités des produits pour entraver le plus possible l'attaquant éventuel. L'exploitant doit veiller à ce que l'installation soit exploitée de la manière la plus sûre possible et que les protections mises en œuvre restent au niveau requis durant toute la durée de vie de l'installation.

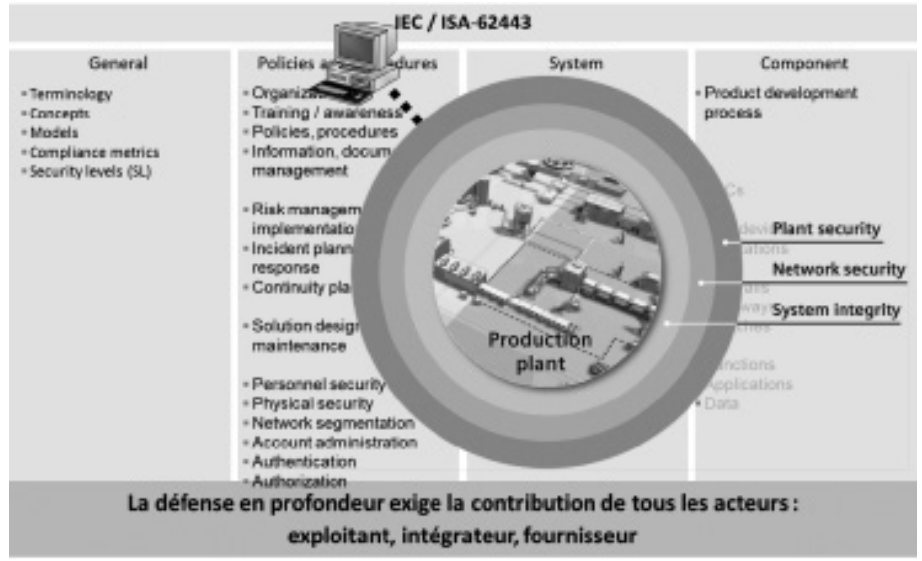

Fig. 3 – *Défense en profondeur*

3.2 Évaluation du risque

Toutes les mesures de la cybersécurité sont basées sur l'évaluation des conséquences des menaces sur les biens qui dépendent de la responsabilité de l'entité. Pour le fournisseur ce sera les produits qu'il commercialise, pour l'intégrateur ce sera la solution dont il a la charge et pour l'exploitant ce sera l'installation qu'il exploite.

L'évaluation est souvent décrite comme un cycle : planifier / évaluer les risques et les contre-mesures, les réaliser, vérifier leur efficacité, les mettre en œuvre et reprendre depuis le départ. Ce modèle est souvent intitulé *Plan-Do-Check-Act* ou PDCA. Dans l'IEC 62443 la notion d'évaluation de risque est la base de tous les documents. L'IEC 62443 reprend le modèle décrit dans la directive VDI/VDE 2182 dont nous allons détailler plus avant les actions et les résultats des différentes étapes.

La documentation de cette activité et des mesures de protection qui en découlent devra couvrir les aspects techniques ainsi que la documentation des processus.

La documentation technique devra comprendre la description de toutes les informations nécessaires à l'intégration d'un composant de sécurité dans la solution d'automatisation. Elle inclut l'utilisation typique, le matériel, les logiciels système, les services de communication, les logiciels d'application, les aspects de durée de vie et les directives des mises en œuvre.

La documentation des processus couvrira toute la documentation des étapes du processus entre autres la description des résultats, de la méthode, la justification des évaluations, les moyens utilisés ainsi que les participants.

Le modèle prend comme point de départ pour le traitement des différentes étapes un bien donné (produit, solution d'automatisation, installation) et la mise en œuvre de ses fonctionnalités dans un environnement donné. Si l'on constate lors d'une des étapes qu'il y a des risques particulièrement élevés ou que la sécurisation aboutit à des coûts injustifiés, on réévaluera les exigences fonctionnelles. Un changement des exigences conduira à un nouveau passage par le cycle.

On démarrera par une analyse structurelle de l'objet à considérer, avec la spécification exacte de ses fonctionnalités, interfaces et flux de données. On décrira également son utilisation et l'infrastructure réseau dans laquelle il est intégré. Pour les produits d'automatisation, on décrira une utilisation typique. L'environnement sera décrit par les grandeurs caractéristiques qui influencent directement ou indirectement l'objet considéré comme par exemple la topographie (locaux, climat).

Étape 1 : Identifier les biens

- Information d'entrée : résultats de l'analyse structurelle.
- Action : à partir de l'analyse structurelle, on définira et on articulera les biens. Il est recommandé de structurer l'objet considéré sur la base des matériels et équipements : composants d'automatisation, infrastructure réseau.
- Résultat : liste des biens.

Étape 2 : Analyser et évaluer les menaces

- Information d'entrée : liste des biens.
- Action : le but de cette étape est la description des menaces pertinentes pour chaque bien de l'objet à considérer. On pourra considérer différents scénarios suivant l'état dans lequel se trouve l'objet à considérer. Dans un premier temps on fera une énumération des menaces découlant de l'organisation, des fonctionnalités techniques ou de l'utilisation. Dans une deuxième phase, on établira une matrice des menaces décrivant pour chaque bien les menaces auxquelles il est confronté ainsi que l'origine et les conséquences immédiates des menaces sur l'objet à considérer.
- Résultat : matrice des menaces.

Étape 3 : Définir les objectifs de protection appropriés

- Information d'entrée : matrice des menaces.
- Action : dans cette étape on décidera pour chacun des biens quels objectifs de protections sont appropriés. La pertinence d'un objectif résulte de la teneur des informations et de la fonction concrète du bien dans le cadre de la solution d'automation ou de l'installation. Les objectifs de protection s'orienteront en général vers les objectifs de protection de l'exploitant pour une opération sans trouble de l'installation. Pour un produit d'automatisation utilisé dans beaucoup d'applications différentes on considérera l'utilisation typique du produit. On pourra aussi définir des objectifs de protection de la propriété intellectuelle du fournisseur ou de l'intégrateur comme par exemple des logiciels ou des données. Le résultat de cette étape sera l'extension de la matrice avec les objectifs de protection.
- Résultat : matrice des menaces avec les objectifs de protection appropriés

Étape 4 : Analyser et évaluer les risques

- Information d'entrée : table des menaces avec les objectifs de protection appropriés
- Action : lors de cette étape on évaluera les probabilités de l'occurrence des menaces potentielles ainsi que l'importance des dégâts causés en cas d'occurrence. Pour la cybersécurité l'évaluation est en général qualitative, par exemple faible / moyenne / forte. Le risque (probabilité-conséquence) tiendra compte de toutes les mesures de protection déjà mises en place et sera analysé par rapport à un risque acceptable. On définira si une mesure compensatoire pour réduire le risque est nécessaire ou non.
- Résultat : table des risques évalués pour les menaces pertinentes

Étape 5 : Définir les mesures de protection et évaluer leur efficacité

- Information d'entrée : table des risques évalués pour les menaces pertinentes
- Action : lors de cette étape, on décrira les mesures de protection et leur mise en œuvre contre les différentes menaces. Les mesures peuvent être d'ordre technique, organisationnel ou être une combinaison des deux. Elles se baseront sur la réduction de risques que l'on aura jugée nécessaire lors de l'étape précédente. On pourra s'appuyer sur des catalogues, des expériences et différentes sources de documents. Une solution globale sera ainsi définie par la sélection des mesures. L'efficacité de l'ensemble des mesures est souvent donnée par la combinaison des mesures. Il peut être judicieux d'adresser une menace donnée par plusieurs mesures et de considérer plusieurs alternatives de solutions globales. L'évaluation de l'efficacité des mesures se fera sur le même schéma que l'analyse des risques en général de façon qualitative, par exemple faible / moyenne / grande. On fera également une évaluation économique des solutions globales possibles à partir du coût de chaque mesure.
- Résultat : liste des mesures de protection avec leur efficacité et leur coût

Étape 6 : Sélectionner les mesures de protection

- Information d'entrée : liste des mesures de protection avec leur efficacité et leur coût
- Action : le but de cette étape est de sélectionner la combinaison de mesures de protection la plus appropriée, c'est-à-dire qui répond le mieux aux buts et à la politique de sécurité de l'entité responsable. On considérera les aspects économiques, les objectifs stratégiques et les possibilités de mise en œuvre. Il faudra intégrer le coût total de la mise en œuvre des mesures durant toute la durée de vie de l'installation. Les objectifs stratégiques incluent entre autres les budgets, responsabilités opérationnelles et la gestion de la continuité de l'activité. Les possibilités de mise en œuvre devront tenir compte par exemple des infrastructures, des concepts déjà validés *(best practices)*, de l'organisation ou des rôles et responsabilités.
- Résultat : sélection des mesures de protection

Étape 7 : Mettre en œuvre les mesures de protection

- Information d'entrée : liste des mesures de protection à mettre en œuvre
- Action : les mesures sélectionnées devront être mises en œuvre dans le contexte global de l'installation. Un concept opérationnel devra garantir la pérennité de la mise en œuvre. Il est conseillé de mettre en place une surveillance proactive.
- Résultat : Mesures de protection mises en œuvre

Étape 8 : Faire des audits du processus

- Information d'entrée : documentation des activités et des mesures de protection
- Action : l'audit doit couvrir toutes les étapes précédentes et répondre aux questions suivantes : toutes les étapes sont-elles été réalisées ? Les résultats

de chaque étape sont-ils évalués ? L'évaluation est-elle fondée ? Tous les résultats sont-ils documentés ? On documentera tous les résultats de l'audit et on définira la pertinence et le délai d'un nouvel audit. En particulier on documentera toutes les insuffisances et déviations et surveillera leurs remédiations. En plus de l'audit du processus on intégrera la surveillance de l'efficacité des mesures de protection dans la gestion de la qualité.

- Résultat : Rapport d'audit

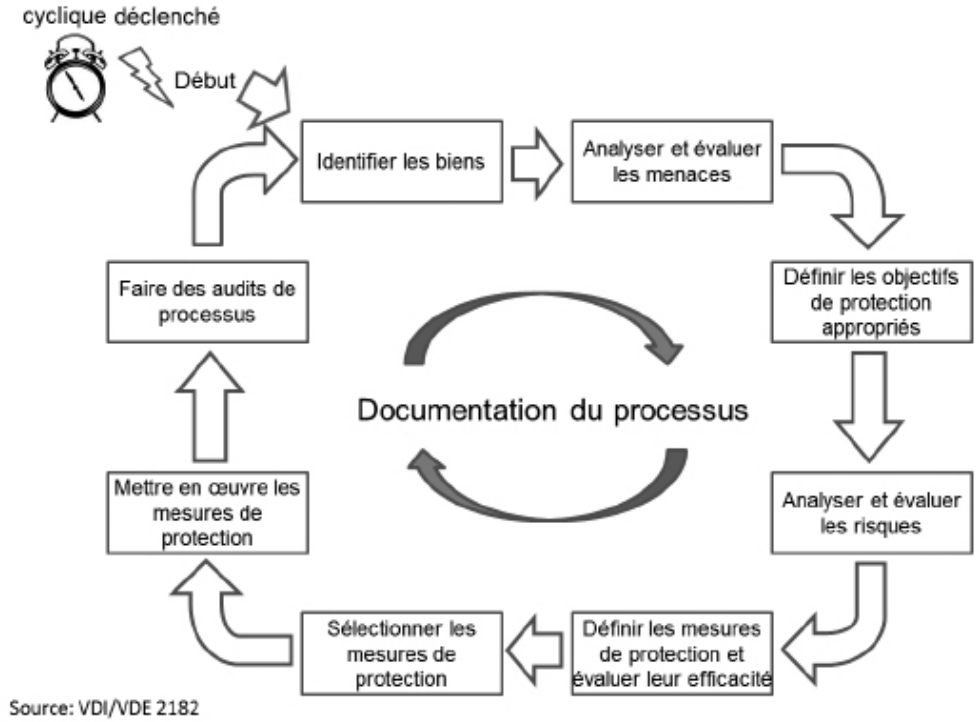

FIG. 4 – *Analyse de risque, cycle Plan-Do-Check-Act*

Les cycles PDCA conduits par les différents acteurs ne peuvent pas être considérés comme étant indépendants, les informations d'entrée ainsi que les informations qui en résultent des activités interfèrent.

Le fournisseur (rôle PS, *Product Supplier*) intègre les exigences des marchés cibles dans la définition des fonctionnalités et des caractéristiques de sécurité des produits. Ceux-ci peuvent être considérés comme une synthèse des exigences de nombreux projets d'intégration et d'exigences d'utilisateurs finaux. Les informations qui en résultent des activités des fournisseurs sont intégrées dans les cycles suivants. Elles doivent inclure toutes les informations nécessaires à l'évaluation de l'utilisation des produits dans une solution d'automatisation. Ce sont la documentation technique des capacités fonctionnelles des produits, mais également des directives pour leur intégration et utilisation