

IEC 62443 : vers une définition holistique des niveaux de sécurité

La philosophie de la norme IEC 62443 (ISA99) relative à la cybersécurité des installations industrielles, repose sur deux approches complémentaires :

- d'une part, une analyse des mesures de nature organisationnelle (les « policies and procedures »), à mener selon les principes des normes ISO 27001 et 27002, adaptées et retranscrites dans le cadre du standard IEC 62443-2-1 (révision en cours de finalisation) et complétées par l'IEC 62443-2-4 dans le cas des intégrateurs et fournisseurs de service ;
- d'autre part, des règles techniques, définies dans le standard IEC 62443-3-3 (norme publiée) permettant de définir de façon objective, grâce à une centaine de critères, les niveaux de sécurité (SL allant de 0 à 4) que l'on peut accorder à une installation donnée au regard de chaque exigence essentielle définie par la norme (FR 1 à FR7).

Le standard IEC 62443-3-3 applicable aux systèmes, et son extension l'IEC 62443-4-2 applicable aux composants de ces systèmes, constituent une avancée majeure dans le domaine de l'évaluation de la cybersécurité des installations industrielles car ils prennent en considération les spécificités du monde industriel et proposent une approche technique rationnelle pour mener les évaluations.

Cependant, aux côtés de l'approche technique, l'approche organisationnelle héritée de l'ISO 27000, reste qualitative. Ceci fait que, si les cotations SL0, SL1...SL4 que l'on peut accorder à un système prennent bien en compte les qualités intrinsèques du système (c'est-à-dire sa « capability »), elles n'intègrent pas toutes les données particulières à son exploitation dans un environnement donné.

Afin de remédier à cette situation, un nouveau groupe de travail, animé par Pierre Kobes (Siemens) et Lee Neill (Wurldtech), l'ISA99-WG3-TG3, a été constitué. Son objectif est de mettre au point une approche holistique afin de parvenir à une notion de « niveau de protection » intégrant l'ensemble des aspects à prendre en considération.

Pour ce faire, la notion de niveau de protection s'appuierait sur le concept de « niveau de maturité (Maturity level) » introduit dans l'IEC 62443-1-1 (Revision) et précisé dans l'IEC 62443-4-2. Ce concept est dérivé de celui de maturité logicielle (Maturity Level ou CMMI) introduit il y a une trentaine d'années par le Carnegie Mellon Institute dans le domaine du développement des logiciels et communément utilisé dans l'industrie. Dans le cas de la cybersécurité, il s'agirait de caractériser la maîtrise des intervenants dans la mise en œuvre des différentes pratiques permettant de construire la cybersécurité (figure 1).

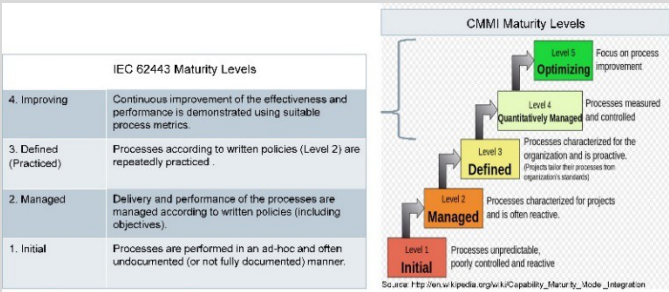


Figure : Maturity levels et CMMI – Source : ISA

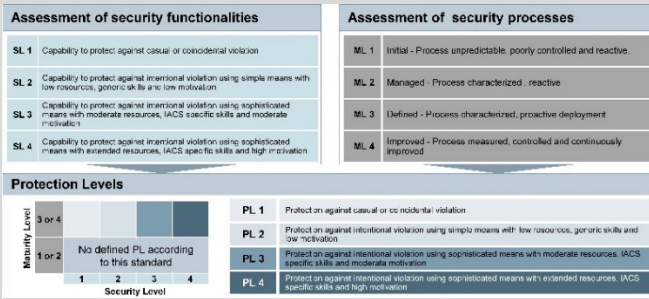


Figure : Combinaison des Security levels et des Maturity levels pour définir les Protection levels – Source : ISA.

Partant de là, disposant des Security levels (SLs) afférant à un système et du Maturity levels (ML) afférant à l'organisation qui en est responsable, il semble possible de combiner les deux afin de définir un niveau de protection (PL ou Protection level) d'une installation.

Ceci est l'idée générale et elle nous semble intéressante. Mais le groupe démarre tout juste ses travaux et il y a

encore du chemin afin que cette approche ne devienne un standard, approuvé et documenté.

Jean-Pierre Hauet – jean-pierre@hauet.com