Sûreté et cybersécurité : comment concilier deux objectifs essentiels de la sécurité industrielle

Villeurbanne, mardi et mercredi 18 et 19 octobre 2016

Prise en compte des cyberattaques dans les méthodes d'analyse de risque classiques

Jean-Marie Flaus, Eric Zamai*Chargé d'affaires - Network Engineering & Cybersecurity - Schneider Electric*

Tel : +33 (0)4 76 82 62 29

G-SCOP, 46, avenue Félix Viallet - 38031 Grenoble Cedex 1 – France

Email: jean-marie.flaus@grenoble-inp.fr , eric.zamai@grenoble-inp.fr

Mots clés : ***analyse de risque, étude de danger, détection intrusion, arbre de défaillance, LOPA, Bowtie, EBIOS***

La cybersécurité des systèmes industriels est une problématique de plus en plus importante actuellement. Les installations sont de plus en plus interconnectées et les sources de menace sont chaque jour plus nombreuses. En France, dans le cadre de la loi de programmation militaire, des dispositions légales et réglementaires demandent une gestion explicite du risque généré par la cybermenace. Il en est de même au niveau européen.

Les conséquences potentielles de ce risque incluent une destruction des installations, la mise en danger des populations, des pertes de productivité et des baisses de qualité voir des non-conformités des produits.

Ces conséquences sont les mêmes que celles recensées dans les analyses de risques et les études de danger menées habituellement. Cependant, dans ces études la malveillance est volontairement exclue.

Les méthodes d'analyse du risque engendré par les attaques informatiques des systèmes industriels sont le plus souvent basées sur les approches de gestion de la sécurité informatique. Elles s'appuient sur les normes de la famille ISO 27000 ou ISA99 ou sur les concepts de défense en profondeur et sont mises en œuvre de façon indépendante des analyses de risques « classiques ».

L'objectif de cette communication est de passer en revue les méthodes d'analyse de risque utilisées dans les études de danger (APR, AMDEC, Arbre de défaillance, Bowtie, LOPA) et de montrer les points communs et les différences avec les méthodes d'analyse de sécurité informatique (EBIOS, arbre d'attaques, arbres de défense, défense en profondeur) et d'analyser comment elles se situent les unes par rapport aux autres.

Nous montrons ensuite comment combiner certaines de ces méthodes pour prendre en compte le cyber-risque dans les études de danger et comment exploiter le modèle du risque obtenu comme support pour la détection d'intrusion et en particulier distinguer les pannes dues au vieillissement ou aux erreurs humaines des cyber attaques.

Un petit exemple d'installation industrielle permettra d'illustrer l'ensemble.

Références

- Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS), ANSSI, 2010.
- Maîtriser la SSI pour les systèmes industriels, ANSSI, 2012

- ISA99/IEC 62443: a solution to cyber-security issues?, Jean-Pierre Hauet, ISA Automation Conference – Doha (Qatar) - 9 & 10 December 2012
- Analyse des risques des systèmes de production industriels et de services : Aspects technologiques et humains, Jean-Marie Flaus, Lavoisier, 2013.