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

Villeurbanne, mardi et mercredi 18 et 19 octobre 2016

Comment la sûreté de fonctionnement informatique peut-elle concilier Sécurité-Security et Sécurité-Safety ?

Dr. Gilles TROUESSIN
Auditeur/Consultant/Expert/Formateur en sécurités des systèmes d'information
Tel : +33 (0) 6 63 10 50 76
10 allée des Demoiselles – 31400 TOULOUSE
Email: gilles.trouessin@orange.fr

Mots clés : *Sûreté de fonctionnement (ou dependability) ; sécurité-immunité (ou security) ; sûreté-innocuité (ou safety) ;*

Depuis plus de trente ans, dans la communauté académique de la recherche (fondamentale et appliquée) en sciences de l'information et, plus récemment, dans des secteurs de l'industrie particulièrement exigeants vis-à-vis de la résilience (aéronautique et espace, transports automatisés, nucléaire et production d'énergie, (télé-) communications, santé et hospitalier, etc.). **la Sûreté de fonctionnement (SdF) d'un système informatique est définie comme « cette propriété générique d'un système informatique qui permet aux utilisateurs de ce système de placer une confiance justifiée dans le service que celui-ci délivre à ceux-ci » [Laprie1988][1].**

Originellement issue de la fiabilité du matériel et de la tolérance aux fautes, la Sûreté de fonctionnement (ou Dependability) se caractérise, d'abord, à travers ses **attributs perceptifs**, puis ses **moyens pour la sûreté de fonctionnement** et, enfin, **ses entraves à la sûreté de fonctionnement**.

Ses attributs perceptifs sont : la **fiabilité** (ou reliability), la **sûreté-innocuité** (ou safety) [parfois appelée, à tort, **sécurité** ou **sûreté**], la **maintenabilité** (ou maintainability), la **disponibilité** (ou Availability), **l'intégrité** (ou Integrity) et la **confidentialité** (ou Confidentiality) ; ces trois dernières [D+I+C] constituant la Sécurité (ou Security), ou **sécurité-immunité** [allusion aux virus informatiques], ou **sécurité informatique** [de façon un peu restrictive], ou encore **sécurité du Système d'Information** [de façon plus moderne].

Ses entraves sont rassemblées à travers la chaîne fondamentale « **faute – erreur – défaillance – faute – …** », chacune pouvant être la cause originelle de la suivante, et ce de façon potentiellement récursive.

Ses moyens couvrent tout le spectre des fautes et erreurs possibles : **prévention** et/ou **élimination de fautes** (**l'évitement de fautes), tolérance** et/ou **prévision de fautes (l'acceptation de fautes), traitement d'erreur,** etc.

L'objectif de cette proposition d'intervention est de revisiter les principaux concepts de base issus de la culture historique de la sûreté de fonctionnement informatique pour contribuer à aider à concilier **sécurité-immunité** [appelée ici **cybersécurité**] et **sûreté-innocuité** (appelé ici, Sûreté), à travers une approche plus globale, de type « **security for safety** », capable de prendre en compte, à la fois, les fautes intentionnelles (ou intrusions), les **fautes accidentelles** (ou incidents), mais aussi les **actions délibérées** (avec ou sans intention malveillante).

---

[1] [Laprie1988] J.C.Laprie, 1988, Sûreté de fonctionnement et tolérance aux fautes - Concepts de base. Rapport LAAS n°88.287, Toulouse.