Place d'ADELI

Sécurité(s) et Sûreté(s)

…participent à la qualité des données/programmes/systèmes,
…participent de la qualité de tout le cycle de vie du logiciel.

Dès lors qu'il est question de sécurité de systèmes informatisés :
*Entend-on simplement **qualité des informations** au sens disponibilité, intégrité et confidentialité des données manipulées ? C'est-à-dire : s'agit-il de sécurité-« **security** » ?*
*Entend-on uniquement **qualité des systèmes** dits « critiques » au sens innocuité des systèmes informatiques « hautement critiques » ? C'est-à-dire : s'agit-il de sécurité-« **safety** » ?*
*Entend-on globalement **qualité du service** fourni à l'utilisateur, au sens fiabilité, innocuité, … des matériels, logiciels ? C'est-à-dire : s'agit-t-il de sûreté de fonctionnement-« **dependability** » ?*

Sécurité & Sécurités : collision de termes… mais collusions de solutions…

Longtemps appelée sécurité informatique, dans les années 80, puis sécurité des systèmes d'information, depuis les années 90, cette sécurité peut être subdivisée en trois volets majeurs :

- la *sécurité juridique*, préalable indispensable ;
- la *sécurité procédurale*, complément incontournable ;
- la *sécurité technique*, souvent simple partie émergée de l'iceberg sécurité.

Une ***politique*** de sécurité efficace combine divers aspects de la sécurité technique :

- authentification ;
- autorisation ;
- contrôle d'accès ;
- gestion des privilèges ;
- gestion des informations sensibles…

Sécurité juridique

Le premier volet de la sécurité (premier par la chronologie, l'importance et la complexité, mais, malheureusement, également, souvent le premier à être omis par négligence ou par faiblesse intellectuelle) aborde les aspects juridiques, au sens strict ou dans une acception plus large.

Les aspects juridiques de la sécurité ou *sécurité juridique*, concernent les contraintes légales et les textes réglementaires. Citons pour mémoire quelques exemples : la loi informatique et libertés, la loi « télécommunications » et ses décrets d'application et arrêtés relatifs aux régimes cryptographiques, les lois sur la bioéthique, le code de déontologie du médecin, la loi sur la signature électronique et ses futurs décrets d'application sur les prestataires de services de certification etc.

Préalable indispensable à toute démarche d'expertise en sécurité qui se voudrait effective et efficace, la sécurité juridique permet d'exprimer les obligations et les responsabilités de chaque acteur du système ; elle exprime, aussi et surtout, leurs permissions, leurs interdictions et leurs limites d'action.

Les aspects éthiques et déontologiques abordent, s'il le faut, la composante juridique dans un cadre plus large et plus citoyen, dans des sphères liées à des corporations ou régies par des codes de déontologie, de bon usage ou de bonne pratique.

Il s'agit de la sphère santé : médecine, pharmacie et autres professions, constituées autour d'un conseil de l'ordre, départemental, régional et/ou national, ou d'autres sphères d'activités tout aussi sensibles, comme les notaires, les avocats, les huissiers de justice, les magistrats, etc. etc.

Extensions inévitables de la stricte sécurité juridique, les sécurités éthique et déontologique prennent en compte les dimensions, sociétale et citoyenne, spécifiques et originales, de certains métiers et champs d'activités.

Sécurité procédurale

Deuxième des trois wagons du petit train de la sécurité des systèmes d'information, la *sécurité procédurale* sert de tampon[1] entre les commandes juridiques et les livraisons techniques. En d'autres termes, les aspects organisationnels et procéduraux servent ainsi de courroie de transmission[2] entre les obligations et interdictions légitimes et les réalisations informatiques.

Une famille bien connue de mesures de sécurité recommande la séparation, spatiale, temporelle, fréquentielle… dont l'illustration pratique parfaite du point de vue procédural est la séparation des pouvoirs. Ainsi, pour respecter le célèbre dicton : « ne pas mettre tous ses œufs dans le même panier », la séparation des pouvoirs consiste à répartir les obligations et les contraintes, entre plusieurs individus distincts ; chacun d'eux étant investi de responsabilités exclusives et/ou complémentaires. Cette solution est préférée à la centralisation des obligations et des contraintes sur un seul individu, toujours faillible.

Citons, pour mémoire, les procédures les plus connues, celles qui sont applicables lors de périodes douloureuses de la vie d'un système informatique: secours à mettre en œuvre lors de sinistres sérieux, reprise sur incidents, etc. Pour des raisons d'efficacité, chaque acteur doit parfaitement connaître les tâches qui lui incombent.

En amont de la mise en œuvre de techniques classiques de sécurité, des protocoles de sécurisation, opérationnels, organisent les rôles, les fonctions et les responsabilités des acteurs. De cette façon, toute décision-action importante sera prise après confirmation, par une combinaison de tâches dont la bonne exécution sera rigoureusement contrôlée.

Sécurité technique

Cette sécurité, trop souvent considérée comme locomotive[3], est brandie par ceux qui veulent se convaincre de sécuriser leurs applications, leurs transactions, leurs transferts, leurs fichiers, leurs systèmes, etc. La *sécurité technique* est la plus ample en variété et en histoire, la plus connue des trois voitures de la sécurité ; il y a, peut-être, ce côté James Bond sommeillant en chacun de nous qui se réveille au quart de tour dès que l'on entend « carte à puce », « mot de passe », « code secret », « contrôle d'accès », « cryptographie », « clé de chiffrement », « clé de brouillage » etc.

Sans nous répandre, ici, en détails, qui déborderaient d'une année entière de Lettres d'ADELI, mais simplement pour nous mettre en appétit, introduisons rapidement et grossièrement[4] les branches essentielles qui constituent une bonne, car préventive, politique de sécurité :

- *authentification :* pour corroborer une identité proclamée ;
- *autorisation :* pour définir *qui ?* a le droit d'accéder *comment ?* et *à quoi ?* ;

---

[1] *Quoi de plus normal pour des wagons…*

[2] *Bis : quoi de plus normal… pour de la mécanique…*

[3] *Décidément on ne quitte plus le monde ferroviaire…*

[4] *i.e., à partir de définitions illustratives simplistes mais explicites, en attendant des définitions officielles plus précises.*

- *gestion des droits d'accès :* pour faire évoluer les droits d'accès dans le temps et dans l'espace en fonction d'événements prévus dans les diverses politiques ;
- *gestion des privilèges et de dévolution des droits :* pour déléguer des droits de base (droits d'accès) et pour définir et faire évoluer les droits élevés (privilèges) à attribuer ;
- *gestion des informations sensibles et critiques :* pour générer, protéger, archiver, utiliser, diffuser… des informations vitales pour la survie du système.

Un trio sécurité

Voici donc le trio majeur de la sécurité : *responsabilité* des acteurs, *superstructure* organisationnelle, *infrastructure* opérationnelle… Un petit voyage dans chacun de nos trois wagons de sécurité nous conduit à nous poser successivement les trois séries de questions suivantes :

- *juridique :* qui est responsable de quoi et pourquoi sécuriser le système ?
- *organisationnel :* que faut-il sécuriser, où et quand ?
- *technique :* comment faire, comment faire faire pour mettre en œuvre ?

Sûreté & Sûretés : collision de termes… et collusion entre les méthodes…

Il y a collision de termes entre la *sécurité-« **security** »* et la *sécurité-« **safety** »* étant donné qu'il n'y a qu'un mot en français pour désigner :

- d'un côté, la propriété liée aux fautes intentionnelles ;
- de l'autre, celle liée aux défaillances catastrophiques pour les individus et l'environnement.

Il y a également collusion d'actions et d'incidences puisqu'une atteinte à la *sécurité-« **security** »* peut avoir des conséquences graves s'il s'agit de systèmes critiques, conséquence sur la *sécurité-« **safety** »*, s'il s'agit de données ou décisions vitales (mal-)intentionnellement détournées.

Inversement : collision de termes entre la très spécifique *sécurité-« **safety** »* (parfois hâtivement appelée *sûreté* au lieu d'*innocuité*) et la très générique *sûreté de fonctionnement-« **dependability** »* (parfois tout aussi hâtivement appelée *sûreté* ou même *fiabilité*) qui regroupe les attributs perceptifs de la propriété qui consiste à *« placer une confiance justifiée dans le service délivré à l'utilisateur par le système »*.

Innocuité des systèmes critiques

Les systèmes critiques sont ceux dont la moindre perturbation non prévue, mal anticipée, non parée induit à une non-qualité de service, préjudiciable à l'utilisateur final. Les logiciels critiques et les ateliers (spécification, développement, intégration, recette, exploitation) sont d'une taille (nombre de lignes de code) et d'une complexité telles que, seules, des méthodes éprouvées ou reconnues permettent d'avoir une confiance justifiée dans le produit fini alors obtenu.

Citons comme simples exemples immédiats de systèmes critiques nécessitant cette innocuité, la famille des systèmes embarqués, dans les engins de transport habités ou terrestres, maritimes ou spatiaux (avionique, spatial, ferroviaire[5], etc.). Ajoutons comme exemples de systèmes hautement critiques, car potentiellement très dangereux, toute la famille des logiciels de «*command and control*» en milieu hostile ou pouvant le devenir (nucléaire, militaire, centrales énergétiques, etc.).

Fiabilité des systèmes cruciaux

Une autre forme de besoin en sûreté de fonctionnement, au-delà de la *sécurité-**security*** et de la *sécurité-**safety***, est la *fiabilité-**reliability***, parfois appelée continuité de service. Cette fiabilité concerne, éventuellement les systèmes cités *supra*, mais aussi et surtout des systèmes que l'on

[5] *Décidément, on n'y coupe pas…*

pourrait qualifier de cruciaux dans une entreprise ou un service de production et dont la paralysie totale, ou même seulement partielle, est directement nuisible à l'activité de l'entreprise.

Citons, pour exemple, les systèmes hautement sollicités et/ou en temps réel (autocommutateur téléphonique, gestionnaire de bases de données ou de connaissance, etc.). Citons, également, les systèmes très complexes très sollicités également mais, surtout, dont la logique interne est trop complexe pour être reproduite en semi-automatique, voire en manuel (système de réservation aérienne, de réservation ferroviaire, de gestion de parcs hôteliers et de villégiature, etc.).

Sûreté de fonctionnement informatique

La *sûreté de fonctionnement* (traduction de ***dependability*** plus élégante que *« dépendabilité »*) d'un système informatique ou informatisé est *« la propriété générique qui permet à l'utilisateur de ce système de placer une confiance justifiée dans le service qu'il leur délivre »*[6].

Il s'agit d'un concept générique qui se décompose en autant de propriétés complémentaires et interdépendantes, selon le, ou les, attribut(s) perceptif(s) pris en considération pour construire un système réputé « sûr » :

- *disponibilité :* vis-à-vis du *fait d'être prêt à l'utilisation* ;
- *intégrité : non-altération inappropriée de l'information* ;
- *confidentialité :* vis-à-vis de la *non-divulgation non autorisée de l'information* ;
- *sécurité-**security*** : *non-rétention, non-altération ou non-divulgation non autorisée d'information* ;
- *fiabilité :* vis-à-vis de la *continuité de service* ;
- *sécurité-**safety***, *innocuité* : *non-occurrence de conséquence environnementale catastrophique* ;
- ou aussi *maintenabilité :* vis-à-vis de l'*aptitude aux réparations et aux évolutions*.

La sûreté de fonctionnement intègre bien évidemment une foultitude de facteurs dont il est possible de dresser une taxinomie en passant par la chaîne récurrente des entraves à la sûreté de fonctionnement :

- la *défaillance* lorsque le service délivré dévie de l'accomplissement de la fonction du système, ou de ce à quoi il est destiné ;
- l'*erreur*, partie ou état du système susceptible d'entraîner une défaillance ;
- la *faute*, cause prouvée ou supposée d'une erreur.

Cette combinaison de facteurs concerne, par exemple pour ce qui est simplement des fautes,

- fautes physiques *versus* fautes d'origine humaine ;
- fautes accidentelles versus intentionnelles ;
- fautes intentionnelles bénignes versus nuisibles ;
- fautes de développement versus opérationnelles ;
- fautes internes versus externes ;
- fautes permanentes versus temporaires, etc.

D'autres typologies classent les erreurs selon leur latence, leur criticité, leur gravité, etc.

Elles classent les défaillances selon :

- le mode caractérisé par le domaine de défaillance (défaillance en valeur ou temporelle) ;
- la perception des défaillances par les utilisateurs (défaillance cohérente, incohérente) ;
- le comportement du système en cas de défaillances (sévérité, gravité des défaillances) ;

---

[6] *in* «Guide de la Sûreté de Fonctionnement» *, J.C.Laprie (Ed.) 2° ed., ISBN2-85428-341-4, Cépaduès Ed., France, 1995.*

- mais aussi le comportement des systèmes tolérants les fautes (silencieux sur défaillance, arrêt sur défaillance, etc).

Les « *moyens* » pour la sûreté de fonctionnement sont également répertoriés en quelques catégories, elles-mêmes subdivisées en diverses techniques et méthodes :

- *prévention des fautes :* comment *empêcher l'occurrence ou l'introduction de fautes* ;
- *tolérance aux fautes :* comment *fournir un service correct au système en dépit des fautes* ;
- *élimination des fautes :* comment *réduire la présence (nombre, sévérité) de fautes* ;
- *prévision des fautes :* comment *estimer la présence, la création et les conséquences des fautes*.

«Security, Safety, Quality, Dependability and…Privacy'»

Toutes ces propriétés, exprimées en anglais, ne sont que des associations ou recombinaisons, plus ou moins subtiles, d'une kyrielle de propriétés élémentaires à satisfaire ou de techniques de base à assembler et à mettre en œuvre :

- la *disponibilité*, propriété à double face :
  - disponibilité des informations au sens de la sécurité,
  - ou bien disponibilité du système au sens de la sûreté de fonctionnement ;
- la *sécurité*, propriété combinée : association de la *disponibilité*, l'*intégrité* et la confidentialité ;
- la *confidentialité*, une propriété à raffiner : *confidentialité-**discretion*** classique au sens bancaire ou militaire et donc réversible (la ***discretion*** pouvant être levée sur motif légitime), ou bien *confidentialité-**seclusion*** en corrélation avec le respect irrémédiable de l'*intimité-**privacy*** et de la vie privée (la *confidentialité-**seclusion***[7] se devant de n'être maîtrisée que par le cyber-citoyen en personne) ;
- la *sûreté de fonctionnement*, un concept générique…confidentialité, disponibilité, fiabilité, intégrité, sécurité-security, sécurité-innocuité, maintenabilité, …performabilité, …

Toutes ces propriétés sont autant de facteurs de qualité des données et informations manipulées, des logiciels, progiciels et applicatifs les traitant et des systèmes informatiques ou d'information en général : ainsi, elles ***participent à la qualité*** des données, programmes et systèmes.

Ces propriétés sont, certes, interdépendantes mais aussi et surtout tributaires de la qualité préconisée dans le cycle de conception, fabrication et exploitation du système informatique globalement : ainsi, ces propriétés et concepts ***participent de la qualité*** du cycle de vie du logiciel dans son ensemble.

Nouveaux concepts, nouveaux termes, nouvelles propriétés, nouvelles définitions et acceptions peuvent désormais être livrés aux appétits des Adéliens.

Pour le dessert, apportons les mots « tarte à la crème » dont on use et abuse dans nombre de lieux, mais néanmoins mots-clés incontournables pour la construction des futurs systèmes d'information sûrs (fiables, pérennes, sûrs, authentiques, intègres, disponibles, …) :

- ce sont les très connus *TPC-**TTP***[8], et autres *ICP-**PKI***[9], *IGC-**KMI***[10], *IGP-**PMI***[11] moins célèbres ;

---

[7] ***Seclusion*** *(G.B.) : «adaptation physiologique par laquelle un animal ou une plante s'isole du milieu, empêchant passivement les actions défavorables de s'exercer sur lui », et, par analogie, «technique consistant à interdire toute possibilité de s'immiscer dans la vie privée (électronique) des individus, en empêchant à la source toute identification nominative ».*

[8] *Tierce Partie de Confiance -* ***Trusted Third Party***

[9] *Infrastructure de Clef Publique -* ***Public Key Infrastructure***

[10] *Infrastructure de Gestion de Clefs publiques -* ***public Key Management Infrastructure***

[11] *Infrastructure de Gestion des Privilèges -* ***Privilege Management Infrastructure***

- ce sont les notions d'anonymisation et de pseudonymisation, et de risques de désanonymisation par inférence déductive, inductive, abductive ou adductive…
- ce sont les techniques de détection de virus et vers informatiques, ou encore celles de détection d'intrusions par modèles comportementaux ou par scénarios d'attaques isolées ou concertées…

De nouveaux thèmes de réflexions pourront ainsi être lancés sur demandes de chacun de nous…

De nouveaux travaux ou ateliers pourraient même être mis sur les rails[12] dans l'optique de, pourquoi, construire des SECURIscope, CONFIscope, PSEUDOscope, et autres FIABIscope, DISPOscope…

De nouvelles communications par la Lettre d'ADELI ou par tout autre vecteur d'information et de nouvelles commissions innovantes seraient alors à imaginer et à mettre en œuvre.

Pour toutes ces raisons, cette brève (car déjà terminée) cure de mise en appétit se veut être :

- un appel à contributions par des articles ;
- un appel à propositions de réflexions ;
- un appel à composition d'autres synergies et d'autres cinématiques pour contribuer à la propagande Sécurité(s) & Sûreté(s)…

Post-Scriptum : Tout détail précis et définition formelle des différents concepts et diverses théoriques évoquées *supra* figureront dans des articles et documents futurs d'ADELI.

Une bibliographie des ouvrages de références en *Sécurité*, *Sûreté* et *Tolérance aux fautes*, sera également fournie en temps utile.

☛ *Avis*

par courriel : gilles.trouessin@cnamts.fr
par courrier : CESSI-CNAMTS - 14, place Saint-Étienne - 31000 TOULOUSE
par téléphone : +33 (0) 6 6610.5076
par télécopie : +33 (0) 5 622.622.43

Gilles Trouessin
(tout nouveau) Vice-président d'ADELI
chargé du Développement des Activités Nouvelles
Ingénieur d'Études en Sécurité au CESSI[13]-CNAMTS[14]
Animateur du GE-SSIS[15] et membre de la CN SSI[16] d'AFNOR
Expert au TC251/WGiii[17] du CEN et aux TC215/WG4 et WG5[18] de l'ISO

[12] *Encore et toujours… dans le chemin de fer…*

[13] *CESSI : Centre d'Études des Sécurités du Système d'Information de la CNAMTS.*

[14] *CNAMTS : Caisse Nationale de l'Assurance Maladie – Travailleurs Salariés.*

[15] *GE-SSIS : Groupe d'Experts 'Sécurité des Systèmes d'Informations de Santé' d'AFNOR.*

[16] *CN SSI : Commission de Normalisation en 'Sécurité des Systèmes d'Informations' d'AFNOR.*

[17] *TC251/WGiii : Comité technique 'Informatique de Santé' / Groupe de Travail 'Sécurité, Sûreté et Qualité' du CEN.*

[18] *TC215/WG4 & 5 : Comité technique 'Informatique de Santé' / Groupes de Travail 'Sécurité' & Cartes à puces à l'ISO.*