La qualité logicielle au service de la sécurité - IT-expert Magazine

18 Jul 2016
by Aurelie Magniez
La part de l'informatique embarquée dans l'électronique embarqué va croissante notamment avec le développement de l'Internet des objets.

On les retrouve ainsi sous de très nombreuses formes telles que les microcodes ou firmware, les interfaces de programmation applicative (API), les calculateurs, les capteurs, les agents intelligents.

Alors que les microcodes ont, pendant longtemps, été mis à la disposition du public par leurs constructeurs, certains d'entre eux ont décidé d'encadrer plus strictement leur accès aux fins de se réserver la garantie et la maintenance de leurs serveurs.

A l'instar de ses concurrents Oracle, IBM et Cisco, le constructeur HP a, en effet, cessé de diffuser librement les mises à jour de certains de ses microcodes en annonçant en février 2014, qu'« une garantie ou un contrat actif sera exigé pour accéder aux mises à jour du micrologiciel des serveurs HP Proliant ».

Il en est de même des interfaces de programmation applicative (API), disponibles en libre accès sous forme de logiciels libres jusqu'à l'affaire Oracle America c. Google, Inc., jugée par la Cour d'appel des Etats-Unis en 2014 à l'issue de laquelle ils ont été considérés comme constituant des œuvres de langages suffisamment structurées et matérialisées (individualisées) pour être éligibles à la protection par le droit d'auteur (http://www.alain-bensoussan.com/api-application-programming-interface/2015/08/04/).

Dans un contexte où l'opacité des logiciels embarqués prime de plus en plus, se pose inévitablement la question de leur transparence et, partant de leur auditabilité.

Il existe trois niveaux de qualité d'un logiciel (que l'on peut retrouver notamment dans les normes relatives à la qualité logicielle : ISO/CEI 9126, ISO 14598, ISO/IEC 25041, ISO 9000-3 – cf. Références en fin d'article) :

- la qualité dite fonctionnelle du logiciel, consistant en la capacité d'un programme à exécuter les tâches pour lesquelles il est conçu. Ce niveau de qualité revêt une importance strictement économique ;

- la qualité de l'architecture du logiciel, également liée à son ergonomie, consistant à déterminer les facteurs de coûts d'exploitation et de maintien en conditions opérationnelles du logiciel. Ce niveau de qualité va déterminer les risques opérationnels de non-pérennité ou liés aux coûts d'exploitation du logiciel ;
- la robustesse du logiciel, consistant à déterminer si le logiciel peut être facteur ou cause de risques plus importants que son propre dysfonctionnement. Cette question est intrinsèquement liée à la notion de dommage sériel.

Le dernier niveau de qualité peut se révéler problématique dès lors qu'il n'existe pas de couverture assurantielle pour les dommages sériels.

Il n'existe pas non plus de définition légale du dommage sériel, qui peut être défini comme un dommage « en série » ou « en chaîne » ou encore comme la multiplication, dans le temps et/ou dans l'espace, de dommages causés à des personnes et/ou à leur bien, et dont l'origine se situe dans un seul et même événement générateur (cause technique).

Les assureurs écartent habituellement l'indemnisation de ce type de dommage en mettant en place des techniques contractuelles permettant de délimiter clairement leurs obligations (clause de globalisation permettant de considérer comme un seul et même sinistre tous les dommages et toutes les réclamations issues d'un même fait générateur).

Ainsi pour éviter la survenance d'un dommage sériel provoqué par un logiciel embarqué, un audit de qualité non seulement sur les deux premiers niveaux de qualité de celui-ci – mais surtout sur le dernier niveau de qualité – s'avère nécessaire pour mesurer la qualité intrinsèque du logiciel embarqué et, ainsi déterminer le risque qu'il puisse causer un tel dommage sériel.

C'est là que se situe l'enjeu de l'auditabilité des logiciels propriétaires embarqués, certes soumis, en tant qu'œuvre de l'esprit, protégés par le droit d'auteur, mais dont les exigences de sécurité semblent prévaloir dans les domaines les plus sensibles tels que dans le domaine des transports (routier, ferroviaire, aéronautique), de l'aérospatial ou de la défense.

Sans pour autant opter pour l'utilisation de logiciels libres, un tel audit ne peut intervenir que si les éditeurs permettent à un bureau de contrôle, de manière partielle et encadrée, d'avoir accès aux codes sources de leurs logiciels propriétaires embarqués afin de mesurer leur qualité et d'identifier d'éventuels dysfonctionnements et failles de sécurité.

Selon les résultats de l'audit, il conviendra de mettre en œuvre, le cas échéant, des mesures de redondance et de sécurité adaptées pour gérer la couverture de ce risque (mise en place de « back up » et de « back up de back up »).

Références :

(1) La Norme ISO 9126 : « Technologies de l'information : qualités des produits logiciels », en application depuis 1992, définit un ensemble d'indicateurs pour la qualité logicielle et facilite le processus d'évaluation logiciel et la spécification d'exigences fonctionnelle ou non-fonctionnelles. Elle ne fournit qu'un cadre de description sous forme de caractéristiques détaillées en sous-caractéristiques (capacité fonctionnelle, fiabilité, facilité d'utilisation, rendement ou efficacité, maintenabilité, portabilité) mais pas de méthodologie associée.

(2) La Norme ISO 14598 « Ingénierie du logiciel – Evaluation du produit » définit une démarche méthodologique pour l'évaluation d'un système logiciel au regard des caractéristiques et sous-caractéristiques définis dans la Norme ISO 9126.

(3) La Norme ISO/IEC 25041 « Ingénierie des systèmes et du logiciel – Exigences de qualité et évaluation des systèmes et du logiciel (SQuaRE) – Guide d'évaluation pour les développeurs, les acquéreurs et les évaluateurs indépendants ».

(4) La Norme ISO 9000-3 « Acquisition, fourniture, développement, exploitation et maintenance des logiciels et des services de support associés » donne un cadre pour la gestion des projets informatiques à destination des équipes de qualité (cadre du système qualité, cycle de vie du produit, support).

Benoit de Roquefeuil, avocat
Directeur du pôle Contentieux Informatique

Alexandra Massaux, avocat
Responsable d'activité au sein du département Contentieux informatique

Alain Bensoussan-Avocats est un cabinet d'avocat entièrement dédié au droit des technologies avancées depuis 1978. Pour la 5e année consécutive depuis 2010, il a été distingué par ses pairs, « Best Lawyer » de l'année en « Droit des Technologies ».

Site : **http://www.alain-bensoussan.com/**