DÉVELOPPEMENTS TECHNOLOGIQUES

La sécurité des instruments informatisés

J.-F. MAGANA, Sous-Directeur de la Métrologie, Ministère de l'Économie, des Finances et de l'Industrie, France – Membre du CIML pour la France

Introduction

La métrologie légale a pour objectif d'apporter une confiance suffisante dans les résultats des mesurages. Les instruments de mesure doivent avoir des caractéristiques métrologiques adaptées (exactitude, fidélité, sensibilité, durabilité) qui leur permettent de fournir des résultats de mesure justes pendant leur durée de service, mais ils doivent également être insensibles à des influences extérieures qui puissent fausser ces résultats, ou être protégés contre ces influences, ou encore mettre en évidence l'existence de facteurs qui risquent d'altérer les mesurages.

Les influences que nous prenons en compte peuvent tenir:

- aux conditions d'installation de l'instrument (horizontalité d'une balance, horizontalité d'un compteur d'eau, longueurs droites de tuyauteries, etc.);
- à l'environnement de l'instrument (très peu de facteurs influençaient le fonctionnement des instruments mécaniques, ils étaient surtout susceptibles d'affecter leur durabilité);
- aux actions de l'utilisateur (mauvaises manipulations ou tentatives de fraude: les instruments mécaniques ne permettaient que des opérations élémentaires. Les erreurs de manipulation étaient réduites).

Lorsque les instruments étaient mécaniques, les facteurs de risque et les parades à ces risques étaient simples, peu nombreux, et pouvaient facilement être étudiés quasi-exhaustivement.

Les manipulations frauduleuses étaient interdites par des procédés simples:

- soit elles étaient visibles;
- soit elles étaient interdites par des protections physiques de l'accès aux éléments de l'instrument (scellements).

À cette époque (jusqu'au milieu des années 70), le métier de la métrologie légale exigeait une compétence essentiellement en mécanique et en mécanique des fluides, voire un peu de thermodynamique. Depuis, la tendance générale et constante dans les administrations a été de réduire les effectifs, ce qui a freiné le renouvellement des personnels et le recrutement de compétences nouvelles.

Pendant ce temps, l'utilisation de l'électronique, mais surtout de l'informatique dans les instruments de mesure, ont bouleversé profondément l'état de l'art.

L'évolution technologique électronique

L'électronique a considérablement développé les performances des instruments, au prix d'une sensibilité accrue à leur environnement (température, humidité, perturbations électriques et électromagnétiques, etc.). La fiabilité et la durabilité des instruments sont devenues des sujets critiques, auxquels le Document OIML D 11 apporte des éléments de réponse. Les métiers ont évolué, mais d'une manière qui permettait aux personnels de la métrologie légale de s'adapter à peu près correctement à ces nouvelles technologies.

Une difficulté commençait toutefois à apparaître: l'extrême rapidité de l'évolution des composants électroniques, qui soulevait le problème de la conformité des instruments au modèle approuvé. Ce problème n'était pas complètement nouveau, puisque même sur les instruments mécaniques, les qualités d'acier, la qualité du traitement de surface de certaines pièces métalliques, la composition des matières plastiques, voire même le conditionnement des granulés de plastique avant injection, étaient essentiels, et bien sûr difficiles voire

The English translation of this article ("Security of computerized instruments") will be published in the July 1999 Bulletin

impossibles à vérifier sur le produit fini. L'assurance de la conformité des instruments électroniques a donc été traitée de la même manière que l'assurance de la conformité des instruments mécaniques, ce qui a donné des résultats satisfaisants. La conformité relève de la responsabilité du fabricant et est présumée jusqu'à preuve du contraire. À l'initiative du fabricant ou des autorités de contrôle, des instruments ou des parties d'instruments prélevés aléatoirement dans la production peuvent être soumis à tout ou partie des épreuves de l'approbation de modèles. Cet examen de type "boîte noire" apporte une confiance suffisante dans la conformité des instruments électroniques.

L'évolution informatique

L'utilisation de l'informatique, en revanche, a fondamentalement changé les métiers de la métrologie légale. Un instrument informatisé peut être apparemment très semblable à un instrument électronique, et il peut sembler n'en être qu'une évolution. Ceci est cependant trompeur. Qu'apporte en effet l'informatique aux instruments?

- Elle n'apporte pas d'amélioration de fond des résultats bruts de mesure. L'élément clé pour la performance métrologique d'un instrument est le capteur. Si les capteurs ont pu progresser en fidélité et en reproductibilité, ces progrès ne doivent rien à l'informatique. L'informatique permet de modéliser le comportement d'un capteur et d'appliquer au traitement de son signal, de manière automatique, les procédures complexes que l'on pourrait appliquer au niveau d'un laboratoire d'étalonnage.
- Elle apporte des capacités de calcul et de traitement considérables. La puissance de calcul qu'apporte l'informatique permet d'effectuer des corrections de pression, de température, de masse volumique, sur une mesure de débit, avec un taux d'échantillonnage élevé. Elle permet de rectifier des courbes de réponse non linéaires de capteurs. Elle permet aux conversions analogiques-numériques de se raccorder à un seul composant étalon au lieu de plusieurs.
- Elle permet des fonctions considérablement plus nombreuses, plus complexes et parfois en dehors du champ de la métrologie légale. Un terminal de station-service gère les pompes à essence, mais gère également la comptabilité des transactions par carte bancaire, les niveaux de produits dans les cuves de la station, et la boutique présente dans cette station-service.
- Elle permet à des instruments différents de fonctionner en réseau. Sur un centre de réception de betteraves, en sucrerie, l'informatique relie en réseau les lecteurs de badges d'identification, les ponts-bascules "entrée" et "sortie", les différentes bascules et balances de pesée des échantillons, les saccharimètres du laboratoire d'analyse.
- Elle apporte de nouvelles vulnérabilités, beaucoup plus complexes et invisibles. L'informatique apporte aux instruments la possibilité de dialoguer avec l'utilisateur et de recevoir des ordres, fussent-ils élémentaires. Or toute possibilité d'adresser des ordres à un système informatique ou de lui fournir des paramètres ou des données peut être également une possibilité d'en corrompre le fonctionnement.

Les métiers de la métrologie légale sont par conséquent beaucoup plus fondamentalement modifiés par l'introduction de l'informatique que par l'électronique. Alors que l'électronique nécessitait une évolution des compétences que l'adaptation des personnels par une formation permanente suffisait à satisfaire, l'informatique introduit une rupture radicale. Les techniques nécessaires sont relatives à la sécurité des systèmes informatiques et ne peuvent s'acquérir que par une formation lourde.

L'étude réalisée en France

La Sous-direction de la Métrologie a fait étudier par des experts en sécurité des systèmes informatiques les exigences actuelles des réglementations (transcrites des Recommandations de l'OIML les plus récentes), les méthodes et procédures d'approbation de modèles (harmonisées en Europe par les différents Guides et projets de Guides de WELMEC), l'instruction de certains dossiers d'approbation de modèles et l'état de l'art en matière de sécurité informatique chez certains fabricants français d'instruments de mesure. Cette étude, dont des extraits sont donnés en annexe, montre comment les questions de la métrologie légale sont abordées par des professionnels de la sécurité informatique, et quelles sont les compétences requises, respectivement pour:

- spécifier les exigences réglementaires en matière de sécurité informatique des instruments de mesure;
- approuver des modèles d'instruments au vu d'une certification de sécurité délivrée par un organisme spécialisé;
- traiter complètement un dossier d'approbation, y compris la sécurité informatique.

Cette étude aborde également la problématique des modifications des modèles d'instruments après leur approbation et de la prise en compte de ces modifica-

tions dans la réglementation. Cette question, extrêmement importante, ne fait toutefois pas l'objet du présent article.

La fraudabilité des instruments

Une des questions centrales évoquées dans ce rapport sur la sécurité des logiciels d'instruments de mesure est la fraudabilité des instruments. Frauder un instrument mécanique a toujours été possible, ne serait-ce qu'en le déplombant et en le replombant avec des poinçons contrefaits ou volés. La différence qu'apportent les technologies informatiques tient à la facilité de diffusion de la fraude. Un type de fraude sur un instrument mécanique restait limité par la disponibilité des outils et du savoir-faire nécessaire (faux poinçons). Une possibilité de fraude sur un instrument informatisé peut instantanément être communiquée à de nombreux fraudeurs potentiels, voire diffusée sur Internet. En outre une fraude sur un instrument informatisé peut être discrète et ne pas être visible lors du contrôle de l'instrument.

Une autre caractéristique de la fraudabilité des instruments informatisés est qu'elle repose sur la confidentialité d'informations détenues par les fabricants et par les réparateurs. Les clés permettant d'accéder aux paramètres et aux zones protégées d'un instrument sont immatérielles (mots de passe, messages cryptés, etc.). Même si l'instrument sait se défendre contre des tentatives d'intrusion, une vulnérabilité subsiste si certains personnels du fabricant ou du réparateur sont susceptibles de divulguer ces clés. Si la divulgation de ces clés par un employé indélicat ne porte pas de préjudice au fabricant, il restera peu de moyens juridiques pour réprimer de tels actes. L'arsenal pénal des réglementations de métrologie légale n'est pas adapté à ces nouvelles délinquances. La complicité de fraude peut être invoquée, mais la fraude sera pour sa plus grande partie une fraude potentielle et non constatée.

La tentation de fraude

Les différentes catégories d'instruments ne sont pas menacées de fraude de la même manière: certains utilisateurs sont fiables (forces de l'ordre par exemple), certaines fraudes ne seront pas rentables. Une recommandation de l'étude devrait être suivie rapidement: définir une échelle de cotation des catégories d'instruments au regard de la tentation de fraude. La tentation de fraude peut s'évaluer en contrebalançant deux types de considérations:

- les gains escomptés par les fraudeurs, dépendant du nombre d'instruments en service, du coût des produits ou services mesurés par les instruments;
- le risque que la fraude soit découverte sans dispositions particulières anti-fraude imposées aux instruments (délation, recoupements entre plusieurs mesurages indépendants, risques de fuites dûes au nombre de personnes impliquées, etc.).

On peut ainsi définir une échelle de risque initial de fraude (avant que ce risque soit réduit par les sécurités exigées par les réglementations). La détermination de la résistance des mécanismes de sécurité des instruments devra ensuite être faite au vu de ce risque initial.

La réalisation des risques de fraude

Une autre question que soulève cette étude est de décider des dispositions à prendre au cas où une vulnérabilité résiduelle devienne connue du public (mot de passe par exemple). Trois cas sont envisageables:

- soit le risque de fraude est accepté en l'état;
- soit il est possible en réparation, de reconfigurer les mécanismes de sécurité ou d'activer des mécanismes de sécurité palliant cette vulnérabilité (reparamétrage ou reprogrammation) sur les instruments en service;
- soit les instruments doivent être retirés du service.

Cette question s'est posée pour un diffuseur de télévision cryptée, lorsque les plans de son premier décodeur ont été publiés dans une revue. Cette chaîne cryptée a mis à l'étude une nouvelle génération de décodeurs, qui a totalement remplacé la précédente. Dans ce cas la décision était économique et privée. En métrologie légale, une telle décision, si elle doit être prise par les autorités réglementaires, soulèvera de difficiles problèmes, notamment en matière de responsabilités.

Aucun système informatique n'est dépourvu de risques résiduels quant à sa vulnérabilité. Les risques résiduels sont acceptables lors de l'approbation de modèles; ils peuvent devenir inacceptables lorsqu'ils passent de l'état de risques à l'état de menaces avérées, alors même que l'instrument est strictement identique. Ceci soulève un difficile problème de responsabilité. Un industriel assure la responsabilité des défauts des instruments qu'il produit. Toutefois lorsqu'un risque résiduel a été identifié et accepté, même implicitement, par l'autorité d'approbation de modèles, en cas de réalisation de ce risque on ne devrait pouvoir appeler que la responsabilité de cette autorité. Peut-on juridi-

quement considérer comme un défaut caché un risque connu, dès lors qu'il se réalise? Peut-on tenir l'organisme d'approbation de modèles responsable des conséquences de la réalisation de ce risque? Ces questions sont juridiquement complexes, mais doivent être traitées.

Les compétences des experts de métrologie légale

Le rapport d'étude propose enfin une description des compétences requises pour exercer l'activité de réglementation et d'approbation de modèles, ainsi qu'un plan de formation à cet effet. Trois niveaux sont définis, répondant aux objectifs suivants:

Niveau 1:

Savoir formuler les exigences réglementaires (dans les domaines électronique et informatique);

Niveau 2:

Savoir lire et comprendre un rapport d'évaluation de la sécurité informatique d'un instrument;

Niveau 3:

Savoir évaluer la sécurité informatique d'un instrument.

Il suffit de lire cette partie du rapport, décrivant les pré-requis de base et les plans de formation correspondant à ces trois niveaux, pour réaliser que la métrologie légale est désormais un nouveau métier.

Chaque responsable d'une unité technique en métrologie légale pourra juger quelle proportion de son personnel possède les pré-requis et est apte à suivre les formations décrites. Ce constat sera souvent inquiétant pour les organismes qui n'ont pas connu un rapide et récent renouvellement de leur personnel avec un profil de recrutement tel qu'il est proposé dans le rapport.

Certains pourront penser que l'auteur du rapport a volontairement placé la barre très haut dans ses recommandations afin de valoriser les organismes spécialisés en sécurité informatique. Ce n'est pas notre sentiment, et le travail accompli en commun par des experts de la Sous-direction de la Métrologie, avec cet expert, sur l'analyse pratique de dossiers d'approbation, nous a convaincus que ces recommandations sont pertinentes.

Nos experts, qui procèdent régulièrement à des approbations de modèles d'instruments informatisés, appliquent l'état de l'art admis en Europe, qui représente une partie des méthodes présentées dans le rapport. L'approfondissement préconisé apparaît nécessaire aux spécialistes de la Sous-direction de la Métrologie pour mieux dominer le sujet, avec une approche et des outils plus complets et plus cohérents.

Conclusion

Un dernier conseil pour les responsables d'organismes de métrologie légale qui ne seraient pas convaincus de la nécessité d'un renouvellement profond des compétences: comparer l'évolution des âges (et des types de formations):

- des concepteurs d'instruments de mesure dans la plupart des entreprises;
- des spécialistes des services de métrologie légale.

Sans retirer le moindre mérite à nos anciens, dont l'expérience et le jugement sont encore précieux, la comparaison ci-dessus est éloquente. ■

Extraits du rapport de la société CR2A-DI sur la sécurité des instruments informatisés

2.3 Fraudabilité des instruments de mesure

L'examen de la sécurité des logiciels soumis au contrôle légal peut être modulé en fonction de la fraudabilité de la catégorie des instruments de mesure dont ils font partie intégrante. La fraudabilité des instruments de mesure peut être déterminée en fonction de divers paramètres, comme par exemple:

- les enjeux associés à la fraude, c'est-à-dire le gain potentiel que peut apporter la fraude. Ce gain potentiel est à comparer à celui qu'apporte la fraude à l'utilisation: il n'est peut-être pas nécessaire ni justifié de protéger à l'excès les instruments de mesure si l'on peut aisément pratiquer la fraude à l'utilisation;
- les pénalités encourues, à comparer au profit que peut apporter la fraude;
- la détectabilité de la fraude, c'est-à-dire la probabilité de sa détection dans un délai raisonnable;
- le nombre de personnes qu'il est nécessaire d'impliquer dans la fraude;
- le nombre d'instruments de mesure produits: un agresseur ne mettra jamais plus de moyens en œuvre que ce que pourra lui apporter le fruit de son agression. La mise au point de dispositifs de fraude (par exemple, le "sucre" des taximètres) peut nécessiter plusieurs mois d'études, de conception, de développement. L'agresseur cherchant un retour sur investissement, il est plus rentable pour lui de chercher les moyens de

frauder au moyen d'un instrument de mesure reproduit à des milliers d'exemplaires. En effet, la taille de sa clientèle potentielle est directement proportionnelle au nombre d'exemplaires de l'instrument de mesure mis sur le marché;
- la nature de la clientèle visée par la transaction effectuée au moyen de l'instrument de mesure: les industriels disposent lors d'une transaction de plus de moyens de recoupement des informations et de vérification que lorsqu'il s'agit d'une vente au grand public. Il est donc plus probable de voir se commercialiser "sous le manteau" des dispositifs de fraude dans le cadre des transactions visant le grand public;
- la catégorie d'utilisateurs (agents de la force publique, postiers, huissiers, experts, garagistes, transporteurs routiers, détaillants, ...).

Lorsque les enjeux sont particulièrement importants, il peut s'avérer nécessaire d'exiger que la partie métrologique de l'instrument de mesure fasse l'objet d'une évaluation selon les critères ITSEC. Dans ce cas, le niveau d'évaluation doit être déterminé le plus tôt possible, le respect de certains critères d'évaluation ayant une influence sur le processus de développement et sur l'organisation interne des fabricants: pour qu'une évaluation selon les critères ITSEC aboutisse avec succès, ces critères doivent être respectés avant le début du développement. Le cas de l'approbation de modèle d'un instrument de mesure faisant l'objet d'une évaluation selon les critères ITSEC est abordé plus en détail dans la suite du document.

2.4 Objectifs de sécurité

Les objectifs de sécurité énoncés ci-dessous ont un caractère générique, afin de pouvoir s'adapter à toute catégorie d'instruments de mesure. Ils sont exprimés indépendamment de toute notion d'évaluation selon les critères ITSEC:

- prévenir les tentatives de fraude réalisées au moyen d'outils du commerce (éditeurs de texte par exemple);
- prévenir les fausses manipulations non intentionnelles;
- garantir que l'instrument de mesure ne comporte pas de fonctions cachées qui permettraient de modifier son comportement métrologique. Ces fonctions cachées peuvent soit exister à l'insu du fabricant (défaut de conception ou vulnérabilité de l'un des constituants de l'instrument de mesure), soit être volontairement ajoutées au logiciel de métrologie par l'équipe de développement, dans le but de négocier leur utilisation sous le manteau;
- garantir l'exactitude (c'est-à-dire l'intégrité) des données métrologiques durant tout le mesurage, durant leur transmission, durant leur impression et/ou leur affichage et, éventuellement, durant toute la durée de leur stockage. Le détenteur d'un instrument de mesure ne doit pas pouvoir modifier ces données;
- garantir la disponibilité des données métrologiques durant tout le mesurage et, éventuellement, durant toute la durée de leur stockage;
- garantir l'origine des données métrologiques lors de leur transmission;
- garantir l'inviolabilité des mécanismes de sécurité critiques;
- garantir qu'il n'existe pas de défaut de conception, d'implémentation ni de mise en œuvre;
- garantir que chaque catégorie d'utilisateur (détenteur, réparateur, ...) n'a accès qu'aux seules fonctionnalités qui lui sont autorisées;
- garantir que les différents modes d'utilisation prévus permettent de s'assurer de l'identité de l'utilisateur (identification et authentification);
- garantir que tout dysfonctionnement de la partie métrologique du logiciel est détecté et empêche le mesurage;
- garantir l'exactitude de l'identification du logiciel (numéro de version, numéro de série, ...);
- garantir le fonctionnement permanent des fonctions et mécanismes de sécurité;
- garantir la présence de certains dispositifs obligatoires, lorsque cela est approprié;
- garantir la préservation de la sécurité en cas de dysfonctionnement de l'instrument ou en cas de discontinuité de service (défaut d'alimentation électrique par exemple);
- garantir s'il y a lieu la protection de la confidentialité, de l'intégrité et de la disponibilité des éléments secrets (clés de chiffrement, mots de passe, ...), y compris en cas de dysfonctionnement;
- dans le cas où cette fonctionnalité est prévue, assurer l'imputabilité des actions effectuées sur l'instrument de mesure ayant une influence sur la partie métrologique (étalonnage, saisie de tarifs, ...) par une journalisation de ces actions.

Les instruments de mesure subissent des tests en laboratoire permettant de s'assurer de leur continuité de fonctionnement malgré des perturbations électriques, électromagnétiques et atmosphériques (hygrométrie, température). Les dysfonctionnements qui pourraient survenir à cause de ce type de perturbations sont donc en dehors du champ de l'étude et ne donnent pas lieu à l'expression d'objectifs de sécurité.

3.1 Détermination du niveau d'évaluation pour une catégorie d'instrument de mesure

Le coût d'une évaluation ITSEC dépend de la taille de la cible d'évaluation et du niveau de l'évaluation. Les critères ITSEC déclinent des exigences en assurance conformité et en assurance efficacité.

Les exigences d'assurance conformité peuvent se résumer ainsi:

- *niveau E1:* à ce niveau, il doit exister une cible de sécurité et une description informelle de la conception générale de la cible d'évaluation. Les tests fonctionnels doivent indiquer que la cible d'évaluation satisfait à sa cible de sécurité;
- *niveau E2:* outre les exigences du niveau E1, il doit exister une description informelle de la conception détaillée. Les éléments de preuve des tests fonctionnels doivent être évalués. Il doit exister un système de gestion de configuration et un processus approuvé de diffusion;
- *niveau E3:* en plus des exigences du niveau E2, le code source et/ou les schémas descriptifs des matériels correspondants aux mécanismes de sécurité doivent être évalués. Les éléments de preuve des tests de ces mécanismes doivent être évalués;
- *niveau E4:* en plus des exigences du niveau E3, il doit exister un "modèle formel sous-jacent de politique de sécurité

supportant la cible d'évaluation". Ce modèle formel est une présentation abstraite des principes de sécurité importants qu'une cible d'évaluation devra faire respecter. C'est une modélisation d'exigences de sécurité qui doit être obligatoirement réalisée dans un langage formel et accompagnée d'une interprétation informelle sous l'angle de la cible de sécurité. Les fonctions dédiées à la sécurité, la conception générale et la conception détaillée doivent être spécifiées en style semi-formel;

- *niveau E5:* en plus des exigences du niveau E4, il doit exister une correspondance étroite entre la conception détaillée et le code source et/ou les schémas descriptifs des matériels;
- *niveau E6:* en plus des exigences du niveau E5, les fonctions dédiées à la sécurité ainsi que la conception générale doivent être spécifiées en style formel de manière cohérente avec le modèle formel sous-jacent de politique de sécurité.

La signification de la cotation de la résistance des mécanismes est la suivante:

- pour que la résistance minimum d'un mécanisme critique soit cotée élémentaire, il doit être manifeste qu'il fournit une protection contre une subversion accidentelle aléatoire, bien qu'il soit susceptible d'être mis en échec par des agresseurs compétents;
- pour que la résistance minimum d'un mécanisme critique soit cotée moyenne, il doit être manifeste qu'il fournit une protection contre des agresseurs dont les opportunités ou les ressources sont limitées;
- pour que la résistance minimum d'un mécanisme critique soit cotée élevée, il doit être manifeste qu'il ne pourra être mis en échec que par des agresseurs disposant d'un haut degré de compétence, d'opportunité et de ressources, une attaque réussie étant jugée normalement au delà du réalisable.

Dans le cadre des logiciels, les agresseurs peuvent mettre en œuvre des moyens d'attaque tels que des dictionnaires de mots de passe (disponibles sur Internet) qui permettent de découvrir des mots de passe et d'accéder ainsi à un mode d'utilisation privilégié (ce genre de logiciel est généralement utilisé pour obtenir les droits de l'administrateur). Les agresseurs peuvent également mettre en œuvre des outils de rétroingénierie qui permettent de reconstituer le code source à partir du code exécutable. Il devient alors aisé de modifier le code afin d'y introduire des fonctionnalités complémentaires ou de modifier son fonctionnement.

Le niveau d'évaluation doit être choisi principalement en fonction de la fraudabilité potentielle de la catégorie d'instruments de mesure et des enjeux associés à la fraude. Par exemple, s'il est réellement nécessaire de s'assurer de ce qu'il n'existe pas de fonctions cachées dans le logiciel de métrologie, il est alors préférable que le code source soit examiné par les évaluateurs. Dans ce cas, seule une évaluation à partir du niveau E3 permet de s'en assurer.

De même, si les enjeux associés à la fraude sont tels qu'il est pratiquement certain que des tentatives de fraude de grande envergure, pouvant prendre une tournure internationale (comme c'est déjà le cas sur Internet où des sites entiers sont consacrés au piratage informatique), seront entreprises pour contourner les mécanismes de sécurité protégeant la partie métrologique des logiciels, il faudra alors viser une résistance des mécanismes élevée.

Note: Cette constatation sur Internet implique une première recommandation: il est nécessaire que l'autorité de métrologie légale procède (ou fasse procéder) à une veille technologique sur Internet dont l'objectif est de rechercher régulièrement s'il existe des sites (ou des forums) consacrés au piratage des instruments de mesure soumis au contrôle légal. Afin de conserver l'anonymat pour ces recherches, il est préférable de souscrire un abonnement Internet séparé et d'utiliser un pseudonyme. En effet, l'adresse X.Y@industrie.gouv.fr est trop voyante et risque de faire échouer la "filature".

4.1 Eléments caractéristiques du logiciel pour l'approbation de modèle

L'un des objectifs de cette étude est de déterminer les éléments caractéristiques du logiciel à demander aux fabricants d'instruments de mesure en vue d'une approbation de modèle. Ces éléments caractéristiques sont ceux qui permettent de s'assurer en tout ou partie des éléments suivants:

- l'intégrité de la partie métrologique du logiciel est régulièrement contrôlée, selon une périodicité à définir en fonction de la catégorie de l'instrument de mesure (avant chaque mesurage, à chaque mise sous tension, toutes les heures, ...);
- le mesurage ne peut avoir lieu si le résultat du contrôle d'intégrité de la partie métrologique du logiciel met en évidence un problème. Dans ce cas, un message d'erreur explicite doit s'afficher;
- l'intégrité des indications principales (grandeurs dont les valeurs sont soumises au contrôle de l'État) est préservée et régulièrement contrôlée;
- il est impossible de modifier en cours de mesurage les indications principales qu'il n'est pas prévu de mesurer au cours du mesurage (par exemple, le prix unitaire);
- si l'instrument de mesure comporte un mode programmation/consultation qui permet à l'utilisateur de saisir des données (prix unitaire, nature des produits commercialisés, ...) ou de consulter des données de gestion stockées en mémoire (total des ventes, kilométrage total parcouru, ...), il doit être impossible d'effectuer un mesurage lorsque l'instrument de mesure est en mode programmation/consultation;
- l'accès aux fonctions de programmation, de réparation et d'étalonnage dédiées uniquement aux organismes agréés est protégé par un mécanisme de sécurité (mot de passe par exemple) dont la résistance est appropriée à la fraudabilité de l'instrument de mesure;
- l'intégrité des données métrologiques est contrôlée durant tout le mesurage par un mécanisme de sécurité dont la résistance est proportionnelle à la fraudabilité de la catégorie d'instrument de mesure (CRC, chiffrement, ...). Un message d'erreur explicite s'affiche en cas de problème et le mesurage est si possible arrêté;
- l'intégrité des données stockées en mémoire est préservée et régulièrement contrôlée;
- les données sont stockées en mémoire avec la date de la transaction afin de permettre leur conservation pendant une durée prédéfinie de stockage;

- l'effacement des données stockées en mémoire ne peut avoir lieu avant la fin de la durée prédéfinie de stockage;
- en cas de saturation des dispositifs de stockage des données, les transactions sont bloquées ou un processus spécial d'effacement de données se déclenche. Dans les deux cas, un message d'erreur explicite doit s'afficher. L'effacement spécial de données mémorisées ne doit intervenir qu'après accord explicite et selon une procédure exceptionnelle;
- les interfaces de la partie métrologique du logiciel la protègent vis-à-vis de l'extérieur;
- les protocoles de communication utilisés garantissent le contrôle de l'intégrité des flux d'information;
- le logiciel ne comporte pas de fonctions cachées, c'est-à-dire que le jeu de commandes est exhaustif;
- les temporisations d'affichage des données et de passage du mode utilisation aux modes de programmation ou de consultation de données sont compatibles avec le type d'instrument de mesure. Ces temporisations interdisent toute confusion entre la somme due et une totalisation des données de gestion mémorisées par exemple;
- la confidentialité des informations nominatives, si elles existent, est préservée;
- il est possible d'identifier le numéro de version du logiciel et de prouver que c'est réellement le numéro de version qui s'affiche;
- il est possible de s'assurer que c'est le logiciel qui a fait l'objet d'une approbation de modèle qui est réellement implanté dans l'instrument de mesure;
- la partie métrologique du logiciel a fait l'objet de tests fonctionnels selon un scénario de tests prédéfini. L'étendue de la couverture des tests permet raisonnablement d'assurer la sécurité du logiciel en fonction de la résistance qu'il doit offrir aux tentatives de fraude.

Les éléments de preuve qui permettent au rapporteur d'effectuer les vérifications nécessaires peuvent prendre la forme de documentation descriptive du fonctionnement de l'instrument, de documents de conception (spécification de besoins, conception générale, conception détaillée, dossier d'analyse, logigramme, code source, ...), de fiches techniques de composants, de rapports d'essais, ... Ces éléments de preuve sont actuellement d'une teneur variée.

5.1 Tronc commun de formation

5.1.1 Pré-requis

L'examen de la sécurité des logiciels ou des transmissions électroniques nécessite de disposer d'un certain nombre de connaissances à la fois en informatique/électronique et en sécurité des systèmes d'information. La sécurité des systèmes d'information est abordée au paragraphe suivant: "sensibilisation à la sécurité".

L'objectif du présent paragraphe est de donner la liste des connaissances nécessaires en informatique et en électronique. Étant donné l'ampleur des sujets abordés, il s'avérera très certainement nécessaire de répartir ce noyau de compétences sur plusieurs personnes qui agiront de manière complémentaire.

Note: le fait de répartir des compétences sur plusieurs personnes peut avoir une influence sur l'organisation future de l'organisme d'approbation de modèles. En effet, il sera peut être nécessaire, à l'avenir, de répartir entre les rapporteurs les examens de dossiers d'approbation de modèle par pôles de compétences, en fonction de la structure interne de l'instrument de mesure, plutôt que par catégories d'instruments de mesure, comme c'est le cas actuellement.

Les connaissances nécessaires en informatique sont les suivantes:

- bonnes connaissances générales de la micro-informatique: connaissance de la structure interne et du fonctionnement d'un PC, des différents périphériques;
- bonnes connaissances pratiques des systèmes d'exploitation standards (Windows 3.X, Windows 95, Windows NT, Unix, ...);
- bonnes connaissances générales des grandes notions de base de l'informatique: savoir ce qu'est un système d'exploitation, un langage de programmation, un compilateur, un éditeur de liens, un protocole de communication, ...;
- bonnes connaissances des protocoles standards (TCP/IP, ...) et des couches OSI;
- connaissance pratique d'Internet.

Les connaissances nécessaires en électronique sont les suivantes:

- bonnes connaissances des câblages (paires torsadées, câbles coaxiaux, fibres optiques) et des différents types de topologie de réseau et de leurs conséquences;
- bonnes connaissances générales des composants pouvant faire partie d'un instrument de mesure (RAM, ROM, EPROM, carte réseau, microprocesseur, ...) et de leur utilisation;
- connaissances nécessaires pour l'examen de la pertinence d'un schéma électronique;
- bonnes connaissances générales en électricité.

5.1.2 Sensibilisation à la sécurité

La sensibilisation des rapporteurs à la sécurité des systèmes d'information est un préalable nécessaire à une formation plus poussée à la sécurité. Le plan de la séance de sensibilisation peut comporter deux volets:

- un volet de culture générale sur la sécurité;
- un volet personnalisé.

Le volet de culture générale sur la sécurité peut suivre le plan suivant:

- description générique d'un système d'information: un système d'information se compose de ressources physiques (ordinateurs, réseaux, périphériques, ...) et de ressources logiques (progiciels, applications, données);
- définition des principaux concepts employés en sécurité (objectifs de sécurité, menaces, parades, disponibilité, intégrité, confidentialité, authentification, identification, contrôle d'accès, attaque, vulnérabilité, ...) et explications sur le vocabulaire spécifique à la sécurité des systèmes d'information;

- illustration de quelques cas de sinistres informatiques occasionnés par des attaques (modifications illicites de sites Internet, ...);
- description générale des outils pouvant être mis en œuvre pour procéder à une attaque (dictionnaires de mots de passe, sniffers, ...);
- description générale de quelques vulnérabilités connues (usurpation des droits d'administrateur);
- description des principales fonctions de sécurité employées (contrôle d'accès, audit, ...) et de leur implémentation (utilisation de fonctionnalités du système d'exploitation, présentation des grandes familles d'outils du commerce tels que les firewalls, ...);
- introduction à la sécurité des réseaux;
- présentation succincte des critères d'évaluation ITSEC, des acteurs et des rôles qui y sont associés (SCSSI, CESTI, évaluateur, fabricant, ...);
- présentation succincte de la production documentaire associée aux critères d'évaluation ITSEC (cible de sécurité, fournitures d'efficacité et de conformité, RTE, ...), ainsi que des notions de cible d'évaluation, fonction de sécurité, ...;
- synthèse sur la réglementation associée à la sécurité des systèmes d'information (protection juridique des informations confidentielles, cryptologie, ...);
- présentation des principales méthodes françaises d'évaluation de la sécurité d'un système d'information: MELISA, MARION, MASSIA.

Note: les méthodes MELISA, MARION et MASSIA sont des méthodes qui permettent de conduire des audits sur site afin d'estimer la vulnérabilité d'un système d'information. Bien que ces méthodes ne soient pas directement exploitables dans le cadre de la métrologie légale, leur consultation peut s'avérer intéressante car cela permet d'avoir une vision globale des vulnérabilités qui peuvent exister, ainsi que des menaces et des contre-mesures à mettre en place pour les contrer efficacement.

5.2 Formation de niveau 1

L'objectif de la formation de niveau 1 est d'être en mesure de formuler des exigences réglementaires en termes de sécurité des logiciels et de sécurité des transmissions électroniques. Ces exigences réglementaires visent à servir de cahier des charges pour la rédaction de cibles de sécurité pour les instruments de mesure devant faire l'objet d'une évaluation selon les critères ITSEC. Elles doivent être adaptées au contexte d'utilisation des instruments de mesure, au risque de fraudabilité qui leur est associé, ainsi qu'aux technologies employées. Il convient donc d'approfondir les connaissances en sécurité des systèmes d'information afin d'avoir une vision globale du sujet.

Le niveau de connaissances visé doit être équivalent à celui d'un ingénieur en informatique/électronique disposant d'une expérience de 2 à 5 ans, comprenant une expérience significative en sécurité.

Les aspects à approfondir sont les suivants:

- bonnes connaissances de la réglementation relative à la sécurité des systèmes d'information;
- bonnes connaissances des critères d'évaluation ITSEC;
- bonnes connaissances générales des solutions de sécurité. Ces connaissances doivent permettre de dimensionner les exigences en fonction de la catégorie d'instruments de mesure concernée;
- bonnes connaissances de la sécurité des réseaux;
- connaissance pratique de la méthode EBIOS.

Note: la méthode EBIOS a pour objectif l'expression des besoins et l'identification des objectifs de sécurité. Bien que cette méthode ne soit pas directement exploitable dans le cadre de la métrologie légale, elle apporte un cadre méthodologique appréciable pour déterminer des objectifs de sécurité. Cela s'avère particulièrement utile lorsqu'il est nécessaire de rédiger une cible de sécurité.

5.3 Formation de niveau 2

L'objectif de la formation de niveau 2 est d'être en mesure de comprendre les documents disponibles lorsqu'un produit a été évalué selon les critères ITSEC et qui sont accessibles à l'autorité d'approbation de modèles. Ces documents sont: la cible de sécurité, le certificat, le rapport de certification et les documentations du produit. En effet, les fournitures d'évaluation sont confidentielles, de même que les rapports de fin de tâche des évaluateurs, ainsi que le RTE.

La formation de niveau 2 vient en complément de celle de niveau 1.

Le niveau de connaissances visé doit être équivalent à celui d'un ingénieur en informatique/électronique disposant d'une expérience de 2 à 5 ans, comprenant une expérience poussée en sécurité.

Les aspects à approfondir sont les suivants:

- connaissance pratique des critères d'évaluation ITSEC et du manuel ITSEM;
- bonnes connaissances des solutions de sécurité. Ces connaissances doivent permettre de déterminer si une fonction de sécurité est suffisante pour assurer le respect des objectifs de sécurité;
- notions de cryptologie.

5.4 Formation de niveau 3

L'objectif de la formation de niveau 3 est d'être en mesure d'exercer l'équivalent du métier d'évaluateur. La formation de niveau 3 vient en complément de celle de niveau 2.

Le niveau de connaissances visé doit être équivalent à celui d'un ingénieur en informatique/électronique disposant d'une expérience de 5 à 10 ans, spécialisé en sécurité. Comme cela a déjà été signalé plus haut, les compétences nécessaires devront être réparties sur plusieurs personnes.

Les compétences à acquérir sont les suivantes:

- veille technologique, en particulier sur Internet, pour s'informer des évolutions technologiques et rechercher des vulnérabilités ainsi que des outils d'attaque;
- connaissances poussées des critères d'évaluation ITSEC et du manuel ITSEM;

- connaissances poussées de langages de programmation et de langages assembleur;
- connaissances poussées de systèmes d'exploitation;
- connaissances poussées en architecture de réseau;
- connaissances poussées des protocoles de communication (savoir interpréter les trames de données circulant sur un réseau);
- connaissances poussées de technologies telles que cartes à puce, firewalls, cryptologie, ...;
- connaissances poussées des plates-formes de développement (ateliers de génie logiciel, ateliers de conception assistée par ordinateur, ...);
- connaissances poussées des techniques de test (analyse de flots de données, tests statiques et dynamiques, analyse de couverture de tests, ...);
- connaissance pratique d'outils d'attaque (oscilloscope, analyseur de spectre, machine de décryptage, analyseurs de protocole, sniffers, dictionnaires de mots de passe, outils de rétroingénierie, outils d'analyse de code source, ...);
- si nécessaire, formation aux méthodes formelles (en cas d'évaluation à partir du niveau E4);
- connaissance des techniques d'audit sur site.