## Gouvernance des systèmes STI

Dans les premières générations de STI, chaque système avait son maître d'ouvrage qui en assurait la conception, le financement, l'exploitation et la surveillance. L'enjeu est aujourd'hui de déployer à grande échelle des systèmes interopérables. Chacun des acteurs n'a prise que sur une partie du système d'ensemble. Cette situation a été depuis longtemps perçue comme fragile dans de nombreux domaines. Par exemple, les « chartes d'interopérabilité » mises en place à partir de 1998 pour les systèmes de billettique ont été limitées au cadre régional. Pour la dématérialisation des échanges de données qui accompagnent les transports de marchandises, les entreprises, qui ont pendant longtemps créé des systèmes EDI dans le cadre « d'accords d'interchange » bilatéraux, ne viennent que très progressivement aux logiques de plateformes électroniques. Il est donc nécessaire de préciser les missions à assurer par l'entité qui gère une « interopérabilité », c'est à dire un système composé de sous-systèmes interopérables entre eux.

On remarquera que l'interopérabilité ainsi définie correspond à un phénomène qui a nécessairement un début et une fin : qu' il s'agisse de systèmes nouveaux qui doivent commencer à fonctionner ensemble le même jour (big bang) ou de systèmes qui « s'accrochent » à des systèmes existants, il y a des décisions à prendre sur la validité des études préalables, la liste des acteurs qui sont prêts à un moment donné pour faire des essais et sur l'information que l'on peut donner aux clients sur le périmètre effectif du service dont ils peuvent disposer quand ils s'adressent à l'un de ces systèmes interopérables. Ces décisions ne sont pas seulement à prendre une fois, il s'agit d'une activité permanente qui ne prendra fin que lorsque l'interopérabilité elle-même disparaîtra, par exemple parce que tous les systèmes se seront arrêtés ou parce qu'ils auront été englobés dans un mécanisme plus large de type « bouquet de services » .

D'une façon concrète, il y a dans l'activité consistant à créer et à faire vivre une interopérabilité deux grands aspects : la promotion de la confiance et la gestion des risques. Le premier aspect porte sur la communication et la psycho-sociologique dans la mesure où il s'agit de s'adresser non seulement aux acteurs directement impliqués dans les échanges de données et le bon fonctionnement des opérations, mais aussi à leurs clients pour que les difficultés et les perturbations inévitables soient l'occasion de renforcer l'image de l'ensemble et de sa cohésion, en démontrant par exemple que chaque utilisateur au bout de la chaîne bénéficie d'un service bien meilleur que s'il n'avait en face de lui qu'un seul fournisseur isolé qui pourrait être dépassé par les événements. Le second aspect fait appel à des techniques qui ont été décrites abondamment dans la littérature, à l'intention des responsables de systèmes complexes : analyser les risques (notamment les risques informatiques, ..) examiner de façon raisonnée leurs conséquences pour les entreprises concernées et pour leurs partenaires, en déduire les mesures à prendre pour répondre aux situations critiques et identifier ce que l'on ne pourra pas couvrir (voir annexe 1 pour des références à des méthodologies, qui ne portent généralement que sur des aspects partiels, le responsable doit faire son choix). En principe, ceux qui ont une responsabilité stratégique dans la mise en place du système et sa pérennité devraient être conscients en permanence des limites au-delà desquelles leur organisation ne pourra plus faire face. Mais comment prouver à l'utilisateur final que c'est bien le cas et que les responsables des services qu'on lui propose n'ont pas sous-estimé les vulnérabilités qui pourraient gêner leur politique commerciale ? Ont-ils bien révisé régulièrement les analyses de risques sur lesquelles sont fondées leurs organisations ?

Admettre le fait que les organisations pourraient être dépassées un jour, c'est aussi

admettre qu'il pourrait se produire des crises dans lesquelles il faudra que la puissance publique intervienne pour préserver les intérêts vitaux de la population. C'est une des raisons qui va rendre nécessaire une intervention de l'État dans les mécanismes de gouvernance des STI lorsque ces systèmes prendront une place de plus en plus importante dans la vie quotidienne des citoyens et des entreprises. On appellera ici « régulation » la mission à exercer pour éviter autant que possible la multiplication des crises et réduire leurs coûts pour les tiers et notamment pour les contribuables, sans prendre parti sur ce que doit être ce régulateur (un service de l'administration centrale, une entité spécifique, « indépendante » ou non, avec ou non des mécanismes de consultation structurés...) Il s'agit de faire en sorte que les responsables des systèmes prennent effectivement les mesures qui s'imposent, bien que cela leur coûte de l'argent et éventuellement des difficultés de management. La régulation peut aussi être chargée de vérifier si la réglementation applicable est bien observée par les responsables des systèmes et si globalement les usagers ont bien des services correspondant à leurs besoins, notamment en ce qui concerne la qualité des services rendus. Dans tous les cas on voit mal comment le mécanisme pourrait durablement fonctionner avec des acteurs qui feraient librement ce qui leur rapporte le maximum de profit sans apporter des garanties sur leur capacité à supporter les conséquences directes ou indirectes de leurs actions ou inactions.

Si l'on considère que les échanges d'information liées aux transports de marchandises devraient apporter plus de sécurité et de performance à ce secteur, les politiques publiques doivent:

- encourager l'utilisation des services dématérialisés apportant la confiance aux différents acteurs (transporteurs, plateformes, autorités publiques, chargeurs) dans leurs échanges professionnels et commerciaux. L'un des encouragements important est d'utiliser ces services pour les échanges entre les administrations et les entreprises.
- surveiller l'évolution des marchés et empêcher la création de monopoles, pour permettre aux entreprises de toutes tailles de participer à la modernisation de leur secteur, éviter la captation de valeur et une prise de risque « systémique » irresponsable
- veiller à la prise en compte, par les responsables des services, des risques qui proviennent de leur propre organisation et des vulnérabilités qui découlent globalement du développement des connections entre les réseaux et des évolutions technologiques. Ceci se traduirait par des politiques de sécurité et de qualité qui aient été validées par des expertises indépendantes et régulièrement mises à jour
- se donner les moyens d'alerter les utilisateurs directs sur la baisse de fiabilité (sécurité ou qualité) de certains services et éventuellement de formuler des mises en garde ou des recommandations
- tenir prêts des scénarios d'intervention en cas de crise majeure sur un ou plusieurs systèmes, qui seraient validés dans le cadre de la mise à jour des politiques de sécurité
- mettre en place, dans le cadre des accords internationaux, un système de reconnaissance mutuelle des prestataires de service (accès à la profession), permettant d'identifier les certificats qui accompagneraient les documents issus de systèmes fonctionnant dans des pays étrangers, même s'ils ne sont pas autorisés à opérer sur le marché français

- mettre en place, au niveau européen, des accords de reconnaissance des politiques de sécurité et de qualité, permettant progressivement d'uniformiser progressivement, l'accès par les prestataires aux marchés des différents États membres.

Il est clair qu'on est loin aujourd'hui d'avoir en place les structures et les pratiques qui permettent d'appliquer de telles règles, mais les bénéfices que l'on peut attendre des nouvelles technologies ne pourront pas se concrétiser durablement si un effort collectif n'est pas fait dans ce domaine, notamment en matière de formation des acteurs à tous les niveaux. Ce sujet n'est pas spécifique au domaine des transports de marchandises, ni même aux systèmes de transport intelligents. Il est commun à toutes les utilisations de l'informatique. Les principes décrits ci dessus devront faire partie de l'éducation générale et de la formation professionnelle des citoyens et acteurs économiques et administratifs de la société numérique.

JF JANIN

Mission transports Intelligents

Août 2013

**Annexe 1**

La gouvernance d'une interopérabilité doit tenir compte des trois phases du cycle de vie:

-> avant la mise en exploitation, il faut disposer des études de risques et des scénarios de traitement des risques identifiés comme importants par leur probabilité et/ou leur gravité pour que les responsables puissent dès le départ savoir ce qu'ils ont à faire quelles que soient les circonstances
-> pendant l'exploitation, il importe de suivre si le système est encore conforme aux exigences des utilisateurs (réguliers ou non) et des commanditaires du système. Ceci ne va pas de soi pour une interopérabilité dans laquelle peuvent à tout moment se connecter (et se déconnecter) des acteurs que l'on ne connaît que par leurs interfaces
-> lorsque le système n'est plus conforme, par exemple si une faille de sécurité a été découverte, il s'agit de choisir les actions destinées à réparer ou à réduire les fonctionnalités, éventuellement temporairement, éventuellement pour permettre une fusion-absorption dans un autre système.

La notion de risque est bien centrale dans les missions de la gouvernance:
Le site suivant http://cyberzoide.developpez.com/securite/methodes-analyse-risques/ qui décrit des méthodologies éprouvées. La norme internationale ISO 17799 souvent citée a été remplacée par les normes ISO/CEI 270001 et 270002 qui traitent de la gestion de la sécurité de l'information et des systèmes de management de la sécurité des SI (SMSI)
http://fr.wikipedia.org/wiki/ISO/CEI_27001
http://fr.wikipedia.org/wiki/ISO/CEI_27002

Pour ce qui nous concerne les systèmes déployés en France, on recommande aux services publics, pour l'évaluation des besoins en matière de sécurité informatique, d'utiliser la méthode EBIOS. http://fr.wikipedia.org/wiki/EBIOS, téléchargeable directement sur le site de la ANSSI: http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf