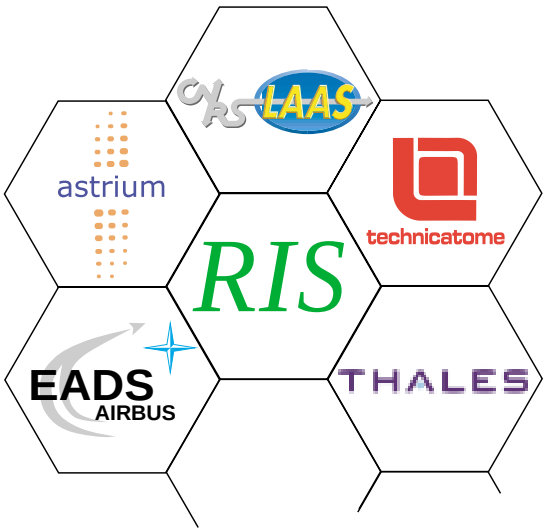

R éseau d' *I* ngénierie de la *S* ûreté de fonctionnement

COMPTE RENDU

de l'atelier thématique du 14/12/2000

« Logiciel libre et sûreté de fonctionnement »

1. Objectifs

Les ateliers thématiques du *RIS* (Réseau d'Ingénierie de la Sûreté de fonctionnement) réunissent des spécialistes des partenaires du Réseau (Astrium, EADS Airbus, LAAS-CNRS, Technicatome et Thales) et, le cas échéant des participants invités. L'objectif est, à partir d'échanges d'expériences et de points de vue, de faire une synthèse préliminaire du thème retenu pour l'atelier, et d'élaborer une ou plusieurs propositions, dans le cas où l'intérêt se dégage, de mener au sein du Réseau des réflexions et travaux plus approfondis sur ce thème.

Le premier atelier thématique du *RIS* a eu lieu le 14 décembre 2000 au LAAS-CNRS sur le thème « logiciel libre et sûreté de fonctionnement ». Le présent compte rendu a pour objectif de faire une synthèse des présentations et discussions de cet atelier et des propositions d'action correspondantes.

2. Participants

Jean Arlat (LAAS, animateur de l'atelier), Jean-Paul Blanquart (Astrium, rapporteur de l'atelier), Philippe Coupoux (Technicatome), Yves Crouzet (LAAS), Jacqueline Daries (EADS Airbus), Philippe David (Astrium), Agan de Bonneval (LAAS), Hervé Delseny (EADS Airbus), Corentin Desquilbet (CEAT), Yves Deswarte (LAAS), Jean-Charles Fabre (LAAS), Serge Goiffon (EADS Airbus), Tahar Jarboui (LAAS), Karama Kanoun (LAAS), Gérard Ladier (EADS Airbus), Eric Marsden (LAAS), Jean-Christophe Mielnik (Thales), Vincent Nicomette (LAAS), Luc Planche (Astrium), Famantanantsoa Randimbivololona (EADS Airbus), Hervé Schindler (Astrium), François Taiani (LAAS), Eric Totel (Astrium), Christophe Vinel (EADS Airbus), Hélène Waeselynck (LAAS).

3. Programme

Introduction et présentation de l'atelier	Jean Arlat (LAAS-CNRS)
Développement avionique et logiciels libres : enjeux et problèmes	Famantanantsoa Randimbivololona (EADS Airbus)
La place des logiciels « open source » à Astrium	Philippe David (Astrium)
Logiciels libres : expérience Technicatome et Linux	Philippe Coupoux (Technicatome)
Utilisation de logiciel libre sur affaire	Jean-Christophe Mielnik (Thales)
Logiciel libre : problématique de certification	Corentin Desquilbet (CEAT)
Discussion générale, propositions de mise en place d'un Groupe de Travail et de programme	

4. Synthèse des présentations

Introduction et présentation de l'atelier.

Les logiciels libres correspondent à un phénomène déjà ancien (les années 80), considérablement amplifié aujourd'hui par l'influence d'Internet, aboutissant à l'incorporation de logiciels libres dans un nombre croissant d'offres commerciales, y compris de la part des fournisseurs les plus importants, et à un transfert progressif des dépenses liées au logiciel, de l'acquisition vers les services associés (transfert et évolution également en termes de métier dans l'industrie du logiciel). Le logiciel libre se caractérise par la disponibilité des sources et le droit de les modifier et de les distribuer. Ce n'est pas nécessairement du logiciel gratuit (mais les coûts sont généralement modiques) et les droits sont précisés par des licences, par exemple la licence GPL, « General Public License ». L'intérêt des utilisateurs et des intégrateurs de logiciel pour les logiciels libres provient précisément de la possibilité d'accéder aux sources, mais aussi de la mutualisation des efforts de développement via Internet, qui favorisent la mise au point et l'évolution des logiciels. On peut également citer l'accroissement d'indépendance vis-à-vis de solutions « propriétaires », et l'accroissement d'interopérabilité par le respect des standards.

Toutefois l'incorporation de logiciels dans des systèmes critiques conduit à se poser des questions sur leur sûreté de fonctionnement, ce qui avait en particulier fait l'objet de travaux du LIS dans le cas des logiciels COTS, et ce qui constitue donc le thème du présent atelier dans le cas des logiciels libres. A titre d'introduction il est à noter que d'une façon générale les utilisateurs de logiciels libres les considèrent comme de bonne qualité, au moins équivalente aux produits commerciaux analogues, et que ceci est confirmé par les différentes études publiées d'évaluation de sûreté de fonctionnement (injection de fautes).

Développement avionique et logiciels libres : enjeux et problèmes (EADS Airbus).

EADS Airbus suit le phénomène des logiciels libres, et Linux en particulier, depuis plusieurs années (veille technologique, R&D sur les systèmes d'exploitation, utilisation de COTS pour moniteurs temps réel et systèmes d'exploitation POSIX). L'évolution des besoins des compagnies, l'évolution des avions et de leur environnement, et l'évolution technologique conduisent à plus de volume et de complexité des logiciels, de nouvelles applications (traitement de données), plus de fonctions génériques. Le développement du logiciel en « tout spécifique » n'est plus industriellement viable, mais l'intégration de COTS n'est pas toujours possible (contraintes avioniques, certification, coûts, dépendance, offre, pérennité, transparence, réactivité, etc). L'approche du logiciel libre est alors à considérer y compris pour le temps réel embarqué où par exemple Linux est souvent présenté comme le futur système dominant aux dépens des technologies « propriétaires ». Deux approches peuvent être aujourd'hui envisagées :

- Logiciel embarqué : intégration de composants logiciels libres : troisième voie vis-à-vis du développement spécifique et de l'intégration de COTS, avec une meilleure maîtrise de ce qui est embarqué, la souplesse d'adaptation et des coûts plus intéressants.
- Environnement : plate-formes à base de logiciels libres : coût, contrôle des évolutions, maîtrise de la pérennité, fonctionnalités, adaptation d'outils, intégration d'ateliers (développement, vérification).

Les points ouverts concernent l'approche pour la certification, l'adaptation du cycle de développement à l'incorporation de composants logiciels libres, les aspects contractuels et juridiques, ainsi que le foisonnement de l'offre, et l'organisation des supports à l'utilisateur.

La place des logiciels « open source » à Astrium.

Quelques logiciels libres sont déjà utilisés, quoique de façon limitée sur les projets spatiaux opérationnels, soit par utilisation explicite, soit par l'intermédiaire de produits commerciaux qui en contiennent. L'Agence Spatiale Européenne (ESA) a récemment organisé un séminaire sur les logiciels libres, qui fait ressortir la notion de cercle dit « vertueux » permettant la maîtrise des évolutions et de la cohérence des logiciels libres, et leur appropriation par les utilisateurs au travers de supports de maintenance, expertise. Ceci peut passer par la mise en place de consortiums (notion de « syndicats ») et de financements initiaux institutionnels. L'ESA poursuit une démarche analogue pour le matériel avec la mise à disposition des sources VHDL du LEON (processeur Sparc spatial de nouvelle génération), faisant état de gains substantiels de temps, coût et aussi de qualité et validation. Dans des domaines très spécifiques, les industriels concernés doivent savoir s'insérer avec la réactivité nécessaire dans de tels schémas, pour conserver leur maîtrise et éviter que les développements ne se déroulent en dehors des contraintes du domaine. Le phénomène du logiciel libre reste difficile à gérer dans des domaines considérés comme très spécifiques (pour des raisons différentes selon que la spécificité vient de l'existence de certaines fonctions logicielles très particulières, ou de caractéristiques très particulières de développement, intégration et validation). Le logiciel libre présente néanmoins des aspects intéressants par rapport aux logiciels COTS, par la possibilité d'agir sur les évolutions, le développement et la validation, et par le fait qu'au delà du retour d'expérience apporté par le grand nombre d'utilisations (de toutes façons difficile à apprécier avec pertinence), la notion de grand nombre s'étend aussi aux développeurs et à la validation.

Il apparaît donc nécessaire de s'organiser pour tirer le meilleur bénéfice des logiciels libres : organisation interne à l'entreprise, mais aussi mise en place d'actions en partenariat. Par exemple la structure du *RIS* pourrait être mise à profit pour échanger des informations sur des logiciels d'intérêt commun aux partenaires, y compris des informations sur les travaux complémentaires menés par chaque partenaire autour de ces logiciels (par exemple à des fins d'adaptation à des contraintes particulières ou pour des besoins de certification). Une approche plus ambitieuse pourrait aller jusqu'à la définition de travaux d'intérêt commun sur un logiciel libre choisi (logique de test, campagne d'injection de fautes, vérification d'intégrité, etc), avec diffusion sur un site Web permettant ainsi de tester en vraie grandeur la réactivité du cercle vertueux.

Expérience Technicatome et Linux.

Technicatome a expérimenté le logiciel libre au travers de l'utilisation de Linux dans un système opérationnel, comprenant à la fois une partie embarquée et une partie au sol, pour l'archivage et le traitement de données. Il s'agit de systèmes à grande durée de vie, nécessitant de résoudre les difficultés liées à l'obsolescence matérielle et logicielle, à la nécessité d'évolution, et de « modernisation » des interfaces. La sélection a porté sur des COTS (HP-UX, Windows NT, Solaris) et sur Linux qui a finalement été choisi en application des critères retenus (standard, pérennité, évolutivité, multi-plateforme, compétences internes, maîtrise, portabilité d'anciennes applications, administration et développement, fiabilité, coût de possession). L'expérience porte sur deux développements en cours, d'autres étant prévus ultérieurement, et se révèle satisfaisante. La réactivité du processus d'évolution et de correction de Linux est en particulier soulignée, ainsi que la standardisation qui facilite la mise en place progressive dans les systèmes industriels.

Utilisation de logiciels libres (Thales).

Thales a mis en place un groupe de travail avec pour objectifs de tirer avantage des logiciels libres, d'éliminer les risques potentiels, et d'améliorer la prise de conscience dans l'entreprise. Environ 120 logiciels libres sont utilisés dans les 7 Unités concernées du groupe, avec environ les deux tiers sous licence GPL (« General Public Licence » de FSF, « Free Software Foundation »). Le phénomène du logiciel libre prend de l'ampleur en apportant aux développeurs une reconnaissance individuelle par les pairs, et aux entreprises un transfert d'activité vers les services, entraînés par l'existence et la notoriété des produits, et l'existence d'un savoir-faire reconnu autour de ces produits. Les principales sources de risques potentiels concernent la propagation des termes des licences aux développements propres, les difficultés de la gestion de configuration, l'existence éventuelle dans un logiciel libre d'algorithmes protégés par brevet, et les difficultés liées au support sur un logiciel libre (en particulier sur une version figée). Les risques croissent pour l'entreprise, de l'utilisation interne vers l'utilisation dans des programmes externes, et de l'utilisation de logiciels libres tels quels, ou avec modifications, jusqu'à l'utilisation de logiciels libres associés à, voire insérés dans, des développement propres. Le groupe a ainsi défini des règles sur l'utilisation des logiciels libres, en fonction des types d'utilisation envisagés, avec en particulier la mise en place de structures chargées de répertorier et analyser les différents types de licences, répertorier les logiciels libres utilisés, et proposer des logiciels libres recommandés. Un effort important est mis sur les aspects juridiques, l'analyse des licences, la protection des développements propres, et la présence éventuelle d'éléments protégés inclus dans les logiciels libres.

Logiciels et certification (CEAT).

La certification porte sur un système, et non pas sur le logiciel en tant que tel, mais le logiciel a néanmoins une place importante dans le processus de certification. Une première difficulté vient des recouvrements entre les processus et règles définis aux niveaux système, matériel et logiciel. De plus concernant en particulier le logiciel, la certification met un très fort accent sur le processus de développement et de validation, plus que sur le produit lui-même, ce qui amène des difficultés par exemple pour les logiciels COTS ou les logiciels libres. Pour les COTS une solution consiste à faire de la rétro-ingénierie, mais il reste des difficultés sur les liens avec le niveau système, le niveau de détail des exigences, les test structuraux et la gestion de projet. Une autre solution consiste en la certification incrémentale, mais conduit aussi à des difficultés liées à la portabilité (indépendance vis-à-vis de la plate-forme) et à la modularité (intégration, modes communs). Pour le logiciel libre, la principale difficulté vient de l'absence d'information sur la conception, ainsi que de l'absence d'exigences de bas niveau et des aspects liés à la vérification du flot de contrôle et du flot de données. La certification de systèmes incluant des logiciels libres peut ainsi être vue comme une véritable révolution culturelle avec une remise en cause des pratiques et standards actuels. Une introduction progressive est recommandée, aux faibles niveaux de criticité (D ou C), par exemple sur les fonctions de maintenance qui semblent de bons candidats.

5. Synthèse des discussions

La discussion porte sur les aspects techniques des logiciels libres et des processus de définition, élaboration, évolution, support, et bien sûr la sûreté de fonctionnement en particulier pour des systèmes soumis à certification. Il se dégage un intérêt fort pour ce phénomène et la reconnaissance d'un marché important, mais aussi des inquiétudes sur la qualité effective des logiciels libres et du processus de correction, sur la validation, la maîtrise de la définition des besoins et du processus d'évolution, la maîtrise du processus de développement à laquelle ne peut se substituer le fait de disposer des

sources, les aspects juridiques, la sécurité, la protection des développements propres, les changements de métier ainsi que de modèle économique dans l'industrie du logiciel.

Structures : la communauté du logiciel libre se structure de façon informelle et décentralisée autour de sites Web, qu'il serait utile de répertorier (voir section 6). Certains sites permettent d'héberger des projets de logiciels libres, d'autres de proposer des spécifications pour un développement de logiciel libre, etc.

Sécurité (présence de virus par exemple) : la situation reste ambivalente, ce qui est confirmé par les travaux du dernier congrès international sur la sécurité informatique (Oakland, 2000). D'un côté, avant leur appropriation pour une application donnée, les logiciels libres sont par définition ouverts, y compris aux actions malveillantes. De l'autre côté la multiplicité et l'indépendance des participants au développement suggèrent qu'il est difficile de mener des actions malveillantes non détectées. Deux types opposés de démarches sont proposés, la sécurisation a posteriori de logiciels très largement utilisés, ou le développement spécifique de logiciels très sûrs. Il est noté que la sécurité des logiciels libres peut être étendue par analogie à la présence non déclarée d'algorithmes protégés.

Adaptations : dans les expériences d'utilisation de logiciels libres rapportées par les participants, en particulier autour de Linux, peu d'adaptations des logiciels libres ont été nécessaires, et ces adaptations sont apparues assez simples à réaliser (disponibilité des sources, lisibilité, structure du code).

Ouverture, protection : l'ouverture des travaux du *RIS* sur le logiciel libre, ainsi que la diffusion des résultats obtenus, est tout à fait envisageable, y compris aux concurrents de partenaires du réseau, et d'ailleurs conforme à l'esprit même du logiciel libre. La protection des travaux doit néanmoins être analysée, de même que, pour le logiciel libre, la protection des développements propres.

6. Pour en savoir plus

Les liens indiqués ci-dessous ont été proposés par les participants, au cours des présentations ou à la suite de l'atelier, comme pouvant apporter des compléments d'information sur le sujet. Ils sont rapportés ici à titre indicatif avec pour seule vérification qu'ils pointent effectivement à la date de rédaction (20/12/2000) vers un site en rapport avec le sujet.

Général :
http://www.fsf.org/philosophy/philosophy.fr.html#LicensingFreeSoftware

Terminologie :
http://www.fsf.org/philosophy/philosophy.fr.html#TOCTerminologyandDefinitions
http://www.fsf.org/philosophy/categories.fr.html

Législation :
http://www.fsf.org/philosophy/philosophy.fr.html#TOCLaws

Licences (GPL) :
http://www.gnu.org/copyleft/gpl.html

Sécurité :
http://www.hsc.fr/resources/presentations/libre3

Fiabilité :
http://www.fsf.org/software/reliability.fr.html

Catégories de logiciels :
http://liberte.aful.org/presentations/logiciels.html

Site de l'ESA sur le séminaire « The Role of Open-Source Software in the Space Business » (5/10/2000) :
ftp://ftp.estec.esa.nl/pub/ws/opensource/OpenSourceSeminar.htm

Un site proposant une structure d'accueil et de diffusion d'information pour les logiciels libres :
http://sourceforge.net/

Conclusions de l’atelier

Le thème « logiciel libre et sûreté de fonctionnement » est reconnu par l’ensemble des participants comme justifiant la mise en place de travaux d’approfondissement par le *RIS*. Ces travaux pourraient prendre l’une des formes suivantes (les propositions indiquées ci-dessous n’excluent, ni au sein du réseau ni en parallèle au réseau avec tout ou partie de ses partenaires, la mise en place d’autres actions en substitution ou en complément sur ce thème) :

1- Organisation de présentations et séances de discussions ciblées, éventuellement avec des participants extérieurs aux partenaires du réseau, avec pour objectif la rédaction en commun d’un ouvrage de synthèse.

2- Choisir un logiciel libre d’intérêt commun et un plan d’actions d’intérêt commun à mener sur ce logiciel (mise en place d’une logique de test, injection de fautes, vérification d’intégrité, etc), diffuser ce plan d’actions sur un site Web, tester la réactivité de la communauté du logiciel libre, suivre et participer au plan d’actions en fonction de l’intérêt suscité par le site.

3- Elaborer une base d’informations (fiches produit : documentation disponible, niveau de validation, maturité, support, etc) sur une liste de logiciels libres d’intérêt commun, et définir un processus de transfert de logiciels libres dans les projets opérationnels (mise en conformité vis-à-vis des standards ou normes applicables, DO-178B, ECSS, etc.).

L’intérêt de l’ouverture des travaux proposés est reconnu par l’ensemble des participants (et en particulier pour la première proposition sur la rédaction d’un ouvrage de synthèse). Cette ouverture concerne à la fois des compétences techniques, expériences ou domaines d’application complémentaires, pouvant être couverts dans d’autres organismes ou entreprises que les partenaires du réseau, et des métiers complémentaires couvrant par exemple les aspects juridiques liés à l’utilisation des logiciels libres, la certification, etc.