L'atelier de génie système AGeSYS

Philippe Baufreton, Jean-Claude Derrien et Marc Malot

AGeSYS (Atelier de Génie SYStème) [1] est un ensemble d'outils intégrés pour une conception « orientée modèles » de systèmes et logiciels embarqués, visant à assurer la cohérence entre description système et description logicielle ainsi qu'à industrialiser le processus d'ingénierie système avec une définition claire des transitions entre système, logiciel et matériel. Il apporte en particulier un couplage entre la modélisation système et la modélisation multi-physique.

Cet atelier a été développé dans le cadre d'un projet collaboratif de recherche et développement porté par Esterel Technologies, avec les fournisseurs de technologies Siemens, Scaleo Chip, Scilab Entreprises et le CEA, avec les utilisateurs du domaine automobile (Continental, PSA, Renault, Valéo), du domaine aéronautique (Airbus, Snecma, Sagem Défense Sécurité, Thales), du domaine ferroviaire (Alstom Transport, Atos, Thales) et avec l'appui des pôles de compétitivité Aerospace Valley (Midi-Pyrénées et Aquitaine) et System@tic (Paris-Ile-de-France). Le projet AGeSYS a reçu le soutien de l'État dans le cadre du Programme d'Investissements d'Avenir.

Le cas d'étude proposé par Sagem concernait les commandes de vol électriques secondaires de l'avion (asservissement des becs et des volets). Ce système, outre les contraintes d'environnement, met en œuvre des contraintes de sûreté de fonctionnement qui sont affinées au cours de la définition de l'architecture par une équipe multidisciplinaire (architectes, concepteurs systèmes, ingénieurs sûreté de fonctionnement, ingénieurs vérification). Il propose un périmètre représentatif d'un développement de système embarqué tout en étant de taille raisonnable pour pouvoir être appréhendé dans ce type d'étude.

L'objectif de ce cas d'étude était de permettre l'évaluation d'un atelier basé sur une approche de type ISDM (Ingénierie Dirigée par les Modèles ou, en anglais, Model-Based System Engineering - MBSE) comprenant à la fois un axe « Développement Système » et un axe « Sûreté de Fonctionnement » conforme aux recommandations des ARP 4754-A et 4761.

Une des problématiques était d'assurer la synchronisation technique entre des modèles utilisés pour structurer l'architecture du système et des modèles utilisés pour mener des analyses de sûreté. L'utilisation de modèles « fonctionnels » et « dysfonctionnels » ainsi que la mise en place de communications entre eux visaient à « simplifier » tout en « améliorant » l'application du processus d'ingénierie système incluant la sûreté de fonctionnement tout au long du cycle de développement d'un système. La simplification attendue consistait notamment à éviter de ressaisir pour mener une analyse de sûreté de fonctionnement des informations qui auraient déjà été renseignées lors de l'analyse fonctionnelle. L'amélioration désirée consistait à éviter les erreurs, les incohérences et les désynchronisations non maîtrisées entre le système pris en compte par l'analyse dysfonctionnelle et la définition courante du système.

L'outillage du processus d'Ingénierie Système

Dans un premier temps, Sagem Défense Sécurité a contribué à la spécification technique des besoins pour l'atelier d'AGeSys. Devant le nombre important d'outils mis à disposition dans le cadre du projet, Sagem a alors décidé de concentrer ses efforts sur la maîtrise de la modélisation système basée sur SysML, qui est le pivot de l'AGeSys puisqu'elle assure une continuité entre les spécifications et la conception du système. Aussi, les différentes solutions de représentation SysML constituent-elles un nœud d'interconnectivité entre les outils AGeSys.

La suite outillée qui a été évaluée par Sagem Défense Sécurité est présentée sur la figure ci-dessous. Pour permettre la compatibilité/communication entre outils dans le cadre du projet, il a été choisi d'utiliser l'environnement Eclipse Kepler.

Sagem Défense Sécurité a défini un processus de modélisation d'architecture système basé sur les modèles SysML et l'a mis en œuvre au travers des outils Papyrus [2] et SCADE System [3]. Le processus proposé permet globalement de représenter les différents points de vue souhaités par nos architectes systèmes (points de vue opérationnels, fonctionnels, organiques). Des souhaits d'évolutions ergonomiques dans le but d'améliorer la productivité lors de la création des objets modélisés ont été émis.

Un processus de support aux échanges entre les métiers « architecture système » et « sûreté de fonctionnement » a été défini. Afin de tester sa mise en œuvre au travers d'une suite outillée, un couplage entre SCADE System™ [3] d'Esterel Technologies et l'outil Safety Architect [4] de la société All4Tec a été proposé.

Un maquettage de ce couplage a été effectué. Les blocs et les liens d'entrées/sorties définis dans SCADE System sont bien récupérés dans Safety Architect mais il a été constaté que la gestion des évolutions entre les deux outils devait être améliorée. Le processus, lui-même, doit être

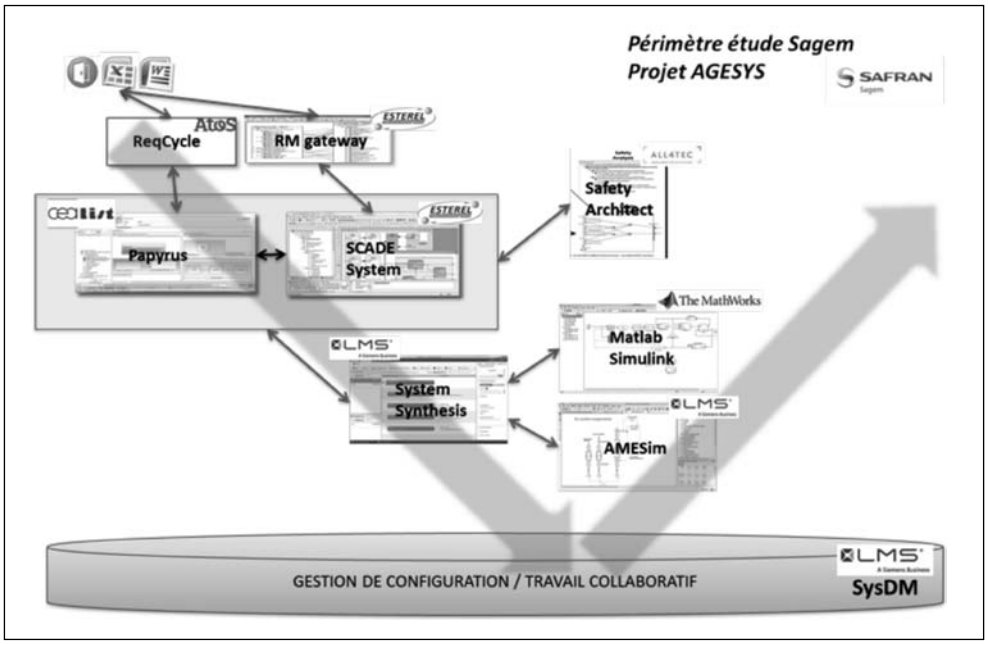

Figure 1 : Présentation de la suite outillée de Sagem

approfondi. Des travaux sur cette thématique pourraient être démarrés dans le cadre de la chaire Blériot-Fabre[1].

Afin de compléter l'évaluation de l'atelier, Sagem a également analysé les besoins et les opportunités de génération documentaire de façon automatique et de gestion des liens de traçabilité entre modèles et exigences. De plus, la mise en œuvre d'un maquettage de co-simulation avec un couplage AMESim-Simulink au travers de SysDM/ System Synthesis a permis de valider cette méthode.

Les résultats obtenus sont tout à fait encourageants et ont fait l'objet d'une diffusion dans le Groupe Safran à travers la société Safran Tech, responsable pour Safran de la centralisation des réflexions amont et des spécifications relatives à la définition d'ateliers de génie système.

Ces travaux s'inscrivent également dans le cadre de l'investissement de Sagem Défense Sécurité dans les initiatives tels que le groupe Embedded France NSL **« Normes pour la Sûreté de fonctionnement Logiciel et système », qui a été créé sous le nom «** Normes et Standards, Sûreté de fonctionnement et Certification » par le CGEE en 2008. Le but de ce groupe est de décloisonner la réflexion, d'identifier les similitudes et les différences entre les normes industrielles et de comprendre leurs justifications. Ces échanges entre experts, acteurs importants de la rédaction de ces normes dans leurs domaines respectifs, permettront à terme de dépasser ces différences, quand c'est possible et justifié.

Références

[1] Thierry Le Sergent et Eric Bantegnie **:** *AGeSYS* **: un environnement d'ingénie***rie système pour le développement et la vérification de systèmes embarquées* ; Génie Logiciel, n° 106, pages 12-15, 19, septembre 2013.

[2] Vincent Lorenzo, Rémi Schnekenburger, Yann Tanguy, Patrick Tessier et Sébastien Gérard : *L'outil de modélisation graphique MDT::Papyrus* **: état actuel et perspectives** ; Génie Logiciel, n° 97, pages 47-52, juin 2011.

[3] Thierry Le Sergent, Alain Le Guennec, Luc Coyette, François-Xavier Dormoy et Bernard Dion : *Intégration des activités d'ingénierie système et logiciel* ; Génié Logiciel, n° 102, pages 46-52, octobre 2012.

[4] Jonathan Dumont, Franck Sadmi et Frédérique Vallée : *Safety Architect*© **: un outil d'analyse de risques s'inscrivant dans le processus d'ingénierie de systèmes complexes ; Génie Logiciel, n° 98, pages 27-33, septembre 2011.**

Biographies

Philippe Baufreton est expert senior en charge de la prospective pour les logiciels embarqués et les architectures au sein de la Division SAFRAN Electronics de Sagem à Massy. Il est membre du groupe NSL « Normes pour la Sûreté de fonctionnement Logiciel et système ».

Jean-Claude Derrien est Directeur Technique R&T – Flight Control Systems - de la Division Avionique de Sagem. A ce titre, il a également piloté dans les sept dernières années le pôle de Compétences du Groupe SAFRAN SEED « Safran Embedded Engineering Development ».

Marc Malot, au sein du service « méthodologie système » de Sagem, est responsable de projets R&T visant à améliorer les processus d'ingénierie système (ingénierie des exigences, ingénierie basée sur des modèles, méthode avancée de vérification et de certification). À ce titre, il a piloté les activités Sagem au sein du projet AGeSys.

1 La chaire Blériot-Fabre « Systèmes embarqués robustes, de la conception à l'architecture » commune à Centrale Paris, Supélec et Safran a été officiellement inaugurée le 12 décembre 2013. Antoine Rauzy, directeur de la Chaire et professeur *au laboratoire Génie Industriel* de Centrale Paris, a donné une leçon inaugurale sur le thème « Des modèles de l'ingénierie à l'ingénierie des modèles ».