Une approche pour la vérificationdes propriétés et des comportements d'un Système de Systèmes (SdS)

Mustapha Bilal, Nicolas Daclin, Vincent Chapurlat
ENS Mines Alès, France
{firstname.lastname}@mines-ales.fr

Un système de systèmes (SdS) est un système complexe (Chapman et Bahill, 1995) basé sur la collaboration et l'interaction entre des sous-systèmes existants (technique ou sociotechnique) afin de remplir une mission commune pour une durée éventuellement limitée (coalition militaire, système de transport aérien, réseau d'entreprises, etc.). La conception ou la re-conception d'unSdSse distingue de la conception classique des systèmes (Blanchard *et al*., 2010). En effet, des systèmes, existant pour la majorité d'entre eux, sont sélectionnés en fonction de leur pertinence, capacités et intérêt propre à la réalisation de la mission visée. Ils sont ensuite assemblés en respectant les exigences des parties prenantes du SdS pour que leur interaction permette de remplir cette mission. Lors de cet assemblage, des interfaces sont requises qu'elles soient physiques (matérielles), informationnelles (modèle et protocoles d'échanges de données) ou organisationnelles (règles, procédures et protocoles) afin d'assurer la nécessaire interopérabilité (Mallek *et al*., 2012) des sous-systèmes. En effet, leur comportement, leur autonomie décisionnelle ou leur organisation propre ne doivent pas être impactés plus que nécessaire, de manière plus ou moins définitive voire risquée, par d'éventuels effets indésirables résultant de l'interaction entre ces sous-systèmes. De fait, le comportement résultant du SdS n'est pas nécessairement celui attendu du fait de l'émergence de comportements imprévisibles dû à ces interactions (Maier 1998). De même, certaines propriétésdu SdS ne peuvent pas être directement déduites de l'ensemble des propriétés de ses sous-systèmes. Les concepteurs d'un SdS sont donc confrontés à un enjeu de taille : comment mieux maitriser ces comportements et ces propriétés dans un temps relativement court, sans un effort supplémentaire et de nécessaires connaissances en termes de modélisation à la fois des scénarios comportementaux émergents et des propriétés ?

Le projet de recherche présenté dans cette communication se concentre sur le rôle conjoint et complémentaire que peuvent jouer des techniques de vérification différentes. L'objectif de ces travaux est d'assurer et par la suite améliorer en «temps réel de conception» i.e. dès les premiers stades de la conception architecturale et des interfaces (Dhillon, 1987), la vérification de l'architecture et du comportement d'un SdS, indépendamment de la nature, de la taille ou de la complexité des sous-systèmes qui le composent.

Il s'agit, d'une part, de techniques de formalisation, à partir des exigences formulées par les parties prenantes, puis de preuve de propriétés sur un modèle décrivant l'architecture du SdS. Il s'agit ensuite d'une technique avancée de simulation du comportement de cette architecture permettant d'atteindre deux buts :

1- Mettre en place une approched'évaluation de plusieurs caractéristiques de type non-fonctionnelles (De Weck et al. 2012) comme proposé dans le cas de l'ingénierie de SdS par (Blanchard *et al*., 2010) ou de systèmes (SeBok 2012)(ISO 2008) en répondant aux hypothèses et principes du Model Based System Engineering (MBSE) (Estefan 2007). Nous retenons ici en particulier la caractéristique de robustesse de l'architecture du SdS. La robustesse est définie ici comme l'agrégation de sa capacité à assurer sa stabilité (il reste apte à assurer sa mission malgré les différents phénomènes d'émergence et des événements externes qui menacent son comportement), son intégrité (il reste apte à remplir sa mission malgré les différents phénomènes d'émergence et des événements internes provoquant des

dysfonctions plus ou moins redoutées de ces sous-systèmes) et son pilotage (il reste apte à maximiser ses performances).

2- Faciliter la détection de possibles erreurs, incertitudes ou omissions et de juger de la plausibilité et de la crédibilité de comportements considérés comme inattendus mais apparaissant au cours de la simulation.

Ce travail doit aboutir à la proposition d'un cadre de modélisation de l'architecture d'un SdS basé sur une formalisation mathématique sous-jacente du concept de SdS. Cela permettra l'emploi de la technique de formalisation et de preuve de propriétés ainsi que la formalisation des caractéristiques non-fonctionnelles essentielles attendues dans un SdS. Ce cadre sera ensuite doté d'une sémantique opérationnelle et de règles de transformation formelles vers un Système Multi-Agents (SMA) (Wooldridge 2009) permettant de simuler le comportement des sous-systèmes composant l'architecture et de caractériser la plausibilité et la crédibilité des comportements alors constatés en cours de simulation sans avoir besoin de préciser des scénarios d'évolution du SdS au préalable.Un SMA est, en effet, une solution efficace et éprouvée pour faire face à des situations complexes dans des environnements distribués (Khosla et Dillon 1997).Il permet de modéliser et de simuler,indépendamment, l'évolution parallèle et les interactions de différentes entités complexes ici les sous-systèmes du SdS(Brandolese*et al*., 2000). En outre, le SMA peut répondre à l'échec individuel de l'un deses éléments sans dégrader le système dans son ensemble et, par conséquent, est capable d'aider à détecter ce type de comportement. Enfin, la technologie BDI (Rao1995) (Beliefs, Desire, Intention)employée dans certains SMApermet de modéliser plus finement des connaissances et des règles de comportement devant être exhibées par les agents modélisant chaque sous-système. Des environnements de modélisation et de simulation pour la conception de systèmes complexes ont été proposés (ID4CS 2009). Ils sontréservés à des domaines particuliers (l'aéronautique par exemple) et ils ne permettent pas d'adresser d'autres types de SdS.

La structure du modèle Multi-Agents retenue pour modéliser l'architecture du SdS est définie selon quatre dimensions (figure 1) : les modèles d'Agents, les modèles d'Environnement, les modèles d'Interaction et les modèles d'Organisation (Demazeau 1995) :

1. Les modèles d'Agents : Ces modèles représentent les agents, dans notre cas, les sous-systèmes. Etant donné que les sous-systèmes pourraient être des natures différentes, il est nécessaire d'avoir différents types d'agents, tels que : les Agents intentionnels (Rao 1995), les Agents rationnels (Russel 1991) et les Agents situés (Agre 1987) (Maes, 1990).
2. Les modèles d'Environnement : Le SdS (ainsi que les sous-systèmes) se trouvent dans un environnement avec lequel ils interagissent. Cet environnement représente l'espace commun entre les sous-systèmes définis précédemment. Il est actif et il réalise la médiation des interactions entre les sous-systèmes (agents) d'une part, et entre les sous-systèmes et les ressources d'autre part.
3- Les modèles d'Interaction : Comme précisé précédemment, les sous-systèmes entrent en interaction ensemble afin de remplir la mission duSdS pour une durée éventuellement limitée. Les modèles d'interaction gèrent cette interaction en définissant et structurant la liaison dynamique de deux ou plusieurs Agents à travers un ensemble d'actions réciproques sur cette durée. Ces modèles définissent également les langages de communication (KQML, ACL, etc.) et les protocoles d'interaction qui gèrent cette communication.
4- Les modèles d'Organisation : Ils définissent les contraintes sur les modèles d'interaction. Autrement dit, ils précisent comment les Agents doivent coopérer afin d'atteindre un but. Ces contraintes sont définies soit par le concepteur soit par les agents eux-mêmes. Parmi ces contraintes, nous pouvons citer : les normes, les obligations, les permissions, les lois, etc. Un

modèle d'organisation est basé sur des sources sociologiques, physiologiques, sociales et Computer-SupportedCooperativeWork (CSCW).

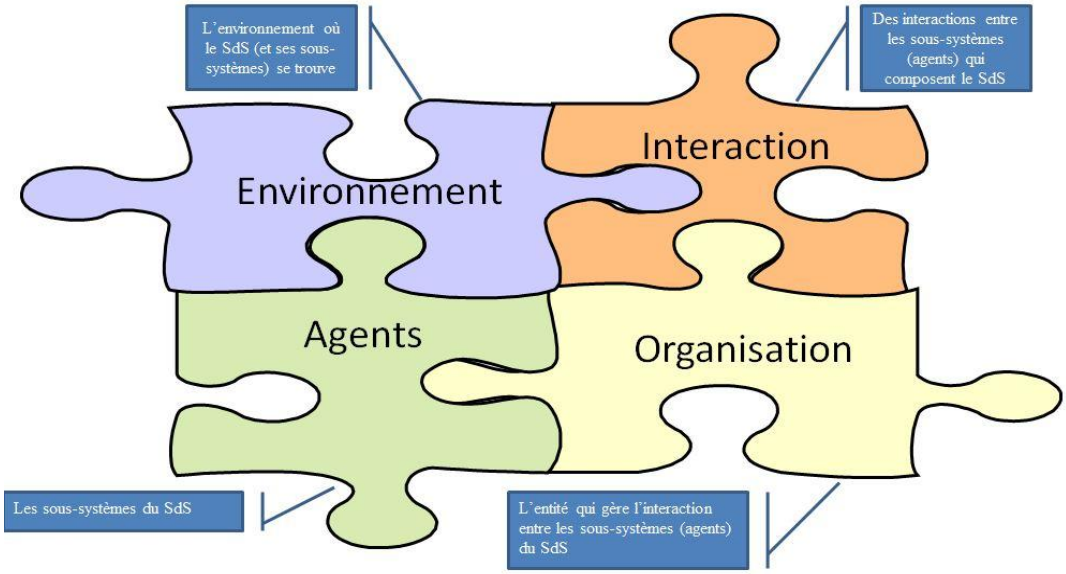

Figure 1: Structuration d'un modèle MA spécifique à un SdS

REFERENCES

(Agre 1987) Agre, P. E. and D. Chapman (1987)." Pengi: An Implementation of a Theory of Activity" . AAAI-87. The Sixth National Conference on Artificial Intelligence, Menlo Park, CA., Morgan Kaufman, Los Altos, CA

(Blanchard *et al*., 2010) Systems Engineering and Analysis by Benjamin S. Blanchard, Wolter J. Fabrycky 2010

(Brandolese, 2000) Brandolese A., Brun A., Portioli-Staudacher A., "A Multi-Agent approach for the capacity allocation problem" International Journal of Production Economics, Vol. 66, pp. 269-285, 2000.

(Chapman etBahill, 1995) Chapman, W.L., Bahill, A.T.: Complexity of the system design problem.

(Demazeau 1995) Y.Demazeau: From interactions to collective behaviour in agent-based systems.In Proc. of the 1st European Conf. on Cognitive Science, Saint Malo, France, April, 1995, p. 117-132

(Dhillon,1987) Dhillon, B, S.: Reliability in Computer System Design. Alex Publishing Corporation (1987)

(Estefan 2007)Estefan, J.A., « Survey of Model-Based Systems Engineering (MBSE) Methodology ». INCOSE MBSE Focus Group Report, 2007

(ID4CS 2009) ANR project 2009, see http://www.irit.fr/ID4CS

(Khosla et Dillon 1997) R. Khosla, T. Dillon, "Intelligent hybrid multi-agent architecture for engineering complex systems," Proceedings of the 1997 IEEE international Conference on Neural Networks, vol. 4,pp. 2449-2454

(Maes 1990) Maes, P. (1990). "Situated Agents Can have Goals." Designing Autonomous Agents .Maes, P. (Ed.). Cambridge, MA., MIT Press: 49-70

(Maier 1998) Maier, M.W.: Architecting principles for systems-of-systems. Systems Engineering 1(4) (1998) 267-284

(Malleke*t al*., 2012)The application of interoperability requirement specification and verification tocollaborative processes in industry

(Rao 1995) A. S. Rao and M. P. Georgeff, BDI-agents: from theory to practice, Proceedings of the First

Intl. Conference on Multiagent Systems, 1995

(Russel 91) Stuart Russell and Eric Wefald. Do The Right Thing. The MIT Press, Cambridge, Massachusetts, 1991

(Sebok 2012) http://www.sebokwiki.org (dernier accès le 23/04/2013)

(De Weck*etal*. 2012) Olivier L. de Weck, Adam M.Ross, Donna H. Rhodes, Investigating Relationships and Semantic Sets amongst System Lifecycle Properties (-ilities), third International Engineering Systems Symposium CESUN 2012, Delft University of Technology, 18-20 June 2012

(Wooldridge and al., 1995) Wooldridge M., Jennings N., Intelligent Agents: Theory and Practice, Knowledge Engineering Review, 1995.

(Wooldridge 2009) An introduction to Multi-agent Systems (2009)