Building Robust Systems with Fallible Construction

(RTO-MP-IST-064)

Executive Summary

Today's NATO military commanders depend on large, complex software systems that must be more predictable and trustworthy than traditional development methods can deliver for the available time and cost investments. This requirement is not quite compatible with the traditional software development that is prevalent in today's military acquisition methods. Today's systems are typically integrated from components that may themselves contain flaws, originating in specification, design or implementation errors, or in miscommunication between different teams involved in the development. "System of Systems", where components are systems in and of themselves, are a significant factor. More seriously, the integration process itself may be flawed. This situation can arise in the NATO context, for instance, when coalitions are formed quickly, and complex systems must be integrated from subsystems supplied by different nations.

The workshop was organized to review past and present understanding of the challenge, as well as examining relevant approaches to address them. Rather than an exchange of pre-prepared material, the workshop was intended as a working meeting with a goal of producing a deliverable that is a summary of the state of the art.

The workshop topic is related to Software Fault Tolerance, a topic that has been studied at least since 1970. Worldwide much has been learned about how to address those problems, as they were understood at the time. However changes in perspective as to what constitute the challenges, and changes in available and commonplace technology, have led to a need to go beyond conclusions reached in the past.

The proceedings include position statements from the participants, slides from the presentations made by the participants, and the one complete paper that was submitted. Minutes of the discussions provide insight into how the deliverable, the final report of task group IST-047/RTG-019, was shaped.

Bâtir des systèmes sûrs à partir de constructions faillibles

(RTO-MP-IST-064)

Synthèse

Aujourd'hui, les commandants militaires de l'OTAN sont tributaires de systèmes logiciels importants et complexes qui doivent être plus prévisibles et dignes de confiance que ce que peuvent produire les méthodes de développement traditionnelles compte tenu du temps disponible et des coûts d'investissement. Ces impératifs ne sont pas vraiment compatibles avec le développement traditionnel des logiciels qui prévaut actuellement dans les méthodes militaires d'acquisition. Actuellement, les systèmes sont en général intégrés à partir de composants qui peuvent contenir des imperfections provenant des spécifications, d'erreurs de fabrication ou de mise en œuvre, ou d'une mauvaise communication entre les différentes équipes impliquées dans le développement. Les « systèmes de systèmes », dont les composants sont eux-mêmes des systèmes dans le système en sont un élément significatif. Plus sérieusement, le processus d'intégration peut être lui-même défectueux. Cette situation peut advenir dans un cadre OTAN, par exemple quand les coalitions sont formées rapidement et quand des systèmes complexes doivent être intégrés à partir de sous-systèmes fournis par différentes nations.

L'atelier a été organisé pour passer en revue les façons passées et présentes d'appréhender les enjeux mais aussi pour examiner les approches pertinentes pour les aborder. Plutôt que d'échanger des éléments préparés à l'avance, l'atelier a été voulu comme une réunion de travail avec pour but de produire un résumé de ce qu'est l'état de l'art dans le domaine.

Le thème de l'atelier concernait la limite de tolérance acceptable aux défauts des logiciels, sujet étudié depuis au moins 1970. Dans le monde entier, on a beaucoup appris sur la façon de traiter ces problèmes, tels qu'on les appréhendait à l'époque. Cependant, les changements de perspective sur ce qui constitue les enjeux et les évolutions de la technologie disponible courante, ont rendu nécessaire d'aller au delà des conclusions retenues par le passé.

Les rapports contiennent l'exposé des positions des participants, les diapositives des présentations faites par ces participants et le document complet unique qui a été proposé. Les minutes des débats donnent une vision interne de la façon dont le produit délivré, compte-rendu final du groupe opérationnel IST-047/RTG-019 a été élaboré.