
Building Robust Systems with Fallible Construction

(RTO-TR-IST-047)

Executive Summary

This is the final report of the Task Group IST-047/RTG-019 on “Building Robust Systems with Fallible Construction”.

The general area of study that the task group was to investigate 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 go beyond conclusions reached in the past.

Today’s systems are typically integrated from components. These components may themselves contain flaws, originating in specification, design or implementation errors, or in miscommunication between different teams involved in the development. More seriously, the integration process itself may be flawed, as when pre-existing components are used for purposes their developers had not envisioned, and the integrators misunderstand the detailed behaviour of the components. Interoperability of systems is more complex than correctness of a single system by itself. We have come to recognize that systems-of-systems have emergent behaviour, because the constituent subsystems were not only never designed as part of an integrated whole, they may actually be procured, owned and operated by independent organizations and have operational demands for results not encompassed within, or even aligned to, the objectives of the super-system itself. Components, and especially subsystems, often have an evolutionary life cycle independent of the life cycle of any system they are incorporated in: what may have been true at some point in time is not guaranteed to remain true in the future.

The Task Group focused on identifying challenges that have not been adequately resolved by traditional Software Fault Tolerance. The Task Group did not have the resources to itself undertake research to produce solutions, but felt that producing a catalogue of issues requiring further investigation was a useful first step leading to their eventual resolution, and in itself was a worthwhile contribution.

Today’s NATO military systems depend on large, complex software with the need to be built and deployed more rapidly and cheaply than traditional development methods can deliver. Moreover, because military commanders depend on these systems, they must be more predictable and trustworthy than traditional development methods can deliver for the available time and cost investments.

Elaboration de systèmes informatiques robustes à l'architecture faillible (RTO-TR-IST-047)

Synthèse

Ceci est le compte-rendu final du groupe de travail IST-047/RTG-019 sur « Elaboration de systèmes informatiques robustes à l'architecture faillible ».

Le domaine général sur lequel le groupe de travail a travaillé concerne la tolérance logicielle aux pannes, sujet étudié depuis au moins 1970. Partout dans le monde, beaucoup a été fait à l'époque pour résoudre ces problèmes.

Toutefois, des changements de perspective sur les défis que cela représente et les changements technologiques courants disponibles, ont abouti à la nécessité d'aller au-delà des conclusions passées.

De nos jours, dès les composants, les systèmes sont intégrés. Ces composants peuvent en eux-mêmes avoir des défauts, qui trouvent leur source dans les caractéristiques, la conception, les erreurs de mise en œuvre, ou une mauvaise compréhension entre les équipes de développement. Plus sérieusement, l'intégration elle-même peut être entachée d'erreurs, comme lorsque des composants déjà existants servent à des fins non prévues par les développeurs, sans parler des intégrateurs qui comprennent mal le comportement spécifique de ces composants. L'interopérabilité des systèmes est plus complexe que l'exactitude d'un seul système en lui-même. Il nous faut bien reconnaître que des systèmes-de-systèmes ont des comportements surprenants, car leurs sous-systèmes n'ont pas été conçus comme partie intégrante d'un tout. Ils peuvent même être achetés, détenus ou exploités par des organisations indépendantes, et être soumis à des exigences d'exploitation non comprises dans ou même alignées sur les objectifs du super-système lui-même. Les composants, et particulièrement les sous-systèmes, ont un cycle de vie autonome, indépendant du cycle de vie du système dans lequel ils sont incorporés : il est nullement garanti que ce qui a pu être vrai à un moment donné dans le temps le sera à l'avenir.

Notre groupe de travail s'est concentré sur l'identification des défis qui n'ont pas été résolus correctement par la traditionnelle tolérance logicielle aux pannes. Notre groupe n'avait pas les ressources pour lui-même rechercher les solutions, mais il a pensé que produire une liste des problèmes nécessitant des investigations plus poussées était une étape utile conduisant à leur résolution éventuelle, et en lui-même une contribution qui en valait la peine.

De nos jours les systèmes militaires de l'OTAN dépendent de gros programmes complexes, qui doivent être élaborés et déployés plus rapidement, encore moins chers que les méthodes traditionnelles de développement n'en sont capables. En outre, comme des commandants militaires dépendent de ces systèmes, ces derniers doivent être plus prévisibles et fiables que les méthodes traditionnelles de développement ne le permettent à ce jour en fonctions des investissements.