Comment construire une argumentation pour la certification ou la mise en conformité de systèmes

Jean-Michel Bruel, IRIT, Université de Toulouse, Toulouse
Rémi Delmas, Uber Advanced Technology Center, Paris
Régine Laleau, Université Paris-Est Créteil, LACL, Créteil
Thomas Polacsek, ONERA, Toulouse
Florence Sedes, IRIT, Université de Toulouse, Toulouse

1 Contexte

Depuis de nombreuses années, nous avons vu le développement et l'usage des méthodes formelles pour garantir des propriétés sur des systèmes. Cependant, l'utilisation de méthodes formelles ne nous ôte pas de certains doutes. Considérons que nous disposons de la preuve mathématique de la correction d'un artefact, sommes-nous sûrs que cette preuve ne contienne pas elle-même des erreurs ? Si elle a été établie par une machine, sommes-nous sûrs que le programme utilisé est lui aussi prouvé ? Nous pouvons ainsi remettre en question tous les éléments, chercher des preuves aux preuves, sans jamais trouver de fin à nos questionnements. Nous sommes typiquement face au problème épistémologique de la régression infinie. Loin d'être un problème purement philosophique, le problème de la confiance dans les moyens utilisés pour établir la preuve de correction se pose cruellement dans le monde de l'ingénierie en général et, plus particulièrement, dans le cadre de la certification. En effet, toute la démarche visant à certifier un artefact n'a qu'un seul but : prévenir les erreurs. Il est donc crucial que les moyens utilisés ne soient pas eux-mêmes entachés d'erreurs ou, tout au moins, que nous ayons confiance en eux.

Nous pouvons simplifier la certification en considérant qu'il s'agit de « savoir si un artefact est correct ». Dans ce contexte, la preuve formelle n'est qu'un élément parmi d'autres permettant d'établir cette connaissance. Comme le souligne Tony Hoare dans son article de 1996 « How Did Software Get So Reliable Without Proof ? » , ce n'est pas grâce à l'utilisation de méthodes formelles que les logiciels sont devenus plus fiables, mais par l'usage de techniques déjà employées dans les autres branches de l'ingénierie comme : des procédures rigoureuses de relecture des spécifications de conceptions, l'assurance qualité fondée sur de larges éventails de tests ou de l'amélioration continue. Dès lors, comment, à partir de ces éléments informels, être sûr que l'artefact final est correct ?

Le problème qui nous préoccupe ici est en fait un problème d'inférence. Nous cherchons à déterminer s'il est acceptable ou pas de passer d'un ensemble de justifications à une conclusion. Pour être plus précis, nous visons l'étude des documentations techniques qui permettent la certification d'artefacts. Nous trouvons ce type de documents, par exemple, dans le domaine de l'évaluation des risques et de la fiabilité des systèmes critiques sous le nom de safety case ou d'assurance case. Le safety case est un document structuré qui fournit une justification et des arguments valables sur le fait qu'un système satisfait des propriétés relatives à sa sécurité.

Parallèlement, hors de la sphère de la certification, depuis quelques années, nous voyons émerger le besoin de démontrer la conformité d'un système par rapport à une norme. En effet, qu'il s'agisse de sécurité ou de protection des données et de la vie privée, les systèmes doivent de plus en plus se conformer à un nombre croissant de réglementations. Ce besoin de conformité à de nouvelles règles, comme le nouveau règlement général sur la protection des données de l'Union Européenne, implique des changements techniques profonds. Ces règles doivent non seulement être prises en compte par les systèmes, mais il est également nécessaire de démontrer qu'un système s'y conforme. Par conséquent, nous devons prendre en compte deux aspects : premièrement, veiller à ce qu'un système soit conforme à un règlement et, deuxièmement, faire en sorte que les moyens de mise en conformité soient accessibles à tous.

2 Problématique

Ce défi se positionne à la convergence de ces deux problématiques que sont la certification et la conformité à un règlement. Dans les deux cas, il est nécessaire d'identifier les exigences propres à ce besoin de convaincre une autorité. En ce qui concerne le respect d'une réglementation, faire valoir qu'un système est conforme à une norme, il faut tout d'abord identifier les exigences résultant de ce règlement. De plus, dans le contexte d'un système préexistant, il peut être utile d'effectuer une étude d'impact réglementaire sur un système. Il est à noter que cette articulation entre le texte d'un règlement (une norme, une loi, etc.), qui tend à définir des objectifs de haut niveau, et un système est commun dans le monde de la certification, qui est également basé sur des normes. Par ailleurs, il est aussi important de s'intéresser à la structuration de l'argumentation qu'elle relève de la certification ou de la conformité à un règlement. Dans les deux cas, en portant notre attention sur les aspects justification, nous opérons un glissement du raisonnement déductif, de la preuve logique, vers une forme de raisonnement plus informel. Cet aspect informel ne doit pas nous arrêter dans notre démarche. En effet, il nous semble possible de dégager des structures permettant de capturer la rationalité de telles argumentations et de définir des approches pour prévenir les raisonnements fallacieux.

3 Challenges identifiés

— comment exprimer les exigences relatives à une norme, un standard, une réglementation ?
— comment relier ces exigences aux exigences fonctionnelles et non fonctionnelles (i.e. sécurité et sûreté) d'un système
— comment s'assurer qu'un système est conforme à une réglementation ?
— comment un système d'information peut aider un processus d'argumentatif ?
— comment renforcer, d'un point de vue argumentatif, la complémentarité entre preuves, tests et simulations ?
— quels formalismes d'argumentation et de méthodes pour une approche incrémentale de la mise au point et de la certification des systèmes ?
— modularité, réutilisation, analyses d'impact ?
— la plupart des outils existants d'argumentation sont graphiques et difficlement utilisables pour des gros projets industriels, comment développer des interfaces utilisateurs pour la saisie et la navigation d'argumentations complexes ?