Uncertain Requirements, Assurance and Machine Learning

Title	Uncertain Requirements, Assurance and Machine Learning
Publication Type	Conference Paper
Year of Publication	2019
Authors	Chechik, Marsha
Conference Name	2019 IEEE 27th International Requirements Engineering Conference (RE)
Keywords	assurance, assurance case, automotive, composability, conventional machine-learned, deductive verification, feature extraction, financial data processing, financial services, formal verification, governing bodies, human judgement, inductive assurance, learning (artificial intelligence), linked evidence, machine learning, machine-learned components, machine-learning, Ontologies, open-world functionality, pragmatic assurance, predefined requirements, privacy, pubcrawl, requirements engineering, Safety, safety assessment, safety-critical domains, safety-critical software, Scalability, security, social networking (online), social networks, Software, software assurance, software construction, Software development, software engineering, Standards organizations, uncertain requirements, Uncertainty, vehicle control, verification proofs

Abstract

From financial services platforms to social networks to vehicle control, software has come to mediate many activities of daily life. Governing bodies and standards organizations have responded to this trend by creating regulations and standards to address issues such as safety, security and privacy. In this environment, the compliance of software development to standards and regulations has emerged as a key requirement. Compliance claims and arguments are often captured in assurance cases, with linked evidence of compliance. Evidence can come from testcases, verification proofs, human judgement, or a combination of these. That is, we try to build (safety-critical) systems carefully according to well justified methods and articulate these justifications in an assurance case that is ultimately judged by a human. Yet software is deeply rooted in uncertainty making pragmatic assurance more inductive than deductive: most of complex open-world functionality is either not completely specifiable (due to uncertainty) or it is not cost-effective to do so, and deductive verification cannot happen without specification. Inductive assurance, achieved by sampling or testing, is easier but generalization from finite set of examples cannot be formally justified. And of course the recent popularity of constructing software via machine learning only worsens the problem - rather than being specified by predefined requirements, machine-learned components learn existing patterns from the available training data, and make predictions for unseen data when deployed. On the surface, this ability is extremely useful for hard-to specify concepts, e.g., the definition of a pedestrian in a pedestrian detection component of a vehicle. On the other, safety assessment and assurance of such components becomes very challenging. In this talk, I focus on two specific approaches to arguing about safety and security of software under uncertainty. The first one is a framework for managing uncertainty in assurance cases (for "conventional" and "machine-learned" systems) by systematically identifying, assessing and addressing it. The second is recent work on supporting development of requirements for machine-learned components in safety-critical domains.

DOI 10.1109/RE.2019.00010

Citation Key chechik_uncertain_2019

security Safety Ontologies Software feature extraction learning (artificial intelligence) machine learning pubcrawl composability social networking (online) social networks uncertainty privacy software engineering software development assurance safety-critical software Scalability formal verification assurance case automotive conventional machine-learned deductive verification financial data processing financial services governing bodies human judgement inductive assurance linked evidence machine-learned components machine-learning open-world functionality pragmatic assurance predefined requirements requirements engineering safety assessment safety-critical domains software construction Standards organizations uncertain requirements vehicle control verification proofs software assurance