NC STATE UNIVERSITY

North Carolina State University is land-grant university and a constituent institution of North Carolina

Campus Box 8206/3298 EB2,
Raleigh, NC, 27695-8206
304. 376. 2859 (phone)
timm@ieee.org (e-mail)

Jan 12, 2022

From the desk of Prof. Tim Menzies[1]

Ideas for SANDIA Labs (Jan 2023)

Computing and Information Sciences (CIS)

- *Trusted Artificial Intelligence:* Consider the case where some capability is built as **an assembly of web-based models**. Those other models may not be documented sufficiently to test them using standard technologies. In "Defeating Malicious Explanation" I work with high-level explanation algorithms to try and **tune the models**, without letting model owners deceive me about the capabilities of their models. There are many extensions that could follow from that work including:
  - apply those methods to much **higher dimensional data**
  - apply the ideas across **more liar algorithms**
- *Human-Machine Teaming to Enable Decision Making: I propose a new method of* "stakeholder testing" which says that when **teams combine** to review and improve a model, they must work at a **much higher level** than standard software introspection. For that work I am exploring **semi-supervised multi-objective explanation algorithms**.

Cyber Innovation (CYBER)

Software Systems Understanding: Assurance and vulnerability research of software system purpose, capability, flaws, communication and data processing and storage. Techniques that advance static or dynamic analyses are encouraged.

- In Faster Multi-Goal Simulation-Based Testing for CyberPhysical Systems I explore how to reduce the cost of testing cyberphysical systems. The next steps in that work would be to:
  - Generate tests using background knowledge from **generative language models.** So here, we need not assume ChatGPT is correct—only that **it is saying things that might apply** (and might be wrong) in the current system,
  - Explore multi-goal metamorphic testing. Current state-of-the-art in that area struggles with the optimization task within their overall method. Using novel optimizers (based on semi-supervised

[1] Tim Menzies. IEEE Fellow, full professor, NC State, computer science, timm@ieee.org. Prof. Tim Menzies (IEEE Fellow, Ph.D., UNSW, 1995) is a full Professor in CS at North Carolina State University where he teaches software engineering, automated software engineering, and foundations of software science. He is the director of the RAISE lab (real world AI for SE) and the author of over 280 publications (refereed). In his career, he has supervised 20 Ph.D. students, and has been a lead researcher on projects for NSF, NIJ, DoD, NASA, USDA (total funding of $13+ million) as well as joint research work with private companies. Also, Prof. Menzies is the editor-in-chief of the Automated Software Engineering journal and associate editor of TSE (IEEE Transactions on Software Engineering) and other leading SE journals.

learning), it would be possible to **dramatically reduce the cost** of testing a cyberphysical system even when t**here is only minimal knowledge available** on the purpose of that system.

New Ideas (NI)

- In Fairer Software Made Easier (using "Keys") I explore the **implications of the manifold assumption** for software development. If many systems can be approximated in a lower dimensional space, then much of what we do in software development can be simplified (by working in that lower dimensional space). But what about things that are truly complex? **Do complex systems have some simpler parts** that can be built and tested much more easily? And **how does the complex talk to the simpler** (and vice versa)?. These are all open and interesting research directions.