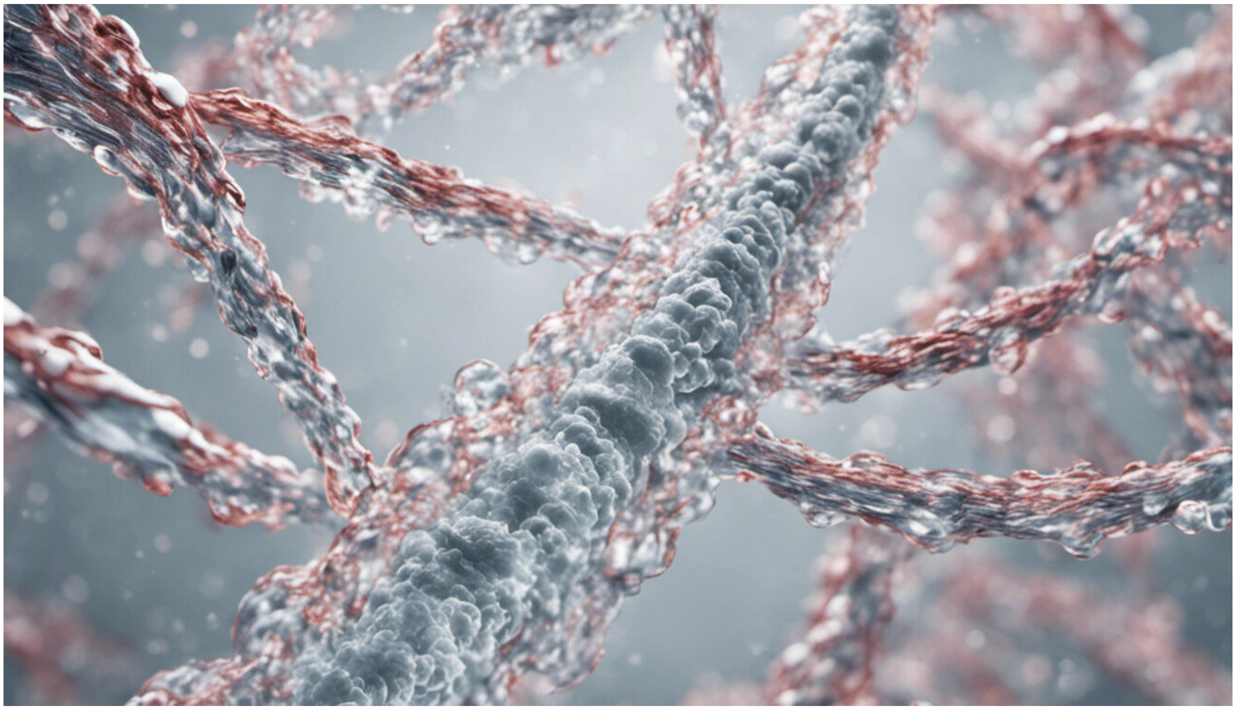
NIST tool enables more comprehensive tests on high-risk software

April 24 2019



Credit: AI-generated image (disclaimer)

We entrust our lives to software every time we step aboard a high-tech aircraft or modern car. A long-term research effort guided by two researchers at the National Institute of Standards and Technology (NIST) and their collaborators has developed new tools to make this type of safety-critical software even safer.

Augmenting an existing software toolkit, the research team's new creation can strengthen the safety tests that software companies conduct on the programs that help control our vehicles, operate our power plants and manage other demanding technology. While these tests are often costly and time-consuming, they reduce the likelihood this complex code will glitch because it received some unexpected combination of input data. This source of trouble can plague any sophisticated software package that must reliably monitor and respond to multiple streams of data flowing in from sensors and human operators at every moment.

With the research toolkit called Automated Combinatorial Testing for Software, or ACTS, software companies can make sure that there are no simultaneous input combinations that might inadvertently cause a dangerous error. As a rough parallel, think of a keyboard shortcut, such as pressing CTRL-ALT-DELETE to reset a system intentionally. The risk with safety-critical software is that combinations that create unintentional consequences might exist.

Until now, there was no way to be certain that all the significant combinations in very large systems had been tested: a risky situation. Now, with the help of advances made by the research team, even software that has thousands of input variables, each one of which can have a range of values, can be tested thoroughly.

NIST's ACTS toolkit now includes an updated version of Combinatorial Coverage Measurement (CCM), a tool that should help improve safety as well as reduce software costs. The software industry often spends seven to 20 times as much money rendering safety-critical software reliable as it does on more conventional code.

The peer-reviewed findings of the research team appear in two papers the team will present on April 23 at the 2019 IEEE International Conference on Software Testing, Verification and Validation in Xi'an, China. The research includes collaborators from the University of Texas at Arlington, Adobe Systems Inc. and Austria's SBA Research.

NIST mathematician Raghu Kacker said that CCM represents a substantial improvement to the ACTS toolkit since its last major addition in 2015.

"Before we revised CCM, it was difficult to test software that handled thousands of variables thoroughly," Kacker said. "That limitation is a problem for complex modern software of the sort that is used in passenger airliners and nuclear power plants, because it's not just highly configurable, it's also life critical. People's lives and health are depending on it."

Software developers have contended with bugs that stem from unexpected input combinations for decades, so NIST started looking at the causes of software failures in the 1990s to help the industry. It turned out that most failures involved a single factor or a combination of two input variables—a medical device's temperature and pressure, for example—causing a system reset at the wrong moment. Some involved up to six input variables.

Because a single input variable can have a range of potential values and a program can have many such variables, it can be a practical impossibility to test every conceivable combination, so testers rely on mathematical strategy to eliminate large swaths of possibilities. By the mid-2000s, the NIST toolkit could check inputs in up to six-way combinations, eliminating many risks of error.

"Our tools caught on, but in the end, you still ask yourself how well you have done, how thorough your testing was," said NIST computer scientist Richard Kuhn, who worked with Kacker on the project. "We updated CCM so it could answer those questions."

NIST's own tools were able to handle software that had a few hundred input variables, but SBA Research developed another new tool that can examine software that has up to 2,000, generating a test suite for up to five-way combinations of input variables. The two tools can be used in a complementary fashion: While the NIST software can measure the coverage of input combinations, the SBA algorithm can extend coverage to thousands of variables.

Recently, Adobe Systems Inc. contacted NIST and requested help with five-way testing of one of its software packages. NIST provided the company with the CCM and SBA-developed algorithms, which together allowed Adobe to run reliability tests on its code that were demonstrably both successful and thorough.

While the SBA Research algorithm is not an official part of the ACTS test suite, the team has plans to include it in the future. In the meantime, Kuhn said that NIST will make the algorithm available to any developer who requests it.

"The collaboration has shown that we can handle larger classes of problems now," Kuhn said. "We can apply this method to more applications and systems that previously were too hard to handle. We'd invite any company that is interested in expanding its software to contact us, and we'll share any information they might need."

More information: R. Smith, D. Jarman, J. Bellows, R. Kuhn, R. Kacker and D. Simos. Measuring Combinatorial Coverage at Adobe; and R. Smith, D. Jarman, R. Kuhn, R. Kacker, D. Simos, L. Kampel, M. Leithner and G. Gosney. Applying Combinatorial Testing to Large-scale Data Processing at Adobe. Both to be presented at IEEE International Conference on Software Testing, Verification and Validation, April 23, 2019.

Provided by National Institute of Standards and Technology

Citation: NIST tool enables more comprehensive tests on high-risk software (2019, April 24) retrieved 3 May 2024 from https://phys.org/news/2019-04-nist-tool-enables-comprehensive-high-risk.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.