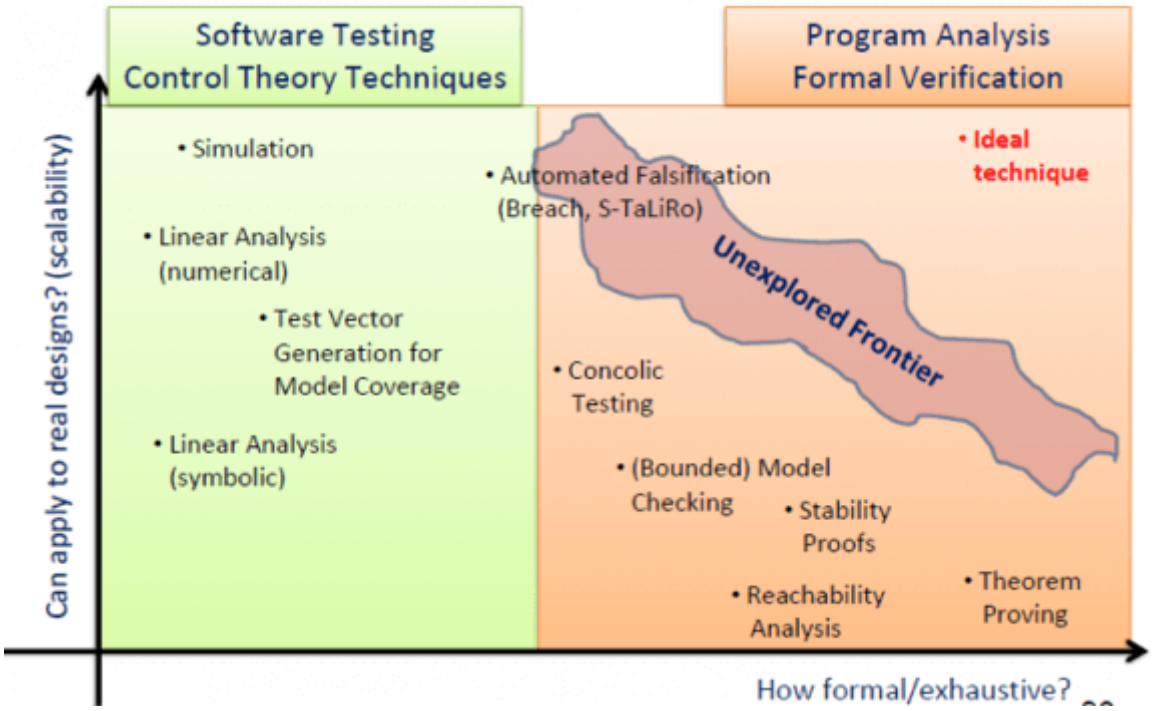
Testing "Mission Impossible" Cyber Physical Systems

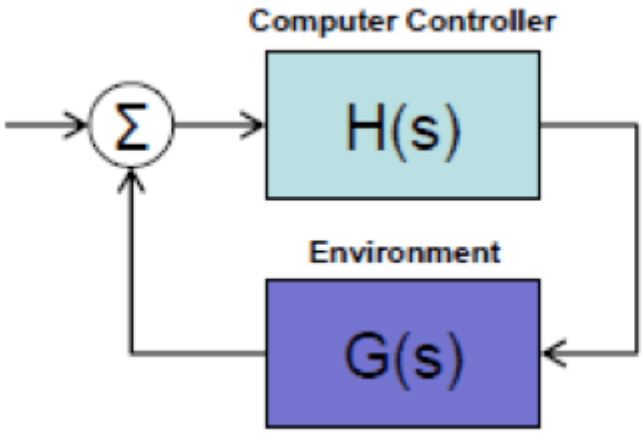
December 14, 2016

Another interesting speaker in my Cyber Physical Systems (CPS) seminar was Dr. James Kapinski. Since he was from the Toyota Technical Center, he focused on power train control and advanced driver assist as two areas in cars that use CPS and where companies are trying to make advances. CPS is basically the field of add software and controls for physical systems thus making them "smart."

Tesla's recent crash highlights the problems that occur when a CPS system fails – the autonomous, driverless car did not see a trailer, went under it and crashed into a power pole. CPS can be approached from both the computer science/software design side and the control engineering design side. Dr. Kapinski approached it from both perspectives.

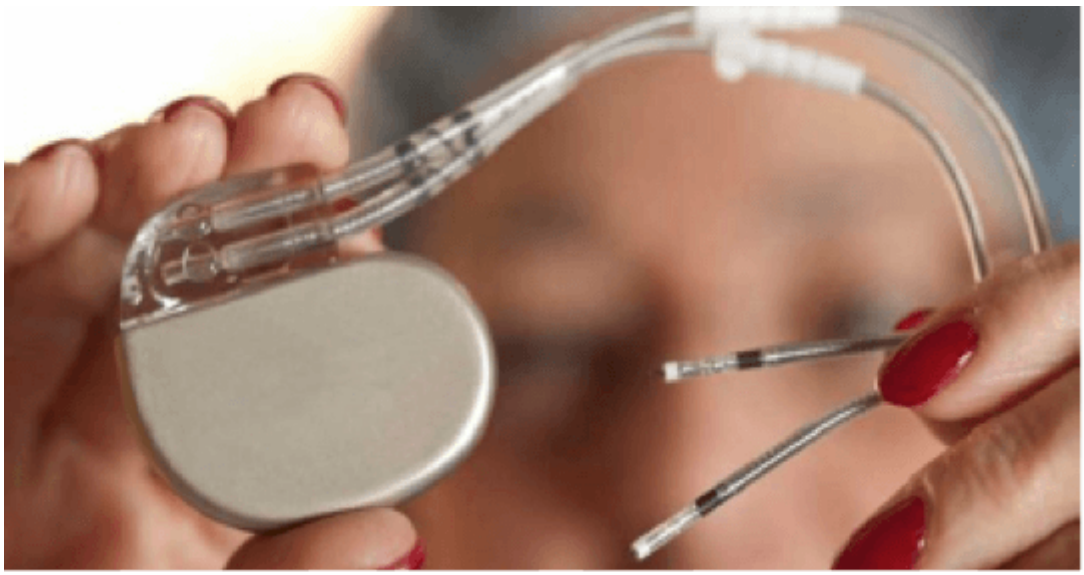


The model-based design approach of control engineers using block diagrams of a controller and its environment works well for concrete simulations of dynamic, complex control systems. However, it does not allow for formal verification which can prove that the system works and/or is stable. Formal analysis techniques from computer science are often too difficult and not scalable for large, complex systems (see top picture).



The main research problem Dr. Kapinski was solving was how to verify a complex industrial, hybrid, dynamical CPS. Specifically, his research addressed the problems of proving stability of a system and/or system safety. A **hybrid system** is one that has both discrete and continuous behavior that varies with time (dynamic).

Their team's **innovation** was using a simulation-based method to get a provably correct and numerically robust certificate of stability using Lyapunov functions. This new technique is finding ways to use information from simulations to develop more formal testing methods for dynamic CPS. Simulations increase confidence in system performance, help design validation, uncover bugs, do not require knowledge of formal testing methods like bounded model checking, and are cheap, fast and scalable.



I learned that Simulink, which I have used to model physiological control systems in BME 511, can also be used for modeling even more complex systems. It can generate a model based on requirements, and most importantly can be used to verify or at least to test different inputs to a system to see how the system responds. This could be useful for many implantable medical devices with sensing

and detection capabilities. Understanding how to test various error use cases and verify safety of an implanted device is critical to prevent FDA recalls and successfully develop devices.

I also learned the difference between testing and verification, both of which are done extensively in the biomedical industry. From Dr. Kapinski's colleague's speech, I learned that verification proves that the input will result in a certain output but testing identifies input cases that would generate errors or bugs but does not prove a relationship between the input and output. Both testing and verification approaches to determining safety are necessary.

PUBLISHED ON DECEMBER 14TH, 2016
LAST UPDATED ON AUGUST 29TH, 2017