Case Study: Verifying Safety of a UUV Heading PID Controller

Submitted by Katie Dey on Sat, 03/10/2018 - 1:59pm. Contributors:
Durward McDonnellRaymond McDowellDaniel GeninIan BlumenfeldAdam W. CushmanJay Guthrie

BIOS

Dr. C. Durward McDonell is a Senior Computer Scientist at JHU/APL. He has a Ph.D. in mathematics from the University of Minnesota. Durward joined APL in 2005. His research interests include formal analysis of computer systems, particularly theorem proving and type theory, and quantum computer science.

Dr. Raymond McDowell is a software assurance analyst with the Software Assurance Research and Applications lab at JHU/APL. He earned bachelor’s and master’s degrees in computer science and engineering from the Massachusetts Institute of Technology and a Ph.D. in computer and information science from the University of Pennsylvania. He has more than 15 years’ experience in industry and academia in the areas of automated support for software engineering and formal specification and analysis of programs and programming languages.

Dr. Daniel Genin is a Senior Computer Scientist at JHU/APL. He received his bachelor’s and doctoral degrees in mathematics from the Pennsylvania State University. After joining APL in 2012 Daniel contributed to a range of different projects from kernel integrity measurement to formal software verification. His current interests are in the area of formal software analysis and verification, as well as reverse engineering and embedded systems.

Ian Blumenfeld received his MA in mathematics from the University of Pennsylvania. He is interested in using formal reasoning in a variety of critical domains. His previous work has used formal methods tools in areas from malware analysis to cryptography. Prior to joining JHU/APL, Ian worked at CyberPoint, Galois and in the High Confidence Software and Systems Group at NSA.

Adam W. Cushman is a member of JHU/APL’s Senior Professional Staff and is Assistant Group Supervisor of the Special Concepts and Engineering Group. He has served as project or technical lead on a wide variety of projects and his areas of interest are in physics-based modeling and simulation, autonomous systems, navigation, guidance, and control, and software development.

Jay Guthrie is a controls engineer at JHU/APL. He received his master’s degree in engineering from Purdue University. He is currently working towards a Ph.D. in electrical engineering at Johns Hopkins University. He is interested in optimization-based control methods with applications in power systems, aerospace vehicles, and autonomous systems.

ABSTRACT

Proportional Integral Derivative (PID) controllers are ubiquitous in cyber-physical systems, from industrial control to drones. Their simplicity and well-understood dynamics make them perfect candidates for safety critical applications. However, simplicity of design is inevitably compromised to address departures of the real-world systems from the idealized linear dynamics. For example, low-pass filtering may be added to reduce noise in the feedback signal, gain scheduling may be added to account for non-linearity in response, and output clamping may be added to constrain the control signal to an acceptable range. As the complexity of the controller design grows, ensuring correct and safe operation of the system becomes a real challenge.

We demonstrate an approach based on hybrid systems analysis and formal methods that allows theorems about safety and correctness of a PID controller to be extended to the source code level implementation. This approach is explored through an application to the heading controller of an Unmanned Underwater Vehicle (UUV). We show how the hydrodynamic model of the UUV can be combined with the mathematical specification of the PID controller logic to verify roll angle safety using the KeYmaera X hybrid systems theorem prover. This is a mainly mathematical endeavor, where the main challenge is adapting well-known control theory results based on Lyapunov function theory to...
KeYmaera X's differential dynamic logic formalism. The resulting proofs establish the safety of the controller at the specification level.
We then use the type constraint mechanisms and proof capabilities of SPARK / GNATprove to formally verify that the source-level SPARK implementation of the controller logic satisfies the assumptions of the KeYmaera X specification proofs. In particular, we are using SPARK contracts to verify that floating point calculations preserve the desired PID recurrences.

Durward McDonnell  |  Raymond McDowell  |  Daniel Genin  |  Ian Blumenfeld  |  Adam W. Cushman  |  Jay Guthrie

License: Creative Commons 2.5

Other available formats:

Case Study: Verifying Safety of a UUV Heading PID Controller
Switch to normal viewerSwitch to experimental viewer

Presentation HCSS 2018