**COLLOQUIUM**

Department of Computer Science and Engineering

University of South Carolina

**Why Functional Hardware Description Matters**

**William Harrison**

Date: **March 13, 2017**

Time: **10:30-11:30am**

Place: **Swearingen 1A03 (Faculty Lounge)**

# Abstract

There is no such thing as high assurance without high assurance hardware. High assurance hardware is essential, because any and all high assurance systems ultimately depend on hardware that conforms to, and does not undermine, critical system properties and invariants. And yet, high assurance hardware development is stymied by the conceptual gap between formal methods and hardware description languages used by engineers.

This talk presents ReWire, a functional programming language providing a suitable foundation for formal verification of hardware designs, and a compiler for that language that translates high-level designs directly into working hardware. ReWire is a subset of the Haskell language (i.e., every ReWire program is a Haskell program) that can be translated automatically to synthesizable VHDL. Furthermore, ReWire programs can be verified as one would any functional program — e.g., with equational reasoning in Coq — but they may also be rendered as efficient circuitry by the ReWire compiler. We describe the design and implementation of ReWire as well as its application to the construction and verification of secure hardware artifacts.

**Dr. William Harrison** received his BA in Mathematics from Berkeley in 1986 and his doctorate from the University of Illinois at Urbana-Champaign in 2001 in Computer Science. From 2000-2003, he was a post-doctoral research associate at the Oregon Graduate Institute in Portland, Oregon where he was a member of the Programatica project. Dr. Harrison is an associate professor in the Computer Science department at the University of Missouri, where he has been since 2003. In December 2007, he received the CAREER award from the National Science Foundation's CyberTrust program. In 2013, Dr Harrison spent a sabbatical year at the National Security Agency's research directorate. His interests include all aspects of programming languages research (e.g., language-based computer security, semantics, design and implementation), reconfigurable computing, formal methods and malware analysis.