Formal Framework for Ensuring Consistent System and Component Theories in the Design of Small Satellite

Jules Chenou [1], William Edmonson [1], Albert Esterline [1] and Natasha Neogi [2]

Abstract We present a design framework for small-satellite systems that ensures that (1) each satellite has a consistent theory to infer new information from information it perceives and (2) the theory for the entire system is consistent so that a satellite can infer new information from information communicated to it. This research contributes to our Reliable and Formal Design (RFD) process, which strives for designs that are "correct by construction" by introducing formal methods early. Our framework uses Barwise's channel theory, founded on category theory, and allied work in situation semantics and situation theory. Each satellite has a "classification", which consists of tokens (e.g., observed situations) and types (e.g., situation features) and a binary relation classifying tokens with types. The core of a system of classifications is a category-theoretic construct that amalgamates the several classifications. We show how to derive the theory associated with a classification and the theory of the system core, and we show how to check whether a given requirement is derivable from or consistent with a theory.

[1] NC A&T State University, 1601 East Market St., Greensboro, NC 27411, U.S.A {jchenou, wwedmons, esterlin}@google.com

[2] National Institute of Aerospace, 100 Exploration Way, Hampton, VA 23666, U.S.A - neogi@nianet.ogr