Appears in Proceedings, Third IEEE International Symposium on Requirements Engineering (RE'97), January 5-8th, 1997, Annapolis, Maryland, USA.

Formal Methods for V&V of partial specifications: An experience report

Steve Easterbrook and John Callahan
{steve,callahan}@cs.wvu.edu
NASA/West Virginia University Software IV&V Facility
100 University Drive
Fairmont, WV 26554

Abstract

This paper describes our work exploring the suitability of formal specification methods for independent verification and validation (IV&V) of

ment teams.

In section 2,

IV&V contractor as less access to t e development team t an is ideal.

			OR		
	C&C MDM acting as t e bus controller	T	T	T	T
	Detection of transaction errors in two consecutive processing frames	T	T	T	T
	errors are on selected messages	T	T	T	T
	t e RT's 1553 FDIR is not in ibited	T	T	T	T
	A backup BC is available	T	T	T	T
A	T e BC as been switc ed in t e last 20 seconds	T	T	T	T
N	T e SPD card reset capability is in ibited	T	T	.	.
D	T e SPD card as been reset in t e last 10 major (10 second) frames	.	.	T	T
	T e transaction errors are from multiple RTs	T	T	T	T
	T e current c annel as been reset wit in t e last major frame	T	F	T	F

tant in tracing problems back to t e informal specification, and in convincing t e development team t at t ere really is a problem.

T e first step was to produce an SCR model of t e specified FDIR be avior. At t is stage we

Current Mode	Conditions											Next Mode
	errors in two cons. frames	bus swch'd last frame	bus switch inhibit	bus swch'd this frame	backup BC avail.	BC swch'd in last 20 sec	card reset inhibit	card reset last 10 frames	errors from mult. RTs	channel reset last frame	channel reset inhibit	
Normal	@T	-	-	F	-	-	-	-	-	-	-	switch buses
	@T	-	T	F	-	-	-	-	-	-	F	reset the
	@T	T	-	F	-	-	-	-	-	-	F	channel
	@T	-	-	-	-	-	F	F	T	T	-	reset the
	@T	-	-	-	-	-	F	F	T	F	T	card
	@T	T	-	-	-	-	-	-	F	T	-	switch RT
	@T	F	T	-	-	-	-	-	F	T	-	to backup
	@T	T	-	-	-	-	-	-	F	F	T	
	@T	F	T	-	-	-	-	-	F	F	T	
	@T	-	-	-	T	F	T	-	T	T	-	switch BC
	@T	-	-	-	T	F	T	-	T	F	T	to backup
	@T	-	-	-	T	F	-	T	T	T	-	
	@T	-	-	-	T	F	-	T	T	F	T	
	@T	-	-	-	T	T	T	-	T	T	-	switch
	@T	-	-	-	T	T	T	-	T	F	T	all RTs
	@T	-	-	-	T	T	-	T	T	T	-	
	@T	-	-	-	T	T	-	T	T	F	T	

Table 2: An SCR Mode transition table. Eac of t e central columns represents a condition, s owing w et er it s ould be true or false; '-' means "don't care"; '@T' indicates a trigger condition for t e mode transition. T e four columns of table 1 correspond to t e last four rows of t is table. T e semantics of SCR require t is table to represent a function, so t at t e disjunction of all t e rows covers all possible conditions (coverage), and t e conjunction of any two rows is false (disjointness).

t at it leads to, but also for t e removal of ambiguities and for improved understanding. For t is benefit, it is t e *process* of formalization, rat er t an t e end product t at is important.

T e fidelity problem is really a special case of a more general problem: management of consistency between partial specifications expressed in different notations. For instance, t e AND/OR tables ave a clear relations ip wit t e SCR mode tables, but if we make a correction to one of t e AND/OR tables, it is fairly tedious to identify t e corresponding correction in t e SCR tables. Similarly, eac time t e developers ide a correction to [illegible]

t e assorted partial specifications drawn from different

continuing t e experiments described in t is paper by examining ow model c ecking can be used to validate t e specifications.

Acknowledgments

Our thanks are due to Chuck Neppach and Dan McCaugherty for many interesting discussions of the work presented here, and to Frank Schneider, Edward Addy, John Hinkle, George Sabolish, Todd Montgomery and Butch Neal for detailed comments on earlier drafts of this paper. This work is supported by NASA Cooperative Research Agreement NCCW-0040.

References

[1] V. Basili. T e experience factory and its relations ip to ot er improvement paradigms. In *Proceedings of the 4th European Software Engineering Conference, Garmish-Partenkirchen, Germany*, September 1993.

[2] J. Calla an and T. Montgomery. An approac to verification and validation of a reliable multicast protocol. In *Proceedings of the ACM International Symposium on Software Testing and Analysis (ISSTA)*, January 1996.

[3] D. Craigen, S. L. Ger art, and T. Ralston. Formal met ods reality c eck: