

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 has less access to the development team than is ideal.



A N D	C&C MDM acting as the 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
	the RT's 1553 FDIR is not inhibited	T	T	T	T
	A backup BC is available	T	T	T	T
	The BC has been switched in the last 20 seconds	T	T	T	T
	The SPD card reset capability is inhibited	T	T	.	.
	The SPD card has been reset in the last 10 major (10 second) frames	.	.	T	T
	The transaction errors are from multiple RTs	T	T	T	T
	The current channel has been reset within the last major frame	T	F	T	F

OR

tant in tracing problems back to the informal specification, and in convincing the development team that there really is a problem.

The first step was to produce an SCR model of the specified FDIR behavior. At this stage we



t e assorted partial specifications drawn from differ-  
ent



continuing the experiments described in this paper by examining how model checking can be used to validate the 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. The experience factory and its relationship to other improvement paradigms. In *Proceedings of the 4<sup>th</sup> European Software Engineering Conference, Garmish-Partenkirchen, Germany, September 1993*.
- [2] J. Calla an and T. Montgomery. An approach 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. Gerhart, and T. Ralston. Formal methods reality check: