Software Engineering and SDI

Martin J. Moore

[Taken from the on-line Soft-Eng Digest, Fri 23 Aug 85, Volume 1, Issue 31]

Dr. David Parnas has quite accurately pointed out some of the dangers inherent in the software to be written for the Strategic Defense Initiative. I must take exception, however, to the following statement from the Boston Globe story quoted in Volume 1, Issue 29, of this digest:

> "To imagine that Star Wars systems will work perfectly without testing is ridiculous. A realistic test of the Strategic Defense Initiative would require a practice nuclear war. Perfecting it would require a string of such wars."

There are currently many systems which cannot be fully tested. One example is the software used in our present defense early warning system. Another example, one with which I am personally familiar, is the Range Safety Command Destruct system at Cape Canaveral Air Force Station. This system provides the commands necessary to destroy errant missiles which may threaten populated areas; I wrote most of the software for the central computer in this system. The system can never be fully tested in the sense implied above, for to do so would involve the intentional destruction of a missile for testing purposes only. On the other hand, it must be reliable: a false negative (failure to destroy a missile which endangers a populated area) could cause the loss of thousands of lives; a false positive (unintentional destruction of, say, a Space Shuttle mission) is equally unthinkable. There are many techniques available to produce fault-tolerant, reliable software, just as there are for hardware; the Range Safety system was designed by some of the best people at NASA, the U. S. Air Force, and several contractors. I do not claim that a failure of this system is "impossible", but the risk of a failure, in my opinion, is acceptably low.

> "But ANY risk is too great in Star Wars!"

I knew someone would say that, and I can agree with this sentiment. The only alternative, then, is not to build it, because any system at all will involve some risk (however small) of failure; and failure will, as Dr. Parnas has pointed out, lead to the Ultimate Disaster. I believe that this is what Dr. Parnas is hoping to accomplish: persuading the authorities that the risk is unacceptable.

It won't work. Oh, perhaps it will in the short run; "Star Wars" may not be built now, or ever. But sooner or later, some system will be given life-and-death authority over the entire planet, whether it is a space defense system, a launch-on-warning strategic defense system, or something else. The readers of this digest are the present and future leaders in the field of software engineering. It is our responsibility to refine the techniques now used and to develop new ones so that these systems *will* be reliable. I fear that some first-rate people may avoid working on such systems because they are "impossible"; this will result in second-rate people working on them, which is something we cannot afford. This is *not* a slur at Dr. Parnas. He has performed an invaluable service by bringing the public's attention to the problem. Now it is up to us to solve that problem.

I apologize for the length of this message. The above views are strictly my own, and do not represent my employer or any government agency.

RCA Armament Test Project
P. O. Box 1446
Eglin AFB, Florida 32542

Martin J. Moore
Senior Software Analyst
ARPAnet: MOOREMJ@EGLIN-VAX.ARPA