Subject: Ariane notes
From: "Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Date: Thu, 25 Aug 2005 13:55:48 +0200
To: undisclosed-recipients: ;

Thanks to Rod Chapman for pointing out Colin O'Halloran's (CoH) paper. It includes information that was not in the Inquiry Board report, and that is relevant to the discussion.

First, a word on terminology. By "function", I have meant and continue to mean some process defined as a function by the architecture. Such functions have features or properties of their behavior. These features or properties can sometimes be functional, sometimes not, for example satisfying real-time constraints. As a matter of logic, if the function is defined to carry on in unbounded time, there are unboundedly many such features or properties. Indeed, there are unboundedly many which are functional in nature (as a matter of logic, one can convert even real-time constraints to a functional form, albeit not one generally useful for specification). I shall call a property or feature of the behavior of the function a "process". (Note this is a specific use of a word which has other meanings in other contexts. I can't think of a better one at the moment.)

Not to CoH's paper.

1. I read in the phrasing of the paper that the fault occurred not in the alignment function itself, but in a function which CoH calls the "quick alignment function", which is a separate function from alignment, and which I shall abbreviate by QAF.

So this answers definitively the question as to the necessity of the function. Is QAF needed for Ariane 5? No; it serves no purpose, because when the launch is interrupted from T-9 to T-5, an Ariane 5 launch will be scrubbed anyway. Note that this was not known at the time that the requirements for the IRS were written (see below). Is it needed for Ariane
4? Yes (or so it was determined by the system engineers. It was used once).

But the particular process in the QAF that led to the overflow was also not
required in the relevant IRS SW for Ariane 4. The original A4 IRS was mechanical-gyro-based and the QAF was implemented in assembler. This system

was re-implemented to use ring-laser gyros for reasons of mechanical reliability (to reduce the chance of random faults) and many functions were
transferred into SW, including the QAF. The process that failed made little
sense for the ring-laser-SW-based system. The Board's best guess was that it was for mechanical gyros. It thus became redundant when the new IRS was implemented with ring-laser gyros and SW written in Ada83.

2. As Gerard has said, the fault was due to system engineering, not software engineering. That the process was required for mechanical gyros
but not for ring-laser gyros is a system engineering issue. QAF need not have included it for either Ariane 4 or 5 in the new IRS.

3. This is an example neither of a COTS issue nor a "software re-use" issue. The answer to Kevin's question whether A501 is an example of either
of these is thus: No.

There was no software re-use here. There was re-implementation. None of
the old assembler code, written for a system in which the process in the QAF made sense, was present in the new IRS (written in Ada83), as far as
I can tell.

As CoH says, "[t]he problem was not straightforward software re-use, [which] frequently occurs, but a more subtle "re-use" of the old requirements." And by "requirements" here, he means engineering requirements, not software requirements.

4. On requirements analysis: "It is reasonable to suggest that as a precautionary measure any functionality that served no purpose on Ariane 5
should have been "switched" off for that configuration of use. However, it
is not clear that at that stage in the A5 programme that they could have anticipated that the [QAF] would not be useful..... design decisions made later might have led to the redundancy in the requirement for quick alignment.

--
Peter B. Ladkin, Professor of Computer Networks and Distributed Systems,

Faculty of Technology, University of Bielefeld, 33594 Bielefeld, Germany
Tel+Msg +49 (0)521 880 7319 www.rvs.uni-bielefeld.de