

sci.space.shuttle: Re: What was the biggest problem for each of the 2 destroyed US space shuttles?

Re: What was the biggest problem for each of the 2 destroyed US space shuttles?

Source: <http://sci.tech-archive.net/Archive/sci.space.shuttle/2004-09/0533.html>

From: Derek Lyons (fairwater_at_gmail.com)

Date: 09/13/04

Date: Mon, 13 Sep 2004 23:08:52 GMT

"Jay Windley" <webmaster@clavius.org> wrote:

> *This quote can also be interpreted to make a case for conservatism. That is, if you can't know ahead of time how systems will behave, then you should expect unanticipated failures. That seems paradoxical, I realize, but I'm saying it seems to argue for staying well within the boundaries so that you can use the resulting margin to address new failures.*

>

> *More appropriately, I believe it addresses the notion that the rules have to be looked at constantly for deficiencies in the design. You have requirements and specifications, but those generally discuss what is to be done and impose looser restrictions on how it is to be done. In order to satisfy the requirements you impose operational rules that initially derive from the design. But those rules are formulated -- especially in the case of new technology -- from a tentative extrapolation of known basic principles. As experience accumulates, satisfying the requirements entails day-to-day operations that reflect what you learn.*

>

> *Engineering decisions are made somewhere between perfect understanding and total ignorance, so any system of rules to govern engineering decisions has to be formulated to allow for variance as experience is accumulated. Pretending that you can see the end from the beginning is not helpful.*

>

> *When you cannot fully predict the behavior of a system as it is designed -- such as in a complex space vehicle -- you have to write the rules that govern its operation based on the information and expertise you have at hand, however incomplete or speculative. Those rules can take the form, "Do not operate the system in this certain way because this bad thing will happen if you do." That's based on past experience with similar systems and upon the general principles of design engineering.*

>

> *But if, for whatever reason, the system is operated adversely and the Bad Thing does not happen, then you might want to question that restriction. If you go back and look at the consequences of your adverse operation and realize that the system had a previously unforeseen margin or protective interaction, then you can relax the operational rule based on new*

sci.space.shuttle: Re: What was the biggest problem for each of the 2 destroyed US space shuttles?

>*information that the original designer did not have. Design ambiguity works*
>*in both directions.*

(I hate to leave that long quote in, but my comment makes little sense without it.)

An interesting example of this can be found in the Thresher accident. Prior to Thresher, reactor operating procedures stressed keeping heat in the reactor as it was believed that retaining the ability to easily restore propulsion was the most important factor in accident recovery. That policy may have contributed to Thresher's doom as it placed the survival of the reactor over the survival of the crew, and placed the crew entirely in the hands of the now known to be flawed emergency blow system.

Post Thresher, the procedures were changed to allow the use of that heat in an emergency for propulsion and power. The emphasis was shifted to placing the survival of the hull and crew over retaining the ability to easily restart the reactor. In another Thresher style accident, it may or may not make the difference, but the option is there.

D.

--

Touch-twice life. Eat. Drink. Laugh.