

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/2004-09/0527.html>

From: Jay Windley (webmaster_at_clavius.org)

Date: 09/13/04

Date: Mon, 13 Sep 2004 11:14:28 -0600

"Jay Windley" <webmaster@clavius.org> wrote in message
news:ci39kp\$44q\$1@news.xmission.com...

|
|| <Jay writes about learning by doing>
||
|| Really? Have a cite for this?
|
| Yes, but not handy this evening.

I like your style of quotation markup, so I will adopt it.

<wynne>

"Beneath a public image of rule-following behavior and the associated belief that accidents are due to deviation from those clear rules, experts are operating with far greater levels of ambiguity, needing to make uncertain judgments in less than clearly structured situations. The key point is that their judgements are not normally of the kind -- how do we design, operate and maintain the system according to 'the' rules? Practices do not follow rules; rather, rules follow evolving practices." (Brian Wynne, "Unruly technology: practical rules, impractical discourses, and public understanding." *_Social Studies of Science_* [18], p. 154)

</wynne>

I believe that rules for operating complex technology exist at two slightly different scopes: one that derives from the design studies, and another that departs from design studies and incorporates knowledge gained in the field. They apply to different activities regarding the system's operation. This is especially important for technologies such as the space shuttle that are considerably innovative. While the written rules can govern at a broad scope, the SRB field joint teams and their operators are better served by information they obtain as a result of operating the joint and of testing it

<petroski>

"The very newness of an engineering creation makes the question of its soundness problematical. What appears to work so well on paper may do so

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

only because the designer has not imagined that the structure will be subjected to unanticipated traumas or because he has overlooked a detail that is indeed the structure's weakest link." (Henry Petroski, *To Engineer is Human: The Role of Failure in Successful Design*, p. 80)
</petroski>

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.

Now having said that, the question that is more interesting to me is why the decision-making process leading up to the eve of the launch seems to have been broken.

In the first chapter of Charles Perrow's *Normal Accidents* he discusses the effects of slowly unfolding data upon operators. Accidents are always investigated in hindsight, and the benefits of that hindsight are frequently used to judge the operators in charge during the accident. A number of psychological factors come into play: the value of interpretation, the basic belief in safety and redundancy.

| | And I'll for a cite for this theory of yours that there is no pre-existing sense of right, wrong, safe, or broken for anomalies for the Shuttle.

| ...But I think you're going a bit farther with the statement than I perhaps intended, or perhaps I'm going too far. You still have the original requirements and expectations, and they still have value, but they are examined and perhaps modified as new information about safety and behavior becomes available.

I believe the quotations above support this view.

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

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

--

The universe is not required to conform
to the expectations of the ignorant.

| Jay Windley
| webmaster @ clavus.org