

The Embedded Muse 50

Editor: Jack Ganssle (jack@ganssle.com)

August 1, 2000

Embedded Failures

On March 12 Sea Launch attempted to boost a communications satellite into orbit from their ocean-based platform, and failed. A single line of code was in error, which allowed the vehicle to blast off with an open second stage pneumatic valve.

Their two earlier launches were successful, as was one this week.

So here's an example of a hideously-expensive failure of an embedded system, one where the firmware was at fault. I have no other details of the failure, but ask any reader who has information to send it to me at <mailto:jack@ganssle.com>.

The firmware content of all products is skyrocketing, yet "reliable code" seems to be an oxymoron. Surely we'll see a breathtaking surge in the number of embedded system failures. Some will be of little consequence, perhaps just annoying our customers. Others will threaten life and limb.

Did you know that Ford recalled some Explorers on June 6, 2000 because air bags, windshield wipers and other accessories could fail? The culprit: a missing pull-up resistor on the computer module.

Surely we can learn from these disasters if we develop a lore of catastrophe. For instance, what does the Los Alamos near-nuke failure of 1998 and Ariane 5's maiden flight explosion have in common? Poor error handling. And error handling is a huge problem for all software, as it's dreadfully hard to anticipate and test all error possibilities.

So I'm collecting stories of embedded disasters, to share with readers. If you know of a disaster - and can validate it - please send me information or references. Just as civil engineers learn from stories of collapsing bridges and skywalks, we can - and should - tune into these problems in our own field.

Contest!

When Signetics created their Write Only Memory part as a joke a quarter century ago, they probably had no idea so many people would be so entranced.

Copyright 2001 by The Ganssle Group. All Rights Reserved. You may distribute this for non-commercial purposes. Contact us at info@ganssle.com for more information.

The Ganssle Group, www.ganssle.com

I have a copy of the part's original datasheet, as well as an actual part (marked "NFG" in case there's any doubt).

Just for fun, here's a contest with the datasheet and the Write Only Memory chip as grand prize. Come to <http://www.ganssle.com>, select the link to the contest, enter your email address, and your name will be tossed into the ring to win the prize. If you'd like, also enter in a suggestion for what you'd use a write-once, read-never part for.

The winner will be announced in this newsletter, and some of the funnier uses for the part will run as well.

Thought for the Week

To the optimist, the glass is half full. To the pessimist, the glass is half empty. To the engineer, the glass is twice as big as it needs to be.

About The Embedded Muse

The Embedded Muse is an occasional newsletter sent via email by Jack Ganssle. Send complaints, comments, and contributions to him at jack@ganssle.com.

To subscribe, send a message to majordomo@ganssle.com, with the words "subscribe embedded *your-email-address*" in the body. To unsubscribe, change the message to "unsubscribe embedded *your-email-address*".

The Embedded Muse is supported by The Ganssle Group, whose mission is to help embedded folks get better products to market faster. We offer seminars at your site offering hard-hitting ideas - and action - you can take now to ***improve firmware quality and decrease development time***. Contact us at info@ganssle.com for more information.

Copyright 2001 by The Ganssle Group. All Rights Reserved. You may distribute this for non-commercial purposes. Contact us at info@ganssle.com for more information.

The Ganssle Group, www.ganssle.com