The Embedded Muse 75

Editor: Jack Ganssle (jack@ganssle.com) September 25, 2002

Editor's Note

Check out http://ee.cleversoul.com, The EE Compendium. A very nice collection of reviews of EE books and links to industry sites. Also check out sublink http://ee.cleversoul.com/software.html, which has links to bug tracking and version control utilities. A lot of folks ask me about these.

I just finished "Inviting Disaster" by James Chiles (HarperBusiness; ISBN: 0066620813; September 2001). A very interesting book, well worth reading. Chiles describes a number of technological disasters. He delves into the root causes of each. Some of the events were averted before anyone was hurt; others resulted in hundreds and thousands of deaths.

I collect embedded disasters – there's so much we can learn from these! But Chiles' book doesn't speak to the embedded world per se. Bridges, ships, airplanes and industrial plants get the most focus. Still, I think the book offers important warnings to anyone building complex systems.

I was struck by how well most of the described systems worked. Rarely was the proximate cause of failure a single event; usually one small problem precipitated a cascade of errors, often made worse by poorly trained human operators. In a few cases superior training and experience saved the day, preventing serious technological failures from turning into headline-busting news.

A lot of failures were at least partly caused by instruments that lied to the operators. In two of those cases (Apollo 13 and Three Mile Island) temperature sensors read max values (at TMI 280 degrees, though the input was closer to 1000) simply because that's as far as the programmers allowed the instruments to read. Any higher value was thought to be impossible. This is a tough problem for us. Specs are notoriously incomplete; it's likely that in these cases developers made decisions that seemed reasonable at the time, decisions that worked very well until an unlikely series of events unfolded.

Chiles doesn't cover the Therac-25 (see http://courses.cs.vt.edu/~cs3604/lib/Therac_25/Therac_1.html) which killed a few patients. We embedded people know of it. But that was 1985, software was much more casually written then. Today we don't tolerate such error-prone methods.

Maybe we do. Check out http://www.iaea.org/worldatom/Press/P_release/2001/panam_adv_info2.shtml. Turns out another therapeutic instrument, meant for much the same application as the Therac-25, recently killed 9 people in Mexico; as of the initial report date (May 2001), another 15 or so were expected to die. It was a complex failure due in part to operator errors. But the machine lied to the users, telling them the programmed dosage was safe. It wasn't.

Civil engineers study old bridge failures. Aircraft designers have a wealth of information from plane crashes. We, too, cannot afford to thwart disaster by learning solely from our own experiences.

Thought for the Week

This issue's Thought for the Week comes from responses to the last Muse's discussion of the IEC's definitions of prefixes for powers of two. To reiterate, the IEC has defined the following prefixes:

2**10 kibi (symbol Ki) (one kibi is 1024)
2**20 mebi (symbol Mi) (one mebi is 1 048 576)
2**30 gibi (symbol Gi) (one gibi is 1 073 741 824)

Tom of Bunyon commented: "For some people, this is byteing off more than we can queue..."

Dave Kellogg made the interesting observation that 1000 terabytes is a petafile…

I like Tim Kramer's thought: "There are 10 kinds of people in the world: those who get binary and those who don't." (Think about it).

Lance Kasari brought up a fascinating problem with the sytem. People will try and mix base 10 and base 2. So 1000 mebibytes does not equal one gibibyte (which is properly 1024 mebibytes). He figures that 1 gibibyte is really the same as a kibimebibyte (1024 mebibytes)… but how do we keep people from giggling when they say this?

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.