WORST-CASE SCENARIO

While Bob Colwell makes some valid points in his August column (“What’s the Worst That Can Happen?” pp. 12-15), I noticed a phrase that took me by surprise: “… plutonium, the deadliest substance on Earth ….”

Upon further research on the Internet, I came across the Health Physics Society, a group that appears to beg to differ on that particular point (http://hps.org/publicinformation/ate/q1339.html). A PDF document linked from that site states, “The fact is that there are many people who inhaled measurable quantities of plutonium many years ago and have suffered no ill effects. The radiological hazards of plutonium are of the same types and magnitudes as those of such naturally occurring radioactive elements as radium and thorium.” In his column, Colwell described thorium as being one of the materials used to produce U-238.

My argument is that while producing a nuclear reactor as a backyard project can be seen as very dangerous, David Hahn would most likely not drop dead at that moment as is suggested.

More likely, Hahn would live long enough to either realize that what he was doing was quite dangerous, thus surviving until his next crazy experiment, or he would push forward to somehow trigger an uncontrolled chain reaction. That would yield a new definition of a “very bad day” for people in close proximity to that shed.

Theodore J. Griesenbrock III
Laveen, Ariz.
teej42@gmail.com

Bob Colwell responds:

There is a boatload of contenders for the title of “deadliest substance on Earth,” and I had been hearing that plutonium was the worst for so long that I had stopped questioning whether it was true. I think periodically clearing one’s mental attic of old memes is a very good thing, and I thank reader Griesenbrock for this reminder.

CONTROL CHARTS

Although I found “Iterative Rework: The Good, the Bad, and the Ugly” (Richard E. Fairley and Mary Jane Willshire, Sept. 2005, pp. 34-41) to be both interesting and well written, I would like to point out one statement that doesn’t seem right.

In the “How Control Charts Work” sidebar (p. 39), the authors correctly state that the control limits are calculated “using three standard deviations from the mean.” However, at the end of the sidebar, they state that the upper control limits (UCL) and lower control limits (LCL) can be determined “based on pragmatic considerations.”

UCL and LCL are the “voice of the process,” and controlling process variations is the only means for changing them. It is customary to set the “voice of the customer” limits, which are then used to determine process capability. But those are not control limits—they are specification limits. The process performance may or may not succeed in satisfying those specification limits.

Using control limits as described in the paper could lead to the wrong conclusions.

Boris Mutafelija
Herndon, Va.
mutafelija@systemsandsoftware.org

STORAGE SECURITY

In “Security in Storage: A Call for Participation” (Standards, Sept. 2005, pp. 103-105), Jack Cole makes some important points regarding security for computer storage devices. USB flash drives also represent a significant security concern, in part because they are small enough to be either misplaced or lost, in which case sensitive unencrypted data could easily be disclosed.

Popular plug-and-play devices like iPods, PDAs, and digital cameras, which are incredibly easy for anyone to operate, could easily spread a virus or destructive code. To leverage the huge convenience these devices offer when combined with USB drives, security efforts should focus on the protection provided by technologies such as firewalls, antivirus software, and content filtering both at the gateway and workstation level.

I agree with the author that data at rest is not as big a security threat as data in flight. However, the most significant security threat to computing devices still lies on the network interface card. System administrators must continue to lock things down at the gateway, which is really the glue that holds everything together—including all those wireless access points.

Securing a network should always have much higher priority than setting up a secure client, especially for organizations that have hundreds or thousands of machines connected to the network. Only a well-configured network will prevent an infected portable device or USB drive from passing malicious code to another device and ultimately to the corporate network, thus compromising the company’s data.

Hong-Lok Li
Vancouver, BC
llhl@ams.ubc.ca

ERRATUM