PAUL STUDEBAKER
EDITOR IN CHIEF
pstudebaker@putman.net

SCRAM

My mother worked for many years at Argonne National Laboratory, measuring radioactivity of air samples from around the world as part of the U.S. government's program to monitor atomic bomb tests. To mark her 25th anniversary, the lab gave her a paperweight—a block of Lucite encasing a ¾ x ¾ x 3-in. black bar of material labeled, "Graphite from CP-1; First Nuclear Reactor; Dec. 2, 1942; Stagg Field—The University of Chicago."

It's coming up on 75 years since Enrico Fermi and associates, with the help of labor by members of the U of C's highly unprofessional but physically fit football team, assembled 400 tons of graphite blocks and 50 tons of uranium oxide into Chicago Pile 1 (CP-1) under the Stagg Field bleachers on the south side of Chicago.

Like most modern reactors, CP-1 was controlled by inserting neutron-absorbing rods into spaces between the tin cans of uranium oxide. The rods—wooden sticks wrapped with cadmium—were hung vertically from rope and pulley mechanisms, controlled by a reheostat on a motor. Slowly raising the rods would start or increase the self-sustaining fission reaction.

By one view, the reactor briefly produced a maximum of 200 Watts. By another, it led to the atomic bombing of Hiroshima and Nagasaki, killing 200,000 people, as well as power reactor disasters at Chernobyl and Fukushima.

Popular lore has it that Fermi stationed a "safety control rods axe man" (SCRAM) by the rope with instructions to cut it and run in the event of a runaway reaction. The acronym has persisted as the expression for an emergency shutdown of a boiling water reactor.

The control rods were also weighted to fall without human intervention in the event of a power outage. When I studied nuclear engineering as a minor in the 1970s, gravity-powered control rod or borated water safety systems were the norm.

In process plants, spring-return actuators and other mechanical fail-safe mechanisms provide similar safety benefits. Engineers go to great lengths to calculate risks and probabilities, and devise safety systems with redundancies and disparate designs, so that no single failure or common mode of failure can result in an unsafe condition.

As systems have become more complicated and plants increasingly computer-controlled, we've built and certified digital controllers that meet our requirements for reliability and redundancy, so we use them for safety systems.

If you asked Enrico Fermi what would prevent a frustrated football player from knocking down the axe man, yanking out the control rods, and destroying Hyde Park, he probably wouldn't have had an answer. How could he also worry about that?

But in this era of cyber insecurity, where the cyber equivalent of an armed terrorist can assault our control system from a remote pumping station or our parking lot or on the web from anywhere in the world, how can we use software-controlled digital systems to perform safety functions?

The criteria for the degree of risk reduction that must be provided by a safety function—the safety integrity level (SIL)—is determined by the severity of the consequences of a failure. The greater the consequences, the more we want to reduce the probability of the failure. To date, the potential consequences of cyber attacks on industrial facilities in the United States and Europe have been easily imagined, but not experienced. So we still see safety issues from cyber attacks as improbable, with consequences we can't define.

So we lump them into the same category as other terrorism: we'll make a lot of fuss if and when something happens, then life will go on. Meanwhile, there's not much point in doing anything about it. Fermi didn't.

What would prevent a frustrated football player from knocking down the axe man, yanking out the control rods, and destroying Hyde Park?