National Aeronautics and Space Administration

System Failure Case Studies

FEBRUARY 2007 Volume 1 Issue 4

SUPERCRITICAL

In the early years of nuclear power development, the first small-scale boiling water reactor exploded catastrophically, claiming the lives of three engineering technicians. This nuclear accident occurred in January of 1961 at the U.S. National Reactor Testing Station near Idaho Falls, Idaho, and is the only nuclear accident resulting in the loss of life ever to occur in the United States. The accident, called a "prompt criticality," resulted from a variety of factors, including inadequate design, inadequate materials testing, and poor procedures and training.

SL-1 Reactor Building prior to January 3, 1961

BACKGROUND: THE COLD WAR

Prior to the break up of the former Soviet Union, the world's two superpowers were locked in a fierce race for technical and military supremacy. This "Cold War" encompassed many elements, including the refinement of nuclear power for a variety of purposes including the development of intercontinental ballistic missiles (ICBMs), and the "race to space." One element of the U.S. national defense strategy in the 1950's and 1960's was the Defense Early Warning system, or "DEW Line." The DEW Line involved the deployment of radar sites across the breadth of northern North America to provide early warning of attack by Russian aircraft or ICBMs. The selected locations for the DEW Line sites were typically very remote, located many miles away from electricity and other utilities and transportation infrastructure, and subject to extreme cold weather most of the year. To provide heat and electricity at these remote locations, a small, simple, light-weight nuclear reactor was to be developed by the U.S. military.

Nuclear Engineering 101

In a nuclear reactor, a controlled fission reaction takes place to produce large amounts of heat. A portion of this heat is removed from the reactor and is used for heating and/or electricity production. The reactor typically requires a fissionable fuel (typically isotopes of uranium), a neutron moderator (typically water), and a means of controlling the rate of reaction. A fissionable fuel is a substance with a nucleus that, upon absorption of a thermal (low-energy) neutron, becomes unstable and "breaks apart" to form two new substances (fission products), heat, and some more neutrons. The neutrons released are of a variety of energies; however, only low-energy, or thermal, neutrons are capable of interacting with additional fuel to produce additional reactions. To convert the high-energy neutrons produced in the reaction to low-energy neutrons, a moderator is used to "slow down" the high-energy neutrons. To operate the reactor at a steady-state (also known as a critical state), a means of controlling the number of thermal neutrons that will interact with the fuel is necessary to control the fission

In January of 1961 a nuclear reactor was destroyed, subsequently killing three engineering technicians.

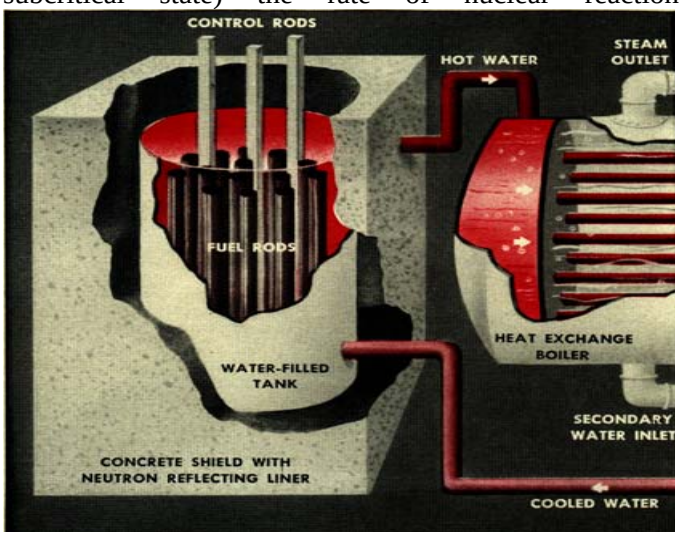
Proximate Cause:

- Rate of nuclear reaction increased to fatal level because of a rapid withdrawal of a control rod

Underlying Issues:

- Continued operation despite frequent control rod malfunctions
- Inadequate testing of new technology
- Lack of rigorous training and detailed procedures
- Insufficient safeguards to prevent improper operating procedures

reaction. Control rods are devices that isolate the fuel elements and absorb neutrons. When a control rod is raised, exposing more of the fuel element to thermal neutrons, the rate of reaction increases; when it is lowered, it isolates the fuel element, and the reaction slows or stops. If control rods are not exercised correctly, an exponential unsteady state can occur by either increasing (also known as a supercritical state) or decreasing (also known as a subcritical state) the rate of nuclear reaction.



Schematic of nuclear reactor, circa 1956.

The SL-1 Reactor

The SL-1 reactor was a 3 megawatt experimental boiling water reactor (BWR) that was to serve as the prototype test and training reactor for the DEW Line applications. Because of the need to transport the reactors to remote areas, weight was a primary design consideration. Since pressures in a BWR are lower than in other types of reactors, the mass and size of the reactor vessel could be reduced.

IT IS ESTIMATED THAT THE CORE POWER LEVEL PULSED TO NEARLY 20,000 MEGAWATTS IN JUST 4 MILLISECONDS.

To achieve the necessary power output from a smaller core it was necessary to use highly enriched uranium as the fuel. In addition, the remoteness of the sites encouraged the system designers to specify reactors that could operate for 3 years without refueling. To meet this challenging core life goal while using highly enriched uranium as the fuel source, the designers incorporated "burnable poisons" into the core design. The burnable poisons dampen the reactivity of the core by absorbing neutrons when the fuel is new. As the fuel is consumed, so are the burnable poisons, resulting in a core that can last longer than one without the poisons.

However, in the late 50's the use of burnable poisons was a new idea that was not well developed. The poison alloys that were available were not able to be fully integrated into the fuel plates, so they were tack welded in strips to the sides of selected fuel assemblies. Apparently, the designers were not satisfied with this arrangement of burnable poison strips (BPS) because plans were made for improved fuel designs in later (production) cores.

What Happened?

The Accident

On December 23, the reactor was shut down for the Christmas holiday. The control rods were dropped into the core to conduct the shutdown and the drop times were recorded in the engineering log. Of the 5 control rods, 3 of them stuck during the shutdown and had to be driven into the core by the drive mechanisms.

At 9:01 PM on January 3rd after a shutdown of 11 days, maintenance procedures were performed to reattach the control rod drive mechanisms to the control rod assemblies. The procedure called for the technicians to raise each control rod about 4 inches to fasten it to the drive mechanism with a nut and washer. During this maintenance activity, a rapid withdrawal of the central control rod by one of the technicians caused the nuclear reactor core to go supercritical. It is estimated that the core power level pulsed to nearly 20,000 megawatts (more than 6,000 times the rated power output) in just 4 milliseconds. The heat generated by the resulting power surge caused the water in the core to explosively vaporize. This steam hammered into the top of the reactor vessel, ejecting the lead shielding and causing the reactor vessel to jump nearly 9 feet out of its support structure. Two of the maintenance technicians on duty at the time were killed instantly by the explosion; a third died a short time later from his injuries.

Proximate Cause

The SL-1 reactor accident was initiated by the withdrawal of its central control rod to a level of approximately 20 inches in the space of 0.5 seconds. Starting from a fully shutdown condition, the action produced a condition in the core technically known as a "prompt criticality," also known as a supercritical state without the contribution of delayed neutrons emitted after fission has occurred.

Underlying Issues

Sticky Control Rods: Engineering logs pertaining to the SL-1 reactor are replete with instances of sticking control rod events. The logs showed that the rods had exhibited stickiness more than 80 times (about 2% of the times that movements had been attempted), and that they failed to

fall freely during a scram (emergency shutdown procedure) 46 times. These difficulties seem to have been increasing, with more than 30 occasions of rod sticking during November and December of 1960, the last operational period before the accident occurred. Plans were underway for a core replacement, but in the meantime a temporary fix had been implemented. An entry from the night order book dated December 20, 1960 states "Each shift will perform a complete rod travel exercise at approx. 4 hours after the start of each shift. This rod exercising will be required of each shift until further notice."

Control rod lodged in ceiling of SL-1 reactor building.

Insufficient Testing of New Technology: The reason behind the occasionally sticking control rods has never been officially determined. However, it is quite possible that the BPSs that had been tack welded to the fuel assemblies had deteriorated. The burnable poison was an aluminum/boron alloy that had a relatively low melting point, and was relatively soft. The tack welds may have failed. Any deformation of these strips could have resulted in the observed sticking.

Before the accident there was little testing of BPS, and no testing of their behavior under the high temperature, high neutron flux conditions present in an operating reactor. Because of the Cold War context, there was a significant sense of urgency to continue with the reactor operation even though the technology was not fully developed.

Lack of Rigorous Training and Detailed procedures: There were also several operational and management failures that contributed to the mishap. The maintenance technicians would have been well aware of the rod sticking problems, and might have decided to conduct a rod travel exercise manually prior to performing the drive reattachment. They might have been especially concerned about sticking since the rods had not been exercised for almost two weeks during the shutdown period.

Unlike modern reactors none of the SL-1's technicians had any background in nuclear engineering. The two operators and one trainee with no nuclear background were unqualified to make operating decisions. It is very likely that the technicians were not aware of the situation that would arise from lifting the control rod to such a height.

Flawed Design of Control Rod System: In addition, the SL-1 reactor was controlled by five cruciform-shaped control rods. Having a small number of rods simplified reactor construction and maintenance by reducing the number of control rod drive mechanisms needed. However, it also made each rod's contribution to the core response much greater than current control rod assemblies, which are typically comprised of 129-185 control rods.

The exact reason the control rod was lifted and the way or rate at which it was retracted will always be shrouded in speculation. Whether it was a sticky rod that interrupted routine maintenance or perhaps the operational reattachment of the rods after a long holiday shutdown the reactor explosion most definitely occurred when increased nuclear reaction was triggered by the distance and rate at which the control rod was removed. This raises the fundamental question why a design was accepted that had not properly taken into account the very real failure mode of inadvertent or malicious intervention regarding control rod movement.

ENGINEERING LOGS PERTAINING TO THE SL-1 REACTOR ARE REPLETE WITH INSTANCES OF STICKING CONTROL ROD EVENTS.

PROBLEM RESOLUTION

Design and Process

The SL-1 accident had many effects, both immediate and long-term. The U.S. military immediately cancelled the SL-1 reactor program. Today's successors to the DEW Line installations, called Long Range Radar Stations (LRRS), use diesel/electric generators to produce heat and electricity.

From a design standpoint, a design criterion previously known as the "one stuck rod" rule is now a requirement for all reactor designs. This criterion requires that the reactor be capable of shutting down even if one control rod is completely removed from the reactor. This "rule" became a rigorous requirement as a direct result of the SL-1 reactor accident.

The accident also led to significant revision of the operations and maintenance policies and procedures for nuclear reactors. For example, today the U.S. military requires that all work on reactor power plants be conducted in rigorous verbatim compliance with detailed written procedures. Furthermore, physical work on the reactors is only performed by highly trained nuclear mechanics. The work is supervised at all times by a nuclear engineer, a senior nuclear mechanic, a quality control engineer, and a radiological control engineer. Critical steps in each procedure are clearly identified, as are associated cautions

and limitations, and require that all involved parties verify through a formal sign off that the step has been conducted correctly and completely before the next step can be initiated.

Response and Recovery

Emergency planning had never before accounted for an event like the SL-1 explosion: medical equipment and facilities were unprepared to handle radioactive bodies; there was a lack of burial procedures for radioactive corpses; shift disaster teams were unorganized; the first rescue workers on the scene did not have proper gloves to protect their hands from the radiation; and instruments were unable to read high radiation fields. Since the SL-1, the Atomic Energy Commission acknowledged that there were weaknesses in the emergency planning and has made great lengths to correct them for future situations.

Applicability to NASA

In today's nuclear and aerospace fields, there is significant pressure to meet project objectives on time and on budget. In this case, the pressure of the Cold War caused deployment of new technologies before adequate development and testing could be performed, resulting in ongoing reactor operation in spite of obvious operational problems with control rods.

While nuclear power engineering is well-established, technologies for removal, treatment, and disposal of high-level radioactive wastes at many DOE sites are still developmental in nature. Similarly, the exploration of our solar system, to Mars and beyond, will require the development of new technologies. Some of these technology requirements are yet but concepts and, therefore, exhibit high degrees of technical, schedule, or cost uncertainty that cannot be avoided or ignored. NASA has established the Technology Readiness Level (TRL) system to track the maturity of emerging technologies (Levels 1-7) as they evolve through all seven stages before incorporating them into a major system.

Uncertainties, credible failure modes, and associated risks must be identified, evaluated, and managed/mitigated from the earliest design stages. At every step of the development process, lessons learned should be documented and used to improve safety, design, policy, or procedures, as applicable. All employees, regardless of assignment or position, can provide valuable ideas or feedback that will help ensure mission success, and improve mission performance.

Questions for Discussion

- Do you feel that the chronic pressure of aggressive schedules is adequately balanced with attention to safety and quality in your organization?

Questions for Discussion (Cont.)

- How could procedures/processes be improved to increase employee participation in providing new ideas for better safety or quality?
- How could your work environment be modified to avoid complacency and emphasize individual responsibility for safety and quality?
- How could procedures/processes for identifying, evaluating, and managing unavoidable uncertainties associated with new technology development be improved?
- Are innovative technologies under consideration by your program/project actually engaged in the system safety hazards analyses process?

References:

Reactor design from the 1950's. [Online image] Available <http://www.animatedsoftware.com/hotwords/nuclear_reactor/nuclear_reactor.htm>.

"SL-1." Radiationworks. <http://www.radiationworks.com/sl1reactor.htm>.

"SL-1 Reactor Accident on January 3, 1961, Interim Report" <http://www.id.doe.gov/foia/IDO-19300a.pdf>, May 1961.

SL-1 Reactor Building, Control rod lodged in ceiling of SL-1 reactor building, Top of the SL-1 reactor vessel. [Online images] Available <http://www.radiationworks.com/sl1reactor.htm>.

"SL-1." Wikipedia, The Free Encyclopedia. <http://en.wikipedia.org/wiki/SL-1>.

"The Aftermath." Idaho National Laboratory. <http://www.inl.gov/proving-the-principle/chapter_16.pdf>.

"The SL-1 Reactor." Idaho National Laboratory. <http://www.inl.gov/proving-the-principle/chapter_15.pdf>.

Thompson, T.J., "The Technology of Nuclear Reactor Safety." MIT University Press, (1964-1973).

"What Caused the Accident? Plenty of Blame to Share." Atomic Energy Insights. Volume 2, Issue 4. 1996. <http://www.atomicinsights.com/jul96/SL-1cause.html>.

System Failure Case Studies
A product of the NASA Safety Center

Executive Editor: Steve Wander stephen.m.wander@nasa.gov

To view this document online and/or to find additional System Failure Case Studies, go to http://pbma.nasa.gov