Date Thu, 28 Oct 1999 103110 -0600
From Meredith Brown racer@lanl.gov
Subject: Yellow Alert- Reactivity Control Program Deficiency

Title Reactivity Control Program Deficiency Discovered during Software Testing

Identifier 1999-LA-LANL-ESH7-0017 Date 10/28/99

LESSONS LEARNED: Borland C++ software control programs may need to incorporate additional coding to compensate for the C++ communication library BIOS command that slows down processing to one character per second when communication between the computer control system and the associated equipment is lost. C++ software was used to control scrams for criticality experiments at a nuclear facility, where the previously unidentified software delay could have allowed an assembly to return to a supercritical state after a scram. The software problem was not discovered in a timely manner because the facility's procedure for validation and approval of new and modified equipment did not contain specific review and approval requirements for software.

DISCUSSION: A general-purpose assembly machine used for criticality experiments failed to remain in a shutdown condition after watchdog circuitry initiated a scram during a quality assurance software verification test. The remotely operated machine was not fueled during the test. The assembly uses two stacks of uranium foils and Plexiglas plates that are moved towards each other to allow supercritical operation. A hydraulic ram is used to quickly move the lower stack a predefined distance from the upper stack, and then a stepping motor is used to move the stacks together. During a scram, the hydraulic ram is programmed to move the stacks rapidly to the most conservative position. The software test involved raising the lower stack to simulate the addition of positive reactivity during normal operations. While the hydraulic ram was moving up, operators disconnected a communication cable to trigger the watchdog circuitry. The watchdog circuitry began the scram sequence when it sensed the loss of communication. When the communication cable was reinstalled during the shutdown sequence, the ram terminated its withdrawal and began lifting the stack again without a new command being entered to raise the stack. Operators repeated the test multiple times, and the improper scram response was intermittently reproduced several times. Facility personnel suspected that the system's secondary memory was not resetting following the scram, which allowed the assembly's hydraulic valves to return to their previous position when the communication cable was reinstalled. To test this theory, personnel inserted a command into a test version of the control software to reset the valves to their neutral positions when communications are reestablished following a watchdog scram. This modification was tested approximately 50 times with no errors detected. Personnel also discovered that the Borland C++ communication library BIOS command slows down the communication to one character per second when it appears to have lost communication. Depending on how much of the control program has been executed and how many commands are left when the link is lost, it may take up to two minutes before the primary computer sends a scram signal to the secondary computer. If communication is reestablished before the primary computer initiates a scram, the secondary computer will restore power, causing the hydraulic valves to return to their previous position.

RECOMMENDATIONS/ACTIONS: Facility management concluded that inadequate resources had been allocated for development and implementation of a formal verification and validation process and for software configuration management. To correct this deficiency, both short- and long-term plans were developed to upgrade the facility's software quality assurance program. The assembly control program was also modified to reset the memory for the secondary computer.

ORIGINATOR Los Alamos National Laboratory
CONTACT Gordon Medford, 505-667-2463 or maddog@lanl.gov
AUTHORIZED DERIVATIVE CLASSIFIER Meredith Brown, 505 667 0604
REVIEWING OFFICIAL Meredith Brown, 505 667 0604
DOE FUNCTIONAL CATEGORY Criticality
WORK ACTIVITY Instrumentation & Control
HAZARDS Radiological
KEYWORDS scram, C++, BIOS, criticality
REFERENCES ALO-LA-LANL-TA18-1998-0011

FOLLOW-UP ACTIONS: Information in this report is accurate to the best of our knowledge. As a means of measuring the effectiveness of this report, please contact the originator of significant action(s) taken as a result of this report or of any technical inaccuracies you find. Your feedback is appreciated.