PENNSTATE

College of Engineering
Radiation Science and Engineering Center

(814) 865-6351
FAX: (814) 863-4840

Breazeale Nuclear Reactor Building
The Pennsylvania State University
University Park, PA 16802-2301

October 18, 1996

Nuclear Regulatory Commission
Document Control Desk
Washington, DC 20555

Re: Station Advisory Notice: PROTROL Software Deficiency
License No. R-2, Docket Nol 50-05

Dear Sir or Madame:

On September 13, 1996, a PROTROL (AECL product) software crash occurred on the Penn State Breazeale Reactor (PSBR) DCC–Z monitoring computer when an unusually long update period was inserted for a real-time trend display. The reactor was secured during this event. At the request of AECL, on September 18, 1996 with the reactor secured, a long update period was entered on the DCC-X control computer and it also experienced a software crash with a resulting watchdog trip indication. For the PSBR console, a separate analog system meets all of the Tech Specs requirements as the safety system, hence the reactor safety was not compromised. Further details of this event are described in the attached Station Advisory Notice from AECL dated September 30, 1996.

On September 19, 1996, AECL indicated that since PROTROL is not used in a safety system at PSBR, they would not have to report it as a part 10CFR21 but would probably do so as a convenient method of getting out this information. On September 23, 1996 PSBR conveyed this information to Tom Dragoun at Region I.

On September 30, 1996, the PSBR and three other plants received a Station Advisory Notice: PROTROL Software Deficiency report from AECL. We are assuming this indicates that AECL decided to use the Station Advisory Notice instead of doing a 10CFR21.

A copy of the Station Advisory Notice is attached for informational purposes and to clarify with Region I that this is in lieu of a part 10CFR21 as earlier indicated to Tom Dragoun at Region I.

Sincerely,

Warren F. Witzig

Warren F. Witzig
Director

Attachment

cc. Region I Administrator
PSBR File

AECL EACL

2251 Speakman Drive
Mississauga Ontario
Canada L5K 1B2
(905) 823-9060 + Ext.
(905) 823-9040
Fax (905) 823-8006

2251 rue Speakman
Mississauga (Ontario)
Canada L5K 1B2
(905) 823-9060 + poste
(905) 823-9040
Fax (905) 823-8006

SAN96-1

1996 September 30

Mr. Mac Bryan
Radiation Science and Engineering Centre
Penn State Breazeale Reactor
University Park, PA
USA 16802

Dear Mr. Bryan,

Station Advisory Notice: *PROTROL* Software Deficiency

This letter and the attached Station Advisory Notice (SAN) serve to inform Penn State Radiation Science and Engineering Centre of the discovery of and possible implications of a deficiency in *PROTROL* software operating in a system provided to your facility by AECL.

AECL requests that you distribute this notice to your staff responsible for the *PROTROL* system, and that its implications for your organization be carefully considered.

AECL stands prepared to discuss the technical issues of this deficiency with your technical personnel. The AECL contact for technical questions is David Fournier, whom you may contact by phone at 905-823-9060, extension 3568, by fax at 905-823-2205, or via e-mail at FournierD@aecl.ca.

AECL further requests that you confirm receipt of this letter and SAN by fax or e-mail to David Fournier.

Yours truly,

J. Pauksens

fr Shaun Cotnam
Account Manager

c: R.D. Fournier
D.A. Meneley
R.A. Olmstead
J. Pauksens

SAN 96-1c
96.09.25

STATION ADVISORY NOTICE

PROTROL[tm] Software Deficiency

Affected Plant/Facility

Penn State University, Breazeale Reactor

STATION ADVISORY NOTICE

SAN 96-1c
96.09.25

PROTROL™ Software Deficiency

Affected Plants/Facilities:

a) Philadelphia Electric Company, Peach Bottom Atomic Power Station
b) GPU Nuclear, Oyster Creek Nuclear Generating Station
c) Penn State Breazeale Reactor
d) King Faud University of Petroleum and Minerals, Energy Research Laboratory

Note: In the above cited nuclear reactor applications, the *PROTROL* system is used for process control, and is not part of the safety systems of the plant, which are completely separate, independent and fully capable of mitigating any fault arising in the *PROTROL* systems.

Purpose:

This bulletin is to advise *PROTROL* users of a deficiency in *PROTROL* software which was discovered by Penn State University staff on September 13, 1996, and to advise our customers of the appropriate procedural precautions to completely avoid the deficiency..

Description:

Discovery Of The Deficiency

Penn State University (PSU) operates a Digital Control Console for its Breazeale Reactor, which includes two *PROTROL* systems used for control and monitoring. DCC-X (digital control computer X) is used for control (in a non-redundant configuration), and DCC-Z is used for extra monitoring, as well as support of printer, historical data storage and LAN connections..

While attempting to configure a real-time trend display on DCC-Z to obtain a plot that would display a 5-day trend, an operator set the update period of the real-time trend to

900 seconds (i.e. a new pixel would be plotted every 900 seconds, filling the 600-pixel wide screen in approximately 5 days). The DCC software immediately failed.

The failure was characterized as follows: the trend plot appeared to paint the screen abnormally fast, most screen functions stopped, and the time scale for the trend showed negative values for time.

PSU repeated this on DCC-X at AECL's request, and the hardware timer (watchdog) immediately dropped out. *(see explanation below of the watchdog function)*

Analysis of the Deficiency

The fundamental time tick of the *PROTROL* kernel is about 27.5 ms. A task running at 900 s intervals thus has a count-down register setpoint of $900/.0275 \approx 32768$. This indicates that the fundamental mechanism for the failure is integer wrap-around in the count-down register for the trend task, which affected its scheduling.

This deficiency is excited when a task period is set greater than about 892 seconds, or about 1000 times the typical values used, such as 0.2 seconds to 1.0 second. (Most displays are useful only if running at the same rate as the control programs, such as FWC which runs at 0.225 or 0.375 seconds).

On the CPUs used in the DFCS systems (10 to 20 MHz '286 or '386 systems) the result of this wrap-around of the count-down register is to make the affected task ready and due to run constantly, thus hogging the CPU. On such relatively slow processors, this results in the self-test program not getting to run and do its self-tests and, if these pass, refresh the watchdog. Thus the watchdog will drop within 2 seconds of pressing the ENTER key to activate an improperly edited trends or barchart display.

Our analysis indicates that the only possible ways of exciting this deficiency are:

- interactively editing the real-time trend display update period to > 892 seconds (i.e. a new pixel about every 15 minutes, so it takes about 5 days to fill the screen)
- interactively editing the bar chart similarly
- off-line editing of the TASKS.DAT file to set the period of any task to be 892 seconds or more (not a major concern since this file is read-only, and should never be modified)

The only realistic means of exciting the deficiency involves interactively editing the barchart or trend display sets. This involves quite different keystrokes than merely viewing the displays, as shown below:

The keystroke sequence to view a trend or barchart is as follows:

- press up/down cursor to select the display set
- press ENTER to display the trend or bar set

The keystroke sequence which excites the deficiency involves editing a trend or barchart then viewing it and is:

- press up/down cursor to select the display set
- press 'F4' to edit
- edit the second field (the display period) to a value of 892 or more
- press 'F3' to capture this change
- press ENTER to display the trend or bar set

ENTRY OF VALUES LESS THAN 892 WILL NOT EXCITE THE DEFICIENCY.

Role of the Watchdog Hardware Timer

All *PROTROL* systems used in sensitive applications that could have important operational implications include an external hardware watchdog timer. This timer must be periodically refreshed by special software routines or its relay contacts open (These contacts are hardwired according to the requirements of the application.) The watchdog timer thus provides a diverse check that all the software is behaving within acceptable bounds. In this case, for example, because the control programs are effectively locked out, so too is the self-test program, which guarantees that the watchdog will not be refreshed. The precise effects of the watchdog dropping out depend upon the details of the application.

Impact on Dual-Channel (DCC-X/DCC-Y) Systems

Tuning and changes of display settings are normally performed on only one DCC at a time. *PROTROL* redundancy is such that there is no software connection between the two DCCs. The watchdogs on the two DCCs determine which DCC controls the plant process. Thus if both DCC-X and DCC-Y are "fit" (running normally and on-line), and the period of a trend or bar display is changed to a value greater than 892 in one of the DCCs, the affected DCC will shut down, and circuits controlled by the watchdogs will ensure that the other DCC will continue to control the plant. If both watchdogs drop out, the control system outputs assume designed states which depend upon the application.

Plant-Specific Impact And Recommendations

Penn State University Breazeale Reactor

System Description

PSU uses one DCC in its control and monitoring system for control (DCC-X), and a second DCC as an additional display/monitoring unit (DCC-Z) . The DCC-X watchdog contacts are hardwired as an additional SCRAM parameter to the hard-wired reactor trip system. There is no watchdog on DCC-Z, as it does display only. All safety functions are completely external to the DCCs.

Possible Impact of the Deficiency

There is no problem if the systems are left as is, and there is no problem if the maintainer views existing bar or trend sets.

There is no problem for all useful and reasonable values of trend update periods (e.g. .3 s, 1.0 s, 5 s).

If a maintainer sets the real-time trend or barchart update period to a value of 892 seconds or longer (i.e. one pixel plotted every 15 minutes) the affected DCC will fail. For DCC-X, this means the control rod drives will be left in place, and the watchdog will drop out. While there will not be any reactor power transient, the drop-out of the watchdog (which is essentailly a hardware timer) will immediately cause a reactor scram. For DCC-Z, this will merely incapacitate DCC-Z, requiring the operator to reboot it.

Recommendations:

1. Ensure that the maintainer is cautioned to set display periods of less than 5 seconds or so, to minimize the likelihood of a keyboarding error that could accidentally cause a value much larger to be entered. If week-long trend displays are needed, then the period should be set to 720 seconds (12 minutes per pixel).

fn=SAN96-1c