Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire

CMD 18-H6.72

File / dossier: 6.01.07
Date: 2018-05-07
Edocs: 5529913

Oral Presentation

Submission from Louis Bertrand

Exposé oral

Mémoire de Louis Bertrand

In the Matter of

Ontario Power Generation Inc., Pickering Nuclear Generating Station

Request for a ten-year renewal of its Nuclear Power Reactor Operating Licence for the Pickering Nuclear Generating Station

Commission Public Hearing – Part 2

June 2018

À l'égard de

Ontario Power Generation Inc., centrale nucléaire de Pickering

Demande de renouvellement, pour une période de dix ans, de son permis d'exploitation d'un réacteur nucléaire de puissance à la centrale nucléaire de Pickering

Audience publique de la Commission – Partie 2

Juin 2018

Canada

Canadian Nuclear Safety Commission
Attn: Louise Levert
Secretariat
by email: cnsc.interventions.ccsn@canada.ca

From: Louis Bertrand, P.Eng.

Re: Hearing 2018-h-03 Pickering NGS relicensing

To the Commission,

I wish to make an oral intervention at the public hearings scheduled for June 26-28, 2018.

The present email is my written intervention in the hearing process.

My professional background is electrical engineering, with a focus on microcontrollers and firmware development. I am concerned about the aging computer equipment in process control at the Pickering NGS. Computers and software cannot be treated as just another component; the failure modes are radically different. I do not believe that the conventional probabilistic risk assessment methodology can reliably account for computer related failures.

The hardware relies on 1970s era mini-computers such as the PDP-11 made by Digital Equipment Corp (DEC). As the equipment ages so does the chances of the failure of one or more integrated circuits. In that era, transistor-transistor logic (TTL) was prevalent, using bipolar junction transistors (BJT). This technology demands a relatively large current from the power supply and consequently dissipates a lot of power as heat. Heat accelerates the natural failure modes of the transistors and interconnections in the integrated circuits.

Minicomputers are obviously no longer available (in fact, DEC is no longer in business, having been bought out by Compaq, which in turn was bought out by Hewlett-Packard). Repairing those old computer boards would be an arduous task and the uncertainty about the reliability of the repair itself should be a major concern. Worse, if the computers are of a later generation, they may use custom integrated circuits which would longer be available (other than maybe as "pulls" from scrapped boards). The old 74-series TTL ICs are at least still available.

Of equal, or perhaps greater concern is the software running on those computers. The software industry is familiar with a phenomenon known as "software rot". This is the idea that software's usefulness and reliability degrades over time, as if there was a real decay process at work. Actually it is not the software itself that degrades (the binary files are intact), but rather the environment in which it operates that changes and slowly reveals incompatibilities, or takes the thread of control through previously unused portions of the software where unexpected defects may be triggered. To counter this, software maintainers must decide between looking backwards and adapting new software to the new equipment; or adopting a new platform and developing new software. As time goes by the costs of doing either increases: legacy equipment

is impossible to find; or the new software requirements become increasingly more onerous in terms of development time and effort.

A legitimate line of questioning to OPG would be to assess the computer hardware-software maintenance capabilities of the organization over time, as equipment fails and as expert staff members retire or pass away. Another legitimate line would be to assess the ability of the organization to develop new programs or modify existing ones to adapt to newer conditions. What are the processes in place to ensure that the software is validated as doing the job it is required to do? What are the testing protocols in place? Are the testers the same as the developers, or is there an independent QA review team? Is the modified software subject to a review by an arms-length independent expert?

I would encourage the Commission to hire a team of independent experts in software development processes to audit OPGs capabilities to maintain its existing code base and develop new software.

Finally, I wish to make several short points about my concerns with the continued operation of the Pickering nuclear generating station.

1 -- OPG is proposing to operate the Pickering reactors well beyond their design life (210,000 full power hours), up to 295,000 full power hours. This number is outside any gray zone of uncertainty about the reliability calculations, and the decision to continue operating to 2024 does not seem to be evidence based.

2 -- The Pickering NGS, once out in a rural area beyond the suburbs of Toronto, is now surrounded by residences, businesses, schools and nursing homes. The city of Pickering is no longer a small suburban village. A large release of radioactive substances during an accident would have a catastrophic impact on Pickering and the adjacent city of Toronto.

3 -- The provincial nuclear emergency response plan, though recently revised, still has no response to a large release accident such as the one that crippled the Fukushima Dai-Ichi station in 2011. I don't believe that the municipal and provincial authorities would be able to devise a safe and effective ad-hoc plan for a large release accident within the time scale of the accident, 24 hours or so. To support my point, I invite you to observe the daily traffic jams on highway 401 through Scarborough and Pickering -- and that's just the commuters.

4 -- OPG must be mandated to make plans for the short term decommissioning of the Pickering reactors. The current plan, to wait 30 or more years before dismantling the station, is unfairly burdening future generations with the expense and risks resulting from the present day operations.

Thank you for your attention.