From: FLEET Barry -NUCLEAR [mailto:barry.fleet@opg.com]
Sent: Friday, November 16, 2012 9:20 AM
To: Consultation; Dallaire, Mark
Cc: WILLIAMS Don -DNNP; MACEACHERON R J -NUCLEAR; HARRIS Elaine -NUCLEAR; CHACHEL Robert -NUCLEAR; FLEET Barry -NUCLEAR; ROMAGNINO John -NUCLEAR; SAAR Cathy -NUCLEAR; THURSTON Anna -REL EST SRVC
Subject: OPG Commernts on draft GD-337, "Design of New Nuclear Power Plants"

N-CORR-00531 P

CD#: N-CORR-00531-05972

Dear Mr. Dallaire,

The purpose of this email is to provide a written submission of OPG comments for the public consultation on draft GD-337, "Design of New Nuclear Power Plants".

Please find attached below a Table listing OPG comments on GD-337. To assist in the dispositioning, the table has been provided in both PDF and WORD format.

If you have any questions regarding OPG's submission, please contact Mr. Don Williams, Senior Manager, Design Review, Darlington New Nuclear Project, at (905) 839-1151, ext. 5673.

Barry Fleet
Manager, Station Support
Nuclear Regulatory Affairs
8-702-5198
bb: 905-626-4660

OPG comments on GD-337, Guidance for the Design of New Nuclear Power Plants

	Document section/excerpt of section	OPG issue	Suggested change
1	RD-337 - general	The timing of the public consultation for comments on RD-337 has not allowed sufficient time for them to be incorporated into GD-337.	OPG (and others) have submitted detailed comments for RD-337 version 2. These comments have not yet been considered for incorporation into GD-337. OPG's comments from RD-337 should be reviewed by the CNSC to determine applicability to GD-337. With respect to "design extension conditions" and "complementary design features", this document should be revised throughout to be consistent with the resolution of OPG's comments regarding such terms in its review of the draft RD-337 version 2.
2	Preface This document provides expectations and guidance on how to meet the requirements set out in regulatory document RD-337 version 2, *Design of New Nuclear Power Plants*. Section 1.0 Purpose This document provides expectations and guidance on how to meet the requirements set out in regulatory document RD-337 version 2, *Design of New Nuclear Power Plants*.	Suggest deleting the word "expectations". This document is intended to provide "guidance", not "requirements". However, the term "expectations" may be construed to mean "requirements" and should therefore be omitted.	Change text as follows: Preface "This document provides guidance on how to meet the requirements set out in regulatory document RD-337 version 2, *Design of New Nuclear Power Plants*." Purpose "This document provides guidance on how to meet the requirements set out in regulatory document RD-337 version 2, *Design of New Nuclear Power Plants*."
3	Section 2.0 Scope Further guidance can be obtained from relevant Canadian codes and	Codes and standards referenced in the guide refer to specific revisions. It is unlikely GD-337 will be updated with	Change text as follows: "Further guidance can be obtained from relevant

	Document section/excerpt of section	OPG issue	Suggested change
	standards, as well as appropriate international standards, such as IAEA publications.	the frequency necessary reflect the most recent version of all relevant codes and standards going forward. Suggest adding text to indicate that information can be found in the codes and standards listed or latest codes and standards as applicable, as appropriately agreed.	Canadian codes and standards, as well as, appropriate international standards, such as IAEA publications. *It should be confirmed that the codes and standards used in the design of a new nuclear plant are the applicable codes and standards, as agreed to by the regulator*."
4	Section 5.3 (Page 6) and elsewhere	Reference to CSA N286-05 should be changed to CSA N286-12.	Replace "CSA N286-05" with "CSA N286-12" throughout.
5	Section 7.4.2, page 18 Natural external hazards considered in the design include"	As noted earlier in this section, hazards are evaluated and may be screened out based on extremely low probability. The statement in question implies no such screening (as may be the case for the listed "geomagnetic storm").	Change text as follows: "Natural external hazards considered in the *evaluation* include..."
6	Section 7.9.1, Page 29 The monitoring should not be limited to process variables of safety and safety-related systems. It should extend to the monitoring of radiation, hydrogen, seismic, loose parts, vibration, and fatigue.	Installation of I&C equipment to monitor for loose parts and fatigue is not practical. Suggest removing these items from the recommended list of parameters to be monitored.	Change text as follows: "The monitoring should not be limited to process variables of safety and safety-related systems. It should extend to the monitoring of radiation, hydrogen, seismic, and vibration."
7	Section 7.9.2, 3rd Paragraph The software provided by a third-party	In some cases, widely used and proven third-party software was not developed to standards equivalent to those used	Add a sentence at the end of the paragraph:

	Document section/excerpt of section	OPG issue	Suggested change
	should have the same level of qualification as for software that is written specifically for the application. The qualification of software should be verified through the national or international standards relevant to the qualification activities of pre-developed software.	for software written specifically for the application.	"...When the third-party software was not developed to equivalent standards, a qualification plan and qualification report should be prepared to demonstrate that this software is fit for its intended purpose."
8	Section 7.9.2, last bullet - verifiability should refer to the extent to which the development processes and outputs have been created to facilitate verification using both static methods and testing	Editorial inconsistency. Change "should refer" to "refers".	Change text as follows: "Verifiability *refers* to the extent to which the development processes and outputs have been created to facilitate verification using both static methods and testing "
9	Section 7.9.3: Instrumentation is also provided for recording vital plant parameters and variables, including:	Suggest to characterize the shown list of vital plant parameters as examples (i.e., "such as") rather than "including". The licensee should determine and justify the vital parameters to be recorded for accident monitoring. Also, "hydrogen concentration" may be inferred rather than directly measured.	Change text as follows: "Instrumentation is also provided for recording vital plant parameters and variables, *such as*:"

	Document section/excerpt of section	OPG issue	Suggested change
10	Section 7.10 Pre-installed equipment can be credited after 30 minutes where only control room actions are needed or after 1 hour if field actions are needed.	The Industry standard of 15 minutes for operator action in the control room and 30 minutes for operator action outside of the control is reasonable and has been validated. The basis and justification for changing from the current industry standard practice needs to be provided. This proposed change could also unnecessarily increase the cost and complexity of plant design.	Change text as follows: "Pre-installed equipment can only be credited after a minimum of 15 minutes where only control room actions are needed, or after a minimum of 30 minutes, if field actions are needed."
11	Section 7.10, last sentence Guidance on redundant connection points for temporary services is described in section 7.3.4.	The reference to section 7.3.4 is unclear. Please clarify or remove this reference.	Clarity is required for the purpose of connection within the design.
12	Section 7.13.1 - a plant level HCLPF being at least 1.67 times the design basis earthquake	Recommend that the basis for a plant level HCLPF at 1.67 times the DBE be explained or referenced.	Basis for a plant level HCLPF at 1.67 times the DBE be explained or referenced.
13	Section 7.13.1 Beyond design basis margin should be such that seismically induced SSC failure probabilities do not contribute to the total core damage frequency and small and large release frequency to the extent that they do not meet the	Are the two acceptance criteria bullets in addition to the safety goal criteria for BDBE?	Clarity is required

	Document section/excerpt of section	OPG issue	Suggested change
	safety goals. The acceptance criteria for beyond design basis earthquake should be: - a plant level HCLPF being at least 1.67 times the design basis earthquake - the containment integrity in the case of beyond design basis earthquake		
14	Section 7.13.1 The acceptance criteria for beyond design basis earthquake should be: - the containment integrity in the case of beyond design basis earthquake	It Is unclear. Is this to say that containment cannot fail for BDBEs?	Change text as follows: - " There is an appropriate level of confidence that containment integrity can be maintained in the case of a BDBE"
15	Section 7.21 Human factors, Analysis, 2nd last paragraph The design should also provide research or study reports for any work carried out as part of the process of developing and testing any new	As earlier stated, there are already HFE Program Plans and HFE Verification and Validation Plans and associated V&V reports. Any study reports regarding use of new HMI technologies would be covered by these.	Delete this paragraph. ~~"The design should also provide research or study reports for any work carried out as part of the process of developing and testing any new human-system interface technologies (i.e., displays and controls) that are new to NPP applications and that may have a bearing on safety."~~

	Document section/excerpt of section	OPG issue	Suggested change
	human-system interface technologies (i.e., displays and controls) that are new to NPP applications and that may have a bearing on safety.		
16	Section 7.21 Human factors, Operating personnel, 2nd paragraph Formal interfaces should be defined between the HF in design group(s) and the various design engineering groups involved in the design process; this facilitates the interactions and sharing of information to achieve good integration of HF considerations in the design.	There should not be a presumption of a particular design organization.	Delete this paragraph. "~~Formal interfaces should be defined between the HF in design group(s) and the various design engineering groups involved in the design process; this facilitates the interactions and sharing of information to achieve good integration of HF considerations in the design~~."
17	Section 7.21 Human factors, Planning, last sentence There should be a sufficient number of trained, qualified and experienced HF specialists to carry out the HF in design activities.	There should be a graded approach with respect to HF in design such that for simple HMI issues, use of an HF specialist is not necessary.	Change text to: "There should be a sufficient number of trained, qualified and experienced HF specialists to carry out the HF in design activities *where these meet established criteria pertaining to system complexity and importance to safety*."

	Document section/excerpt of section	OPG issue	Suggested change
18	Section 7.22.4 Cyber security, first set of bullets on p54 • communication of plant data between the plant and the emergency control centre (either onsite or offsite) should be via unidirectional link	In the last bullet, the use of the word "unidirectional" may be counter-productive. Change "unidirectional links" to "secure protocols".	Change text as follows: "• communication of plant data between the plant and the emergency control centre (either onsite or offsite) should be via *secure protocols* "
19	Section 7.22.4 Cyber security, last set of bullets on p53 The following should be considered for the protection of computer-based I&C systems and components important to safety functions: • the computer-based I&C systems and components important to safety should be protected, along with those support systems and components which, if compromised, would adversely affect safety functions • cyber attacks include either physical or logical threats (with either malicious or non-malicious intent), originated from inside and outside of the perimeter of the system's facility • computer-based systems and	The 4th of 5 bullets is excessive since the key systems requiring protection are already covered by the first and fifth bullets.	Delete the 4th bullet. "~~• any computer-based system, either autonomous or non-autonomous, should be protected~~ "

	Document section/excerpt of section	OPG issue	Suggested change
	components includes computer hardware, software, firmware, and interfaces • any computer-based system, either autonomous or non-autonomous, should be protected • computer-based systems and components for the functions of emergency preparedness system, physical security and safeguards, should be protected, if applicable for the design		
20	Section 7.22.4 Cyber security, last set of bullets on p54 • implementation should not impact performance, including response time, effectiveness or operation of safety functions	The first bullet is unrealistic and does not focus on adverse impacts, which is what we should be concerned with. Change "should not impact" to "should not adversely impact".	Change text as follows: "• implementation should not *adversely* impact performance, including response time, effectiveness or operation of safety functions "
21	Section 8.4: As stated in RD-337 version 2, "redundancy shall be provided in the fast acting means of shutdown" unless the safety analysis demonstrates that, for any AOO or DBA coincident with failure of a single fast acting means of	It is interpreted from this discussion that both of the two independent means of shutdown do not necessarily have to be "fast acting" (only one needs to be). It is proposed to add a statement in the present guidance document to explicitly clarify this	Change text as follows: "Redundancy shall be provided in the fast acting means of shutdown" unless the safety analysis demonstrates that, for any AOO or DBA coincident with failure of a single fast acting means of shutdown, the acceptance criteria can be met. *In which case, only one fast acting*

	Document section/excerpt of section	OPG issue	Suggested change
	shutdown, the acceptance criteria can be met.	point.	*means of shutdown would be required."*
22	Section 8.4.2 The reliability evaluation should be such that the reliability of the shutdown function is such that the cumulative frequency of failure to shutdown on demand can be shown to be less than 10^{-5} failures per demand, and the contribution of all sequences involving failure to shutdown to the large release frequency of the safety goals can be shown to be less than 10^{-7}/yr.	Regarding the reliability of the shutdown function, the basis for the guidance to show 10^{-5} or less failures per demand and 10^{-7}/yr or less contribution to the LRF safety goal are not clear.	Please clarify
23	Section 8.10.4 As stated in RD-337 version 2, "*if operator action is required for actuation of any safety system or safety support system equipment following indication of the necessity for operator action inside the control rooms, there is at least 30 minutes available before the operator action is required*".	OPG has made a comment on the referenced section of RD-337. The basis and justification for changing from an Industry standard of 30 minutes for operator action outside of the control needs to be provided. This change does not appear to be consistent with IAEA guidance.	Please ensure consistency with the updated RD-337.
24	Section 9.4	It is proposed to include the supplementary guide to CSA N286.7.	Reference: *Guideline for the application of N286.7-99, Quality assurance of analytical, scientific, and design computer*

	Document section/excerpt of section	OPG issue	Suggested change
			programs for nuclear power plants (November 2009).
25	Glossary	For clarity and completeness, include a definition for the phrase "alternate AC power", which appears in the definition of "station blackout". Definition should be consistent with G-306 revision.	Add definition as follows: "**Alternate AC Power** - An alternating current power sources that is available to, and located at (or nearby) a reactor facility, and is characterized by the following: 1. Is connected to but not normally connected to the offsite or onsite standby and emergency AC power system, 2. Has minimum potential for common mode failure with offsite power to the onsite standby and emergency AC power sources, 3. Is available in a timely manner after the onset of station blackout, and 4. Has sufficient capacity and reliability for operation all the systems required for coping with station blackout, and for the duration of the required to bring and maintain the plant in a safe shutdown state."