From: George Vayssier [mailto:george.vayssier@hetnet.nl]
Sent: Thursday, October 4, 2012
To: Blahoianu, Andrei; Viktorov, Alexandre
Subject: Review of GD-337

Hi Andrei,
It was a pleasure to meet you and discuss with you during the August meeting in Vienna. You handed me there the draft GD-337, for my eventual comments.
It took me some time before I managed to read and comment the draft GD-337, but now I can offer you my comments.
I have split them up in two parts: a general and a specific part.
Overall, I believe, it is a very good document. But I believe it could be stronger in terms of defending against severe accidents, also in view of the lessons learned after Fukushima. Now, the whole world is revising its policy in this matter, so that is not surprising. I missed also a clear reference to what has been achieved in various modern designs, such as the EPR, AP1000, etc. The GD-337 is there very cautious, where I believe stronger wording could be applied. Of course, it is hooked on RD-337, which is already somewhat older, at least pre-Fukushima.
Further, I have added remarks on the transition DBA-BDBA, which you also addressed during the meeting. The solution seems to be in shifting the traditional DBA somewhat in the direction of the DECs, plus a fully risk-oriented approach, as has been proposed by Commissioner Apostolakis and is also supported by the ASME 'New Safety Construct' and the NTTF-report. Personally, I believe we could even go further, as one of the major goals of new designs should be that they should never cause a societal disruption, as we have seen occurring at Fukushima. ASME mentions this, but Apostolakis does not yet go that far. I have worded this carefully, as the separation between DBAs and BDBAs/DECs is somewhat a religion in nuclear safety - not easy to convert the believers... I send you per separate mail also my comments to Commissioner Apostolakis, as he gave me his (only) paper copy which he had with him at the meeting. I felt I should do more than just saying 'thank you'. Some of this may also be of interest to you.
There are a number of items of more 'classical' nature, such as system classification, QA, etc. These you will find in the section with specific comments. I attach the system classification of the EPR (through the mail to Apostolakis), which I believe is quite advanced. I also attach here my own recent publication on SAMG - so that you also know some of my ideas.
Andrei, I could not read all relevant documents - so some of my comments are covered by reports which I did not or did not fully read. And I am not familiar with Canadian regulatory documents - some concerns may be alleviated if I would better know these. I have not tried to be 'nice and friendly' - you are not served by praise, but by what might be improved.

I hope you will have some use of my observations. Will be pleased to discuss them with you or your staff at an upcoming possibility (e.g. the SAMG assessment which I plan with Alex).
With my best regards,
George
PS. A copy to Alex, as he is my main contact with the CNSC.

Comments on the CNSC draft GD-337,
'Guidance for the Design of New Nuclear Power Plants'

Author: George Vayssier, NSC Netherlands

Date: 3 October 2012

1. Overall comments.

1.1. The draft is a comprehensive guidance to meet the requirements of RD-337 and, as such, a useful guide for users who wish to apply RD-337. It is good to see that there are ample references to IAEA documents, which includes that further experience is obtained in applying IAEA standards which will, in turn, also benefit the IAEA and, thereby, the international nuclear safety community. Some questions here, however, remain (see below).

1.2. In a number of cases reference is made to other documents, e.g. the IAEA documents, as mentioned. It is not clear whether these documents are *endorsed* by the CNSC, i.e. if the applicant refers to these in his application, his application will be approved. The Preface speaks about 'adoption of principles set forth in SSR 2/1', which is not identical as endorsing SSR 2/1, after adaptation to the national Canadian requirements.

In addition, if reference is made to a Safety Guide, it should be realised that automatically the underlying requirements are included, as the Safety Guide only describes one method to meet the requirements. From the text in GD-337 it is not clear whether this indeed is meant, as sometimes a Safety Guide is mentioned, followed separately and only later by the Safety Requirements (e.g. sec. 5, GS-G-3.5, followed later by GS-R-3).

It should be noted that IAEA documents often refer to national criteria, e.g. acceptance criteria for design extension conditions (DECs) and, hence, a reference to such documents should include identification and quantification of such statements (in this case, acceptance criteria are not defined, but safety goals instead; the difference being acceptance criteria being mandatory, whereas safety goals are targets, values that should be reached, if possible).

Note: the IAEA definition of acceptance criteria is not useful, as it contains a loop (it requires understanding of another term, the definition of which depends again on understanding the meaning of 'acceptance criteria').

1.3. In a number of cases ‘additional information’ is mentioned, plus a document where this information can be found. The status of such documents is not fully clear. Are they endorsed by the CNSC for application? If not, what use should the applicant make of such documents? A specific case is sec. 5.6, where IAEA GSR Part 4 is mentioned. This is a very detailed and comprehensive document, which describes in detail how the safety assessment of an NPP must be performed (*must*, i.e. it is a requirement, a ‘shall’ statement). Does CNSC follow indeed this document, either in whole or in part? If so, then many other paragraphs of GD-337 become redundant, as the GSR Part 4 treats these subjects. As said, GSR Part 4 is no guidance document, it is a requirements document, so it is of other nature and at a higher level.
1.4. Similarly, where reference is made to e.g. US-standards, it should be noted that these have originated in and refer to the US regulatory environment (e.g. IEEE, ASME standards). It has not been specified to what extent these foreign regulations have been endorsed by the CNSC.
1.5. A Safety Guide is a document, providing guidance how Requirements are met, not more, not less. In principle, therefore, each paragraph should contain a ‘should’ statement. ‘Information only’ paragraphs have, in principle, no place in such a guide. You can see this in practice in the IAEA Safety Guides, which almost exclusively use the word ‘should’ in each paragraph. The IAEA has also information documents, but these are of different character (Tecdocs, Safety Series Reports, etc.). Alternatively, ‘information only’ parts could be placed in footnotes, annexes, etc. Mixing them with the main guidance text may cause misunderstanding of their use.
1.6. It seems that post-Fukushima lessons are not yet processed in GD-337. For example, there is no reference to the Canadian Fukushima Task Force Report, INFO-0824, which gives a number of fairly strong recommendations. There are other reports about the lessons learned, such as the USNRC SECY 12-0095, and the ASME Presidential Report ‘Forging a New Safety Construct’, June 2012 (sec. 6.7), as well as the French ‘hard safety core’ approach. For example, a severe accident does not only cause radiological consequences for people and the environment, but may also cause societal disruption, i.e. a widely-spread disruption of normal life in a society. Examples are thousands of people who must evacuate their livings in the mid of the night, with the perspective of never being able to return to their homes. And/or contamination of an industrial area, causing a widely-spread loss of economic activity and loss of jobs. If a harbour is struck, also the hinterland can be severely struck, as transport of food and goods via that harbour may come to a complete standstill. Societal disruption is also addressed in the ASME-report mentioned.
The Gd-337 does not treat such consequences. The underlying problem is that the RD-337 does not contain these either.
1.7. Finally, the GD-337 stays with the traditional approach of designing against design basis accidents (DBAs) and ‘having something available’ for accidents beyond

(BDBAs/DECs) In this area, no hard criteria are defined, but safety goals. Although this exceeds the role of GD-337, it may be time to upgrade the DBA by including some DECs (e.g. ATWS, SBO, Loss of Ultimate Heat Sink - LUHS) into the DBA and placing firm requirements on DECs involving core melts. These could include defined measures against steam generator tube creep rupture, against fuel bundle meltthrough, against (calandria) vessel meltthrough, against possible fuel-concrete interaction, against the threat of hydrogen combustion for the containment integrity, and against overpressure of the containment by non-condensable gases. In short, by defining safety functions typically needed to mitigate severe accidents, and requiring measures to fulfill them.
For GD-337, this - at present - necessarily must take the form of recommendations, as the underlying RD-337 does not require such functions to be fulfilled inside predefined acceptance criteria.
An example of such requirements is in USNRC SECY 93-087, added upon by various SECY-docs (e.g. latest now is SECY 12-0095, with reference to earlier ones) following the Fukushima accident. Also the NRC study revealed the at present 'scattered regulatory approach' of some BDBA, as ATWS, SBO, etc.
For widening the DBA and including BDBA/DEC into the 'safety construct', a good reference is also the ASME-report already mentioned about 'forging a new safety construct'. The document proposes an all-risk treatment of both DBA and BDBA/DEC, which is also proposed by an NRC-task force, led by Commissioner Apostolakis: A Proposed Risk Management Regulatory Framework, April 2012.

2. Specific comments.

2.1. Sec. 4.2.4 (accident management) should also refer to the CNSC guide GD-306, 'Severe Accident Management Programs for Nuclear Reactors, and the IAEA NS-G-2.15, 'Safety Guide on Severe Accident Management'. The assessment of the accident management program by the CNSC could follow the IAEA Services Series Report SVS-9, 'Guidelines for the Review of Accident Management Programs in NPPs'. For information (if that part is retained in the Guide), a useful document is IAEA Safety Report Series SRS 32, 'Implementation of Accident Management Programs in NPPs'.
Accident management starts, of course, with Emergency Operating Procedures. A useful document is the Safety Reports Series SRS 48, 'Development and Review of Plant Specific Emergency Operating Procedures' (this is not a Safety Guide).
Note that the field of EOPs-SAMG is strongly in motion after Fukushima: in the US, the FLEX approach is advocated, augmented with Extensive Damage Mitigation Guidelines (EDMGs), which re-establish command and control after an event where a large part of the plant area is destroyed (possibly through violent actions by third parties). A similar approach is followed in France, through the 'hard core approach'.
The whole series of accident procedures then becomes then: AOP (Abnormal Operating Procedures), EOPs, FLEX , EDMG, SAMG.
Note: a certain consideration of portable equipment (FLEX) is given in the last paragraph of sec. 7.3.4.1.
Robustness against severe accidents for new plants is described in SECY 93-087. The CNSC approach should be compared whether it is equivalent.

It should also be compared with the findings of the NRC post-Fukushima NTTF recommendations.
2.2. Sec. 5 (management systems) refers to IAEA GS-R-3. A widely used standard is ASME NQA-1; there exist also an IAEA comparison document on GS-R-3 and NQA-1-2008 and NQA-1a-2009 addenda, which describes inter alia what elements are in NQA-1 which are missing in R-3, and vice versa (Safety Reports Series SRS 70). Note: I did not see a comparison document between CSA N286-05 and ASME NQA-1, it may exist.
2.3. Sec. 6.6.1 (multi-unit site) should possibly take into account lessons from Fukushima, inter alia a common cause failure, damaging more than one unit simultaneously.
2.4. Sec. 7.1 (safety system classification) seems to 'borrow' items from the draft IAEA Safety Guide DS 367, such as the concept of 'preventive and mitigative' safety functions. The concept of 'preventive' safety functions, unique in the IAEA draft guide, was not welcomed by industry - it does not reflect industry practices. At present, the safety guide is still in draft form.
In addition, an overall classification of both pressure retaining components and components fulfilling safety functions (e.g., ECCS) has been abandoned by e.g. US and French industry, after such a system had been set up in earlier versions of safety classification. ANS 58.14 (1993) describes this process in an Appendix. Now there are various classification schemes: for safety, for pressure integrity, for electrical, for seismic, for environmental loads and for QA. A possible inter-linkage between them is presented in ANS 58.14 (1993), Table 7.1.
Although it is not the function of this document to comment the requirements of RD-337, it should be noted that they allow declassification if the probability that the safety function will be called upon is low. Most safety classification schemes assign the safety class only to the safety function of a component, irrespective of the probability that the safety function is called upon. For example, ECCS is a safety function, irrespective of the quality of the primary pressure boundary, whose failure will cause the ECCS to operate. Improving the quality of the primary pressure boundary has no effect on the quality of the design of the ECCS. Where RD-337 allows this, the guide GD-337 should make clear that such declassification is not acceptable.
There should also be no more safety classes than there are industry codes that define the design requirements for particular components. Otherwise, the classification loses much of its meaning.
A very mature safety classification system is that of the EPR, which defines also classification for systems that mitigate DECs. For DECs w/o core melt this is Risk Reduction Catagory A (RRC-A) and for DECs including core melt this is RRC-B.
GD-337 mentions for such systems only that they should have a 'high' safety classification, w/o specifying what that should be.
Note: in the draft DS 367, systems mitigating DECs are classified one class lower than the systems mitigating DBAs. Is this what the CNSC would agree on?
The GD-337 should clearly define what is:
- a preventive safety function,

- a mitigative (mitigatory) safety function,
- the iterative process of safety classification,
as these are not obvious in the context of the document or defined in the glossary.
Note: ‘preventive / mitigative functions’ do not appear in IAEA SSR2/1, neither in the IAEA safety glossary. ‘Safety group’ is defined both in the IAEA glossary and the GD-337 glossary up to and including DBAs, not for DECs.
2.5. Sec. 7.6.2 (single failure, SF) hooks the SF, as in IAEA documents, on the performance of a safety group. Where the safety group is the assembly of equipment to mitigate a given PIE. If we take as an example SBLOCA, we need shutdown, ECCS, containment isolation, containment cooling and containment atmosphere cleanup. This total equipment then constitutes the safety group. The SF principle as defined for the group then requires only one failure to be considered in the whole group. In practice, however, containment isolation is redundant, i.e. SF-proof, as is the ECCS and the shutdown. Hence, the usual design is stronger than the regulation requires. Possibly, the SF should not be hooked on the safety group, but on each individual safety function. This is also the approach taken in ANS 58.14 (either 1993 or 2011 version).
Sometimes people understand the safety group concept in another way, as a safety system comprises more equipment than the safety function requires. For example, an ECCS has jockey pumps, which are not classified for safety, as they are not required during the PIE. Hence, another interpretation of safety group is to consider only those parts of the system which have a safety function during the PIE for which they are designed. In that case, the SF definition for safety groups is valid and does not underrate present designs.
Note 1: present good practice in many designs is to have three of four redundancies for relevant safety equipment (e.g., 4 x 100 % ECCS, 3 x 100 % diesels, etc.). To cover this issue, one could recommend that the SF is also fulfilled during periods of testing and inspection. Note 2: this is formally now only required in Germany in what is called SF+. (single failure plus).
2.6. Sec. 7.7 (codes for pressure retaining components) refers to CSA N285-0-08 and ASME BPVC. To require (formally ‘recommend’) these codes as a minimum is, I believe, an extremely important statement. Nevertheless, these codes do not themselves classify SSC, that is part of the safety classification. For example, see ANS 58.14, where ASME III classes are assigned to various safety classes. I believe, therefore, that sec. 7.7. should refer back to the safety classification.
Leak-before-break (LBB): there is no clear recommendation to apply the concept of LBB. This is, I believe, below the present design of new reactors, which have at least LBB. In addition, some applications go beyond that and require a no-break philosophy (such as in the UK, France and Germany). In France, this has been included in the newest RCC-M (the ‘French ASME-code’) and in Germany in KTA 3206 (at present draft), ‘Analysis Regarding Rupture Preclusion for Pressure Retaining Components’.
I see no reason to deviate for new reactors from this new international standard.
2.7.. Sec. 7.8 (equipment qualification). Also here a reference to safety classification would be useful. Sec. 7.8.4. does not include a recommendation that the equipment should be qualified for DECs. NS-G-2.15 recommends even dedicated equipment to

mitigate DECs. The increased weight of mitigating severe accidents after Fukushima apparently has not been considered while writing this paragraph

2.8. Sec. 7.9 should include a reference to safety system classification. See ANS 58.14 (1993), Table 7.1.

2.9. Sec. 7.13.1 (seismic design and classification): it is not clear whether a DBA and an SSE (safe shutdown earthquake) need to be combined, as is done in many countries. Hence, SSE is not a DBA, but a complication of the DBA (such as LBLOCA). The reason is that an SSE can occur during the whole plant life, not excluding moments where the DBA is postulated to occur. Other countries take a probabilistic approach and believe than SSE and DBA do not occur simultaneously. I never heard of a country assuming the occurrence of a DBA being greater during an SSE and, therefore, possibly combining these on probabilistic grounds.

2.10. Sec. 8.1.0.1 (nuclear design) seems to accept a positive feedback during accidents. Although this was acceptable in Canada during the past, due to the inherent positive reactivity feedback during LOCAs, there exists ample technology to avoid such positive feedback. It is recommended to make this a clear recommendation in GD-337: avoid positive reactivity feedback during accidents (e.g. during LOCA) or compensate it through inherent reactor characteristics (e.g. during steam line break). No engineered safety features should be needed for new reactors to mitigate positive reactivity feedback. Note 1: this may need enriched fuel, but there is no defendable case to increase risk by abstaining from enriched uranium. Note 2: reactivity coefficients may be different during start-up. This should also be considered in analysing reactivity coefficients (sometimes the moderator temperature coefficient is positive).

2.11 Sec. 8.2. (Pressuriser design). The volume of the pressuriser and the pressuriser pressure control system should be such that secondary transients do not (or seldom) lead to opening of the primary pressure relief valves.

2.12. Sec. 8.3.2 (steam and feedwater piping). Modern designs often use LBB for steam lines. In addition, the steam lines outside the containment up to the first anchor are often designed for break exclusion, to prevent SG blowdown outside containment and to protect the containment against pipe whip (see e.g. USNRC Branch Technical Position 3-4).

2.13. Sec. 8.6.2 (containment strength). There should be a clear recommendation that the containment under DEC-loads will remain intact during a pre-specified time (e.g. 24 hours - USNRC approach) and thereafter still provide an effective barrier against the escape of fission products into the environment. Note: there is not a corresponding clear requirement on the containment in RD-337 either. Although this document does not comment RD-337, such a requirement should be placed on new reactor designs. The requirement that the containment function under a severe accident must provide sufficient time to implement emergency measures (RD-337, sec. 8.6.12) is far too weak! The prevention of core-concrete interaction is only covered by a recommendation (‘should’),

not by a requirement. RD-337 is not the place for recommendations, it should define the requirements. Hence, measures to prevent core-concrete interaction are not required! As such, RD-337 lags behind modern developments (EPR, AP1000, AES2006, ESBWR, etc.)
2.14. Sec. 8.6.12 (DECs). Filters should also be protected against hydrogen combustion, notably where the filter condenses the steam and, hence, makes vented gases combustible.
2.15. Sec. 8.8 (emergency heat removal). One of the paramount characteristics of defence against severe accidents is the EHRS function also during severe accidents. This is neither required in RD-337, nor recommended in GD-337, and, as such, does not comply with IAEA regulations and underrates present modern designs (as in sec. 8.6.2).
2.16. Sec. 8.9.1 (Batteries). No time is specified batteries should provide power during an SBO. A load shedding program - to decouple non-essential loads - should be made available.
2.17. Sec. 8.9.2 (Alternate AC). In some countries, NPPs have special connections to neighbouring plants to strengthen their AC. Possibly difficult for very large countries like Canada.
2.18. Sec. 8.10.1 (control room). The habitability of the control room should be specified for a minimum duration, also during DECs, e.g. 72 hours. Also the habitability of the SCR and ESC should be considered for a minimum duration.