NRCExecSec Resource

From: Bob Budnitz <budnitz@pacbell.net>
Sent: Monday, December 30, 2013 4:26 PM
To: NRCExecSec Resource
Subject: Robert Budnitz letter to NRC on SECY-13-0132 (Dec. 30, 2013)
Attachments: Robert Budnitz letter to NRC on SECY-13-0132 (Dec. 30 2013).pdf

TO:
Annette L. Vietti-Cook
Secretary, US Nuclear Regulatory Commission

FROM:
Robert J. Budnitz
734 The Alameda
Berkeley CA 94707

Attached as a PDF file is a letter that I am submitting to you as a public comment on SECY-13-0132, "Staff Recommendation for the Disposition of Recommendation 1 of the Near Term Task Force Report." I am directing this to the Commissioners, and will also send a copy to Mark Satorius (EDO) for his information.

I have written this as a private citizen, as the introductory paragraph of the letter explains. Can you please acknowledge receipt? An email reply wold be sufficient.

Sincerely,
ROBERT J. BUDNITZ

Robert J. Budnitz
734 The Alameda
Berkeley CA 94707
home telephone (510)527-9775
home e-mail: budnitz@pacbell.net

30 December 2013

TO: Annette L. Vietti-Cook
Secretary, US. Nuclear Regulatory Commission
(sent by email to NRCExecSec@nrc.gov and intended for the Commissioners)

COPY TO: Mark Satorius, NRC Executive Director of Operations

SUBJECT: Individual public comment on SECY-13-0132 (December 6, 2013), "Staff Recommendation for the Disposition of Recommendation 1 of the Near Term Task Force Report"

INTRODUCTION and BACKGROUND

I am writing this as a private citizen. This note is intended to provide my personal input to assist the NRC Commission as it deliberates on the staff recommendations in SECY-13-0132 concerning Recommendation One of the NTTF Report.

I am employed at the University of California's Lawrence Berkeley National Laboratory (LBNL), one of the DOE national laboratories. However, I am not a stranger to the NRC -- I was once (1979-1980, a long time ago) the Director of NRC's Office of Nuclear Regulatory Research (RES), and in the intervening years, after leaving the NRC staff in 1980, I have worked as a contractor on a wide variety of NRC projects, mostly for RES but a few for NRR and recently NRO. Most of these projects have been technical (that is, research to develop new knowledge or new methods), but a few have been more directly related to improving a specific regulatory approach or assisting the NRC staff in reviewing an applicant's or licensee's submittal. For decades, and based in part on my early experience as RES Director, I have had a special interest in seeing that the NRC is well focused on fulfilling its safety mission, and that it carries out its work effectively and efficiently. This note is being written with that as a motivation.

For 5-plus years, I have been the Principal Investigator on a set of several interlocking LBNL projects funded by NRC-RES (Office of Nuclear Regulatory Research), all related in one way or another to the issue of the seismic safety of LWRs. One of these projects, NRC-RES Project V6159, underway since August 2010, is called "*Technology-Neutral Framework for Performance-Based and Risk-Informed Approaches for Structural and Seismic Safety.*"

In the course of this NRC-supported work over the past few years, I have developed a set of ideas about how to improve the way the NRC regulations and other regulatory positions deal with the seismic safety of large LWRs. These ideas have led me to the technical proposals that I will write about below, but I need to insist that this is a letter from a private citizen, not endorsed by anybody else, and not necessarily what will emerge at the end of my current NRC-supported project in this same area.

However, I would be remiss if I didn't note that, in the course of the NRC project noted above, I have written a draft report that will perhaps be published as a NUREG/CR report, if and when it gets through the NRC staff review process. The draft report is entitled, "*Toward a More Risk-Informed and Performance-Based Framework for the Regulation of the Seismic Safety of Nuclear Power Plants.*" It lays out an approach for a rather thorough revisiting of the way NRC regulates the seismic safety of LWRs, based on risk-informed and performance-based ideas.

And that is the idea that I wish to advance here. (See below.) My specific ideas about how to revisit the way seismic safety of LWRs is regulated are intended to be an example of how to approach the larger issue of revisiting the body of LWR safety regulations more generally – I therefore proffer the issue of seismic-safety regulation of large LWRs to the Commission as an example or as a "case study."

NTTF RECOMMENDATION ONE

The reason for this note is that I am very disappointed with the NRC staff response in SECY-13-0132 to the NTTF Report's Recommendation One. I will explain why, and will make recommendations about what different course might be taken to alleviate my disappointment. I will concentrate exclusively on the safety regulation of large LWRs.

When I studied the NTTF report two years ago, I was very much struck by NTTF Recommendation One, which says that the NRC ought to establish a "*logical, systematic and coherent regulatory framework for adequate protection that appropriately balances defense-in-depth and risk considerations.*"

I thought (and still think) that this was intended to be a potential vehicle for a broad-based and fundamental revisiting of the framework of regulation, to incorporate a range of risk considerations into NRC's reactor-safety regulations in a way that is not present now, or at least is only present sporadically rather than consistently in those regulations. Specifically, while the current NRC regulations for LWR safety do a pretty good job of incorporating defense-in-depth ideas, they do only a sporadic and inconsistent job of using risk considerations in the regulations. Compared to what I think should be the approach vis-à-vis Recommendation One, the staff in SECY-13-0132 recommends a much more limited set of actions to achieve a much more limited set of objectives. These actions and objectives are all worthy, but in my personal view they are far from what could be accomplished by taking a broader view.

In the technical area I'm addressing here, the seismic safety of LWRs, I believe that a fundamental revisiting of the way NRC regulates has great promise of achieving a number of important endpoints. I believe that, if guided by appropriate NRC Commission policies, there is a good prospect that the community of experts (both on

the NRC staff and in the affected industry, and with input from the broader public) can produce a set of regulations (and Regulatory Guides, Standard Review Plan sections, other staff positions, inspection modules, etc.) that in this technical area would represent a more rational basis for regulation, would use staff resources more effectively, would be a basis for more effective use of industry resources to meet the regulations, would make the safety of our LWRs more understandable, would save lots of industry and NRC money, and most importantly would improve safety (although the safety achieved today in this area is generally more than adequate in my view.) That list of potential benefits sounds like "too good to be true," but in my view it is certainly within reach in this technical area. I can't prove it, but realizing each of those benefits seems more than plausible to me: it seems obvious, albeit in different measures for different situations.

Given the above, I have been hoping first that the Commission (in response to NTTF Recommendation One) would set in place policies to encourage (perhaps even require) revisiting the LWR safety regulations systematically. I have further been hoping that, if this were to occur, the staff might choose the seismic-safety area as one "case study" to examine how much could be accomplished, how, and why. My disappointment is because I see almost nothing even close to being that expansive in my reading of SECY-13-0132. I am very much disappointed in how narrowly the SECY paper interprets what I read into Recommendation One, and I want to try to affect the agency's deliberations. Hence this note.

THE TECHNICAL BASIS FOR MY RECOMMENDATIONS

My technical argument in the seismic-safety area goes as follows. Here I will only touch on the highlights, will leave out some elements of my overall recommended approach, and will only explain the most fundamental reasons why revisiting the seismic-safety regulations makes sense. (Further details are in the draft report mentioned above, but that report is still in draft form awaiting review, and I don't want to rely on it here. This is a letter from me acting as a private citizen.)

My argument has the following elements:

o When the current seismic-safety regulatory positions (CFR, SRP, Reg Guides, staff positions, etc.) was put in place, mostly in the 1960s-1970s-1980s time frame, nobody could do realistic analysis of how the plants actually behave in large earthquakes. Hence, nobody could quantify the "margins," nor understand the major "risk contributors," nor know "how safe the plants are" against a figure of merit like the annual core-damage frequency (CDF), nor know where there might be leverage for changes to improve things.

o Today we can do that realistic analysis – so we can quantify the "margins" (albeit with some uncertainty), we can and do understand on a plant-specific basis the major contributors to the seismic part of the overall risk profile, we can compare our understanding to figures of merit like CDF, and we can ascertain where today's regulations can be improved, even though they already lead to plants that are "adequately safe."

o The improvements in our knowledge have occurred in several different technical areas: we understand the seismic hazard better; we understand how to analyze the seismic capacity of our structures and components better; we can do better systems analysis to understand how the safety of the whole emerges from and depends on the "parts"; and we have an NRC-endorsed consensus-based American National Standard (the ASME-ANS PRA standard) that guides how this analysis is to be done properly. We therefore have a basis for "rationalizing" the seismic regulations using risk-informed and performance-based insights that we didn't have even a decade ago.

o However, there is much more to it. Let me explain starting with the issue of the various code committees. When the AEC and early NRC were putting together the NRC's seismic-safety regulations and the Reg Guides etc. for LWRs, they asked the various consensus code committees to take then-current (non-nuclear) codes and standards for seismic-safety design and analysis and convert them to "nuclear" codes and standards – there was to be more margin, embedded QA, better and more prescribed analysis, better review and inspection, and so on. Each code committee complied, with of course lots of AEC/NRC staff input. These consensus codes have been updated over the years, but this early work (and especially the philosophy embedded in the codes at that time) is still essentially still in place, and it provides the fundamental basis for today's NRC regulation of seismic safety of LWRs. Thus, concrete in NRC-regulated LWRs is to be designed and analyzed for seismic safety according to ACI codes; mechanical equipment according to ASME codes; structures according to ASCE codes; electric equipment (transformers, DC buses, etc.) according to IEEE codes, and so on, based on hazard inputs take in part from ANS standards. [1]

o Of course, each code committee embedded "margins" in their codes, as is necessary, but each did it (appropriately) with different technical issues in mind. Crucially, each did their work independently of the others.

o Let me give a stylized example: Imagine an LWR heat exchanger whose tank is designed and qualified for seismic safety under ASME, sitting on a concrete pad designed under ACI, connected to an electrical bus done under IEEE, inside an auxiliary building done according to ASCE, and so on. All of the designers have used the NRC's design-basis-earthquakes (the SSE, the safe-shutdown-earthquake, and the OBE, the operating basis earthquake) as the prescribed input earthquake motions. What is the item's seismic "margin," in the sense of asking how much extra seismic motion above the design basis can that heat exchanger resist before it gets into trouble in terms of performing its safety function? Well, a realistic analysis can tell us, relying where appropriate in part on test data or earthquake-experience data, and we now know how to do that analysis. However, no such realistic analysis is required by regulation. Meeting the design codes and analysis codes is sufficient. But the various design and analysis codes represent quite a mixture of very different technical considerations – each of them entirely sensible if viewed one-by-one, but an odd (perhaps even incommensurable) set of requirements when taken together. To meet NRC regulations, a "regulatory analysis" must be done and is done to meet the Standard Review Plan, checking against the

---

[1] ACI is the American Concrete Institute. ASME is the American Society of Mechanical Engineers. ASCE is the American Society of Civil Engineers. IEEE is the Institute of Electrical and Electronics Engineers. ANS is the American Nuclear Society.

design basis, and if all is OK the item's safety is found to be "adequate," and hence the item is licensable. But today, while that is true, this seems highly unsatisfactory, given that we can really know so much more, but do not choose to ask!

o But there is more! Each structure or component is designed and analyzed individually to show that it meets the NRC regulations. No account is taken of the fact that various structures and components need to "work together" to make the plant adequately safe against earthquakes. It is assumed that if each item is acceptable then the system is acceptably safe. And in my judgment this is so. But the overall design is not coordinated, and this represents a waste of resources, industry resources and regulatory resources both, because the overall plant design is very much suboptimized (actually, hardly optimized at all.) Further, this represents a major lost opportunity, because of the suboptimality, and also because neither the regulator nor the industry (nor the public!) understands the overall seismic safety achieved as well as they could. Today the technical community knows how to take into account the interaction aspects of a complex design like that of a large LWR in responding to large earthquakes, by using systems-analysis methods, in both design and analysis. However, nobody requires it, and it has not generally been done.

The analyses done in the seismic PRAs bear out the observation that some items have much more seismic "margin" than others, so savings could ensue without compromising safety if things were more rationally balanced. Furthermore, if the analyses that are feasible today were used more fully in regulation, regulatory emphasis could be directed more toward those items and issues which "matter more" to seismic safety. This is the philosophy underlying the NRC's Reactor Oversight Process today, but this approach isn't used fully in the seismic-safety area, in part because not all plants have the analyses and many of those that do don't use them.

o There is still more! The "regulatory analysis" deals with the "design basis" – the NRC's design basis earthquakes (the so-called Safe Shutdown Earthquake and Operating Basis Earthquake.) Fine. However, today no full account is taken in regulatory decision-making of how the individual structures and components perform their individual safety function(s) at various beyond-design-basis earthquake loads (and furthermore, even if so, knowing individual performance wouldn't account for the behavior of the systems and functions in which these items are embedded.) Yet today we can do that analysis too. To support regulatory decisions, however, we don't.

o Still more! Today's seismic PRAs reveal that, while the plants are "adequately safe," their seismic "risk profile" is often dominated by the seismic failure of a single structure or component, albeit the dominant risk arises for earthquakes well beyond the design basis. For many operating LWRs, this seismic risk profile looks very much "out of balance" if examined carefully – a more "balanced" risk profile would not have almost all of the seismic risk of CDF dominated by a single failure. But this imbalance has generally not been accounted for in the design phase, and there has never been a mechanism with regulatory underpinnings to encourage (or require) an LWR designer to make some changes to "spread out the seismic risk" across a broader base of structural or component failures. Yet for newly designed plants, those not yet licensed and built, this is easy to accomplish if a requirement were in place to do so. The risk would be more evenly spread, the plant would be more robust, and hence the plant would be "safer" somehow.

I hesitate to call this a "defense-in-depth" issue, because those words are so "loaded," but I will: If the seismic safety (the "seismic risk profile") of an LWR relies so heavily on the performance of a single item (a structure or component), then if I suppose that that single item is somehow "weaker" than we think (because we've made an unknown error), the entire seismic risk profile of that plant would be concomitantly "less safe", and we wouldn't know it. Said another way, if we suppose that the seismic risk profile "looks fine" to the NRC as analyzed, but that the error I've just postulated exists, then isn't the NRC's understanding of the seismic risk profile in error, and aren't we all unknowingly more confident than we should be? Isn't "defense-in-depth" supposed to assure that something like this does not occur? That is, isn't such a plant relying too heavily on our understanding of that single item to keep its seismic risk profile in line?

o One other technical issue is worth discussing. Specifically, in the library of seismic PRAs on my shelf, a couple dozen in number, many of the important seismic accident sequences involve non-seismic failures or human errors as well as earthquake-caused failures. That is, some sequences involve only earthquake-caused failures, while others (perhaps a third or a half of them) require a non-seismic failure or a human error too before the sequence would lead to a core-damage accident. This observation – this "fact" -- has been known for 30 years. Yet no account is taken of this fact in how the NRC regulates seismic safety of LWRs. NRC's regulations generally address the seismic adequacy of one structure or component at a time – period. Admittedly, the seismic PRAs have generally found that the seismic CDF of our operating LWRs is in an acceptable range. But still -- no regulatory requirements address this "fact" or do anything with it directly. The closest one might come is that, in a regulatory action for an operating LWR that invokes Reg. Guide 1.174, one might observe that the best way to improve the safety of a given accident sequence is to improve the non-seismic-failure or human-error aspect of that accident sequence. But that is indirect, not addressed head-on, and almost a "back-door" acknowledgment of the fact I've cited. A second way this fact might enter into seismic safety regulation is when a new design needs to meet the NRC requirement (in the SRM attached to SECY 93-087 in 1993) that the plant-level HCLPF seismic capacity meet or exceed 1.67 times the SSE. I won't devote space here to explaining why this link is also sort of a "back door" link, but that is how I see it.

In my view, although framing a set of regulatory positions to account for this fact will not be easy, and addressing it will require risk-informed thinking, leaving it permanently unaddressed, as it is now, seems to me to be unsatisfactory.

MY BOTTOM LINE

First, in my opinion advances like those I seek in the seismic-safety area will not likely occur without the NRC being "at the front of the charge." To be sure, the NRC cannot do this alone. Crucially, the consensus code committees play a vital role (and appropriately so!), but in my view not enough progress will happen without the NRC playing a leadership role. This means that the Commission needs to set in place the right set of policies, and the staff needs to devote its resources to the effort (meaning staff expertise in NRR and NRO as well as in RES, funds to help support the code committees, and funds for research projects to develop specific technical bases.)

Also, because this is fundamentally an issue of revising regulations and supporting regulatory positions, the leadership in this area needs, in my view, to come from NRR

and NRO, with RES playing a supporting role as needed. If the Commission turns this over to RES, without requiring NRR and NRO to be intimately involved from the top, it will likely "get lost." I know – I was once the Director of RES. And this is not casting aspersions on the RES leadership, whom I greatly admire.

Specific to the seismic-safety technical area, I recommend that the "community" of reactor-seismic-safety experts, working in part through the code committees and with strong NRC involvement, establish a 5-to-10-year program to address each of the technical issues I've raised above, one-by-one but beginning all-at-once. The goal is to come up, some years hence, with a much more rationalized approach to regulating seismic-safety design and analysis. Because current NRC regulatory positions lean so heavily on the consensus industry codes and standards (and appropriately so!), working though the code committees, as best I can figure, is the only way to get this program of work done.

o The outcome would be, in the reactor-seismic-safety area, a new set of regulatory positions that address head-on the issues that led the NTTF Task Force to write NTTF Recommendation One. The work would also – and not by accident – address head-on part of what the NRC's Risk Management Task Force seems to be seeking to do in NUREG-2150. I did not write "not by accident" because I used NUREG-2150 as a basis – far from it, because I had this whole set of ideas mostly framed in my mind before NUREG-2150 was published. This is "not by accident" because I am by no means alone in trying to think through how to make our seismic safety regulations more rational, more understandable, less expensive for regulators and licensees, and also able to achieve safety advances more rationally too.

o One other issue is very much worth mentioning, and that is my opinion on how difficult this work might be. In my opinion, bringing NRC regulations in seismic safety more in line with the thinking above would not be breaking totally new ground. To its credit, the U.S. Department of Energy's regulatory approach in this technical area has been miles ahead of NRC for a long while. Their DOE Standard 1020 has for many years (since 1994, revised in 2002) been using many (not all, but many) of these risk-informed and performance-based concepts for both design and evaluation, so as to assure adequate seismic safety of DOE's own nuclear facilities. Furthermore, at least one of the relevant code committees has gone a long way down the right path – specifically, the American Society of Civil Engineers Standard ASCE 43-05 (2005) embeds a lot of very forward thinking on this set of subjects in the area of seismic design criteria for nuclear facilities. In Reg Guide 1-208, the NRC staff has endorsed selected parts (but by no means the bulk) of ASCE 43-05's thinking on risk-informed, performance-based seismic design.

MY RECOMMENDATIONS

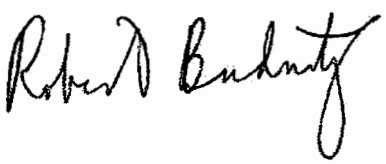
As I wrote at the top of this note, I am deeply disappointed that SECY-13-0132 stops so far short of what I had hoped it would recommend, in terms of a long-term set of agency actions, initiatives, and research projects. I am writing this letter to try to influence the Commission's (and the staff's) deliberations to change that.

Although I believe that the major recommendations in SECY-13-0132 are excellent and should be endorsed by the Commission, (1) I recommend that the Commission should

ask the staff to take seriously what I think are the key underlying reasons why the NTTF wrote Recommendation One to begin with. This means that (2) I recommend that the Commission should reject SECY-13-0132's delineation of the "problem statement" on page 4 of the SECY paper. That "problem statement" is, in my view, much too limited in vision and scope. Instead, (3) I recommend that the Commission should task the staff with developing a plan for a more fundamental long-term set of agency actions, initiatives, and research projects, leading ultimately to re-visiting (in each relevant technical safety area) the body of regulations, so as to take fully into account up-to-date methods of design, analysis, and evaluation, which rely in part on modern advances in engineering and on risk perspectives -- so as thereby to gain the benefits agency-wide that are like those I've outlined above in the seismic safety area for LWRs.

This will not be quick and it will not be easy. In the seismic-safety area, this is likely to be a 5- to 10-year effort. The effort can start with the consensus code committees, in parallel with work by the staff (and ultimately the Commission) on the issues embedded in the current SECY-13-0132 paper, namely issues about defense-in-depth, and about what to do in regulation to address accidents beyond today's design basis. I also believe that the seismic-safety area is likely an ideal "case study" topic, in large part because so much thinking has already been done in that area (DOE is a giant-step ahead of the NRC already), and also because the community of experts is very much "ripe" for this set of advances.

Sincerely,



Robert J. Budnitz