**From:** erniestinyworld [redacted]
**Sent:** October-28-16 8:10 PM
**To:** Consultation (CNSC/CCSN)
**Subject:** DIS-16-05 preliminary responses to questions asked in the DRAFT document

**Q1. Do you agree with the definition of human performance as stated above? Are there changes or alternative definitions you would propose?**

It might be helpful to clearly state what is meant by “safe” and “risk". Sven Hansson, “Safety is an inherently inconsistent concept”, Safety Science, 50 (2012) 1522-1527, provides a good discussion around the issue of vague meaning of safety and how to clarify its use. Similarly, the term “risk” has vague meaning without further clarification. This comment may seem trivial, but these terms appear to be essential to the purpose of the work related to human performance, so it should be clear what we mean by them.

For example on page 3, "To ensure the safe operation of a nuclear facility, continual improvement of provisions that influence human performance should be considered at all organizational levels.”; some may interpret a “near miss” as unsafe; an internal radiation release could be interpreted as not safe even though no public harm resulted. Clarification on what is meant by risk seems to be appropriate as well.

The scope of “humans” should be clarified. There are many mentions of “workers”, “work”, “work conditions”, “routine work”, and so forth. It seems we are talking about paid professionals carrying out their duties although a worker (defined in common usage) is not necessarily paid. Also, do we exclude the public from the scope of humans in this context? This is an important point because, in an accident, the public has shared responsibility for response. A perhaps extreme example is the Mt St Helens volcano where the resort owner, Harry Truman, refused to comply with repeated warnings to leave and ultimately perished as a consequence.

With a clear understanding of “safety" and “risk” (if we agree these are the objective parameters), then it would seem good to isolate “human activities” to those that are important. That is, many activities at work may not be considered important (it would be easy to have examples here) to "human performance” in the context we have in the document.

A nuclear power plant might be said to be at safe level when it is in compliance with all local, regional, and federal codes, standards and laws. We could also say (define) compliance is the plant design. The plant safety level is then defined as the probability of consequential harm (that is, radiation exposure in excess of legal limits) to the public when operated within its design. The plant can be said to be “safe” when operated within its design (although this does not preclude the possibility for catastrophic failures.)

We could define tasks activities) meant to maintain the required plant design as “safety-crititical tasks”. Anything a plant employee does that would reduce the level of safety (implement a non-conforming design, improperly maintain an equipment required for accident mitigation or prevention, and so forth) by deviating from the design we could refer to as a "safety-critical error”.

After clearly defining what is meant by safety, and the expected level of safety, we might have a clearer idea of the definition as follows:

**Alternative human performance definition:** completion of a safety-critical task carried out by employees, contractors, or the public.

**Q 2. Do you propose any changes or alternatives to the CNSC's existing definition of human factors? Please provide rationale for any proposed changes or alternatives.**

The concept of human factors as explained in the document are strongly related to organization and management of the plant. Organizational and managerial decision-making put in place barriers against mistakes that could otherwise lead to deviation from the plant design (that is, reductions in the level of safety). Decision-making regarding the listed organizational barriers are good; all are well-known in helping reduce the likelihood for errors.

Based on the previous response to Q1 and the organizational decisions that can be made to increase the likelihood a safety-critical task is completed error-free, we might want to define Human factors as follows:

**Alternative human factors definition:** Organizational decisions that increase the likelihood safety-critical tasks are performed error-free.

**Q 3. Do you agree with the objectives and practices of a human performance program listed above? Are there items that you would add to or remove from the lists? Please explain.**

In my opinion, focus on the bullet "consideration of human performance as the work actually carried out by individual workers (as opposed to an idealized view of work as anticipated or designed)" is the most important one assuming the design requirements are clear to the person performing a safety-critical task. This places a very high burden on the organization's management, one that in this writer's opinion, is not typically carried out (but not clearly specified as needed); for example, see Catchpole and Wiegmann, Understanding safety and performance in the cardiac operating room: from 'sharp end' to 'blunt end', BMJ Qual Saf 2012;21:807-809 doi:10.1136/bmjqs-2012-001135 where this level of effort is alluded to.

Based on the recognition of this kind of organizational breakdown ("as performed" not congruent with "as imagined") my opinion is that management involvement in safety-critical task performance should be required as part of any human performance program. That is, no safety-critical task should be performed absent direct management involvement. For example, in many cases, management "approves" tasks without actually being involved in the task completion. The "approval" is in many cases simply an acknowledgement the task was done by the correct procedure, or correct forms were completed. This kind of "absentee ownership" (where it may occur) leads to the kinds of issues brought out in the literature on blunt end failures (one very interesting read is Schröder-Hinrichs, Hollnagel and Baldau, From Titanic to Costa Concordia — a century of lessons not learned, Journal of Maritime Affairs (2012)11:151–167).

**Q 4. Do you agree with the elements of a human performance program listed above? Are there items that you would add to or remove from the list above? Please explain.**
The organizational decision-making regarding the plant design (as discussed above) should be part of the human performance program. That is, how does the organization deliberate and arrive at conclusions regarding changes to safety-critical tasks? A "back-end" review should be made for each change to activities related to safety-critical tasks.

A "risk assessment" should be required for any change to the method a safety-critical task is completed to include a review of scenarios with catastrophic failure end states against the design requirement. The question should be asked and answered:

"Does this change increase or decrease the likelihood of catastrophic failure in any scenario.?"

**Q 5. Do you agree with the concept of a human performance program described above? If you would propose other ways of viewing a human performance program and its elements, please describe them.**

Some differences in emphasis are noted in the answer to Q4.

**Q 6. Do you think that the requirement to have a human performance program should be applied using a graded approach to all CNSC-licensed facilities and activities? If so, what might this graded approach look like?**

"Graded" approaches are generally not advisable. In my understanding they are based on quantitative risk assessments which are questionable, especially regarding human performance and organizational factors to risk. That is, probabilistic risk assessment is the typical approach and it (typically in my opinion) ignores organizational factors we are discussing in this document. Again in my opinion, by meeting the "design" as described previously in this email, nuclear power plants will have very low likelihood for catastrophic failure. The exception is the events at the Fukushima-Daichii plants following the great 2011 Tohoku earthquake. In this case, the plant designs were inadequate against the tsunami but presumably met all local, regional, federal codes, laws and standards.

**Q 7. Which type of human performance program (a formal program or otherwise) is most appropriate for the types of nuclear facilities most relevant to your comments, and why?**

In my opinion, a formal program is warranted. The main reason for a formal program is the well-known contribution to catastrophic failures (already described in the document) by organizational failures. Since the regulatory agency is the one responsible for the moral hazard created by the activity (operation of the nuclear plant), formal regulatory authority should be exercised for human performance. A potential difficulty is creating legally—defined standards

for the kind of activity to be regulated; this doesn't relieve the regulator from the responsibility to enforce proper performance of safety-critical activities.

**Q 8. Do you propose any additional or alternative expectations of a human performance program?**

Considerations have been stated in response to previous questions.

Ernie Kee