

**Hanford Advisory Board – Tank Waste Committee – February 4, 2016 draft Rev 5
Safety Culture – Discussion framing – Dirk Dunning, Lead Issue Manager**

Safety Culture

The Hanford Advisory Board has made several attempts at crafting and providing advice on the topic of Safety Culture. The resulting changes have not addressed the root issues and have been far less effective than desired.

The purpose of this discussion is to start at the beginning of why “Safety Culture” as a phrase and topic exists, to develop a common understanding among Committee and Board members, to identify the reasons why we have concerns, and to consider some possible paths to address these concerns, and thereby to better protect workers, the public and the environment, while also leading to improved design and operations. We may at the end recommend that DOE use a different name for this idea to make clear what is actually intended, and/or to break up the idea into its several major areas and name each accordingly (e.g. Design Safety, Operational Safety, Behavioral Safety, Industrial Hygiene, Training, Psychology, Culture, and Practice). This may lead us to recommend a change in how DOE views and evaluates risks and hazards.

The phrase “Safety Culture” has its origins in the Chernobyl Reactor Disaster. At its heart that disaster was made possible by design choices that traded safe design for efficiencies and cost reductions. In the aftermath of the disaster, an expert team was assembled to understand why the disaster happened, and to formulate some way to prevent similar disasters – ‘never again...’!

Lessons un-learned

The phrase “Safety Culture” is a direct result of the Chernobyl disaster. That disaster in turn was a direct result of a severely flawed design. That flawed design was the result of very poor choices about values involving efficiency and cost that led to tradeoffs in the design and applying mitigations to ‘adequately’ address safety.

Following the disaster at Chernobyl, an expert team was assembled to investigate and discover what happened. Based on those results, another expert group was assembled to find a way to prevent similar disasters from ever happening again. Their task wasn’t reactor design, or even nuclear in nature. Their task was more about human nature and complex systems design. They determined that at its most basic, this and many preceding disasters happened because of failures related to ‘safety’, not placing ‘safety’ first, and in the culture that existed, which led to complacency. They then carefully crafted a statement summing up that problem and trying to focus people on “Safety Culture” involved in design and operations. Here is their result:

Safety Culture defined (INSAG, 1988)

“That assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.”

Results and Problems

This phrasing though true fails to be useful or helpful. It does not clearly identify the root problems in design, in psychology, in operations, in training, in culture, reliance on mitigation for unsafe design and other factors. People generally fail to understand the definition, and they often fail to successfully apply

**Hanford Advisory Board – Tank Waste Committee – February 4, 2016 draft Rev 5
Safety Culture – Discussion framing – Dirk Dunning, Lead Issue Manager**

it to prevent problems. The operators at Chernobyl won many awards for their day to day safety and they apparently wrongly extrapolated that as applying to the inherent safety of the plant.

We have had many disasters before and since Chernobyl, such as: Bhopal India, the Challenger, the Columbia, Fukushima Japan, Deep Horizons in the Gulf of Mexico, the ongoing massive natural gas release at Aliso Canyon California, and many more. What is clear is that societally we learned precious little from Chernobyl or the other disasters.

At their heart, these disasters started by designs that traded safety for cost reductions and efficiency, or avoiding burdens on the design. They applied mitigations to offset the unsafe design. They then were precipitated by complacency born from lack of immediate accidents with severe consequences. And they finally concluded with unplanned or unlikely events leading to a major disaster. Good Safety Culture aims to prevent such issues.

Many teams in industry, at DOE and at other sites have developed their own ways of addressing this problem. DOE approached this through “Integrated Safety Management Systems” (ISMS), and other means. Other organizations used other terms. Each definition tends to be abstract and general and to be based on the INSAG definition. ISMS at its core repeats much of the approach called out in the original INSAG definition of Safety Culture. The result is equally difficult for the average person to put into practice.

Safe Design

At its heart, Safety Culture is first and foremost about designing safety into the design of facilities, operations, maintenance, and daily activities; and conversely designing out those aspects that result in safety hazards and risks. Safety Culture is not about identifying safety hazards and then finding ways to offset or mitigate them. That approach is a last resort to be used only when elimination of the hazards is not possible. Mitigation of inherent safety issues can and often does lead directly to other large safety issues and later failures as those involved forget why the mitigations exist.

More than this, Safety Culture is at its core about constantly searching for hazards and finding ways to remove those to the greatest degree practicable, throughout the entire life of the facility. Safety Culture is about training, operations, behavior, values, finding unrecognized problems and more.

Though Safety Culture does involve all aspects of safety, including day to day operations and industrial hygiene, these are not themselves the core of Safety Culture. Neither are they an indication of a healthy Safety Culture. Chernobyl was the clearest example of that. Despite frequent safety awards, the plant remained extremely dangerous and was obliterated in a relatively simple accident. The accident had enormous costs and consequences which go far beyond anything considered in the original safety analyses.

Examples of Issues

Proper application of Safety Culture runs counter to many prevailing philosophical ideas that are common in plant design and operations. Present nuclear culture has at its core an idea and approach that often flows through several stages.

- 1) develop a concept or proposal
- 2) identify ‘major’ hazards and risks

**Hanford Advisory Board – Tank Waste Committee – February 4, 2016 draft Rev 5
Safety Culture – Discussion framing – Dirk Dunning, Lead Issue Manager**

- 3) estimate likelihood and consequence of those risks
- 4) screen the results to eliminate from consideration any risks deemed to be highly unlikely (e.g. less than one in 100,000 per year)
- 5) evaluate ways to deal with risks that are unlikely (e.g. less than one in 1,000 per year)
- 6) mitigate risks that are likely

This analysis proceeds based heavily on likelihood and not on consequence, and relying even more heavily on the idea of minimizing costs. Cost minimization and evaluation of safety measured in costs is at the core of this approach. Often when it incorporates consequence, it does so by assessing the financial costs. Any consequence that is not easily calculated as a financial cost is effectively discarded. This approach routinely evaluates the frequency and severity of risks as being far less likely and far less impactful than later real conditions show them to be.

The “As Low As Reasonably Achievable” ALARA approach begins with an assessment of the potential harm to worker health. This is then assessed using an estimate of the ‘value’ measured in dollars of a human life, and then compared to the estimated financial cost of the proposed work to be done. When the cost to life is greater than the financial cost (often only when) the proposed project may proceed.

As a result of applying these principles, the hazards remain in the systems design with higher likelihood of occurring with extremely severe resulting consequences. When the flaw in the design eventually leads to an accident, the consequences are often terrible. By assigning overly low risk values, planning for such failures and generally omitting all of the equipment, training and preparation required – meaningful response to the disaster is all but impossible. And that very often leads to an even greater disaster as happened at Fukushima.

Also, the current system is often strongly incentivized through costs, awards, and management direction to remove hazards from mitigation or consideration by ‘doing a more refined analysis’ of the risk with the intent of eliminating or reducing the costs associated with mitigating or removing the hazard from the design.

This need not be the philosophical approach. An alternate approach might be to revise this to require that any evaluated design that results in a potential consequence greater than some set level must be eliminated by revising the design. Paradoxically, by focusing on costs in the early stages the end result is often the most costly resulting design, as at later stages unplanned mitigations have to be applied at many levels.

Waste Encapsulation Storage Facility (WESF)

The WESF exemplifies such a problem. As part of the original design, a Safety Basis analysis was performed to identify risks and consequences. In that analysis, DOE identified that should any single pool containing capsules lose its water for any reason, that the resulting radiation dose rates would result in a permanent inability to re-enter the facility and the slow loss of control of all of the radioactive materials in the structure. Over a fairly short period of time all of the capsules would fail and release their contents to the environment.

This does not mean that following such a drain down that some plan would have to be developed to recover. It means that no such plan is possible, that there is no possible means to avoid a major catastrophe. The plans then did not go on to assess what that means to the rest of the site or to site

**Hanford Advisory Board – Tank Waste Committee – February 4, 2016 draft Rev 5
Safety Culture – Discussion framing – Dirk Dunning, Lead Issue Manager**

cleanup work. As radioactive cesium spreads from the facility contaminating the central plateau, a substantial area quickly becomes a no-man’s land – an exclusion zone. Quickly, operations to maintain and retrieve the tank wastes are put into jeopardy.

This analysis doesn’t consider the age related failure of the facility, or irradiation of the concrete and its consequent failure potentially causing this series of events. The analysis included the consequences over the first month, but not after that.

WESF is now beyond its design life. The ventilation systems and hot cells are being grouted to avoid another severe accident scenario. Accumulated radiation exposure has severely degraded the high efficiency filters in the system. The concrete in the basins under the best case analysis is extremely degraded. A water pipe connected to the basins under the facility has no secondary containment and should it fail could lead directly to a drain down accident.

WESF is a good case example of why it is essential at all stages in the life of a facility to constantly challenge and reassess what we think we know, and when we learn that conditions, risks or consequences are different from what we thought, to then address those as directly and early as possible.

Task at hand

Our task is to try to find a better way to highlight the core issues to DOE to help them change their programs to prevent or avoid future disasters here. Our discussion is intended to come to a common understanding of the issue, and to examine possible approaches that may help to achieve this goal. A major part of this will be making the result extremely clear and unambiguous, and – simple. This may well mean recommending changing the name used to describe this, and possibly recommending that it be separated into several major components.

Some of these may possibly include:

- 1) Focusing on the definitions (see presentation by DOE’s Safety Culture head Julie Goeckner), and a one page draft of questions to focus thought and consideration of safety.
- 2) Other definitions or areas by others to address this:
 - a. “Just Culture”
 - b. “Safety by design”
 - c. “Safety Ethics”
 - d. “Science of Safety”
 - e. Others
- 3) This may also involve consideration of major themes
 - a. “Early Integration of Safety in Design” – DNFSB
 - b. Values, integrity
 - c. Simplicity, Elegance, Robustness in design (engineering philosophy)
 - d. “Fail Safe” design, “Intrinsic Safety”
 - e. Vulnerability assessment
 - f. Elimination of ‘catastrophe potential’
 - g. Graceful failure
 - h. –not– ‘cost/benefit’

Hanford Advisory Board – Tank Waste Committee – February 4, 2016 draft Rev 5
Safety Culture – Discussion framing – Dirk Dunning, Lead Issue Manager

- i. –not– ‘risk calculation/threshold’ approaches
- j. –not– ‘bolt on or strap on safety’
- k. –not– ‘add on safety’
- l. –not– ‘safety after the fact
- m. Or as Mike Rowe suggests “Safety Third”.