

Hanford Advisory Board – Tank Waste Committee – September 23, 2015
Safety Culture – Discussion framing – Dirk Dunning, 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 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.

The phrase “Safety Culture” has its origins in the Chernobyl Reactor Disaster. At its heart that disaster was made possible by horrible 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...’!

And so here is a very brief review of why and how that accident happened, leading to the development of “Safety Culture” as a phrase, as a one paragraph statement, and as a field of practice.

Chernobyl

The potential for the disaster was principally created by the addition of graphite to the tips of control rods used to shut down the reactor. Doing this increased the reactors efficiencies and made the reactor slightly more powerful and the power produced slightly less costly. This also meant that when the rods were inserted to shut down the reactor, that as they were first inserted, they made the reactor more powerful before they poisoned the nuclear chain reaction shutting down the reactor.

To overcome this, the designers limited how many control rods could be inserted at one time. They imposed an interlock that only allowed “scramming” of the reactor by inserting control rods in groups called “banks”, so called bank-scrams.

With this design choice, the stage was set and the actors (the managers and operators) entered. Chernobyl was a well-run reactor. The staff had won many safety awards and was well regarded. They felt they were knowledgeable and safe, and they were. But that also made them somewhat complacent and led to a general feeling that they knew what they were doing.

On the day of the disaster, they embarked on a safety test designed to study an unrelated major safety issue involved in the design of the reactor, one which seriously impacted the safety of the reactor during accidents and conditions requiring the reactor to be shut-down – to be scrammed. The test intentionally put the reactor into an unstable low power mode of operation, which the scientists, engineers, managers, and operators thought they understood. Delays led to the necessity of passing the test from one operating crew to the next late in the evening before it began.

As the test progressed, the reactor became more and more unstable. The engineers and operators determined that it was unsafe and required immediate shutdown, so urgent that they over-rode the bank-scam interlock to force the immediate shutdown of the reactor – never remembering the design tradeoff made for efficiency.

Hanford Advisory Board – Tank Waste Committee – September 23, 2015
Safety Culture – Discussion framing – Dirk Dunning, Issue Manager

As the graphite on the ends of the control rods entered the reactor the power level in the reactor rose at a tremendous rate – faster than any human could see or act to stop. Before the operators could even know the error they had made, the power level in the reactor exceeded the combined power output of all nuclear reactors on earth. The water in the core vaporized instantly, the control rods overheated and melted, chemical reactions occurred creating vast amounts of hydrogen and the pressure rose to the point that it blew the 2,000 ton lid off the reactor into the ceiling and the base of the reactor downward four feet. Several explosions happened in series for different reasons that ultimately blew the reactor apart.

Lessons un-learned

Following the disaster, 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 it is true fails to be useful or helpful. People both do not generally understand it, and fail to successfully apply it to prevent problems. It is unclear. Instead, it is all too common for people to hear "Safety Culture" and hear 'safety' (well, I know what that is, and I'm safe), and 'culture' (I'm a good person and I'm cultured), and to short cut to thinking something like – 'ok, I've got this'. All of those involved at Chernobyl thought the same, from the designers to the operators, engineers and support staff.

Following a series of other accidents, incidents and disasters, other teams at other sites 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 tends to be abstract and general. Safety is after-all involved in everything.

And still – since Chernobyl, we have had many disasters like those at: Bhopal, Seveso, Challenger, Columbia, Henderson Nevada, Fukushima, Deep Horizons, and an uncounted many more.

At their heart, these disasters like Chernobyl started by designs that traded safety for cost reductions and efficiency. 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 disaster.

Hanford Advisory Board – Tank Waste Committee – September 23, 2015
Safety Culture – Discussion framing – Dirk Dunning, Issue Manager

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.

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’
 - 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”.