Thoughts on Design

. . . and assumptions

M.G.(Ron) Britton, P.Eng.

Almost every design project has, at its base, one or more assumptions. They are the foundation upon which you can begin to move from problem to solution. Life would be simpler, and more boring, if problems always came with a full list of "facts" and "constraints" so the analysis could be precise and complete. But that only happens in fundamental engineering science courses in the early years of undergrad education. Out there in the real world, things are a bit more complicated.

Back in those undergraduate days we all learned (well we were all told) that strength of materials theory is founded on the assumptions that the materials are isotropic, linearly elastic and homogeneous. The problem with these assumptions is that they are an idealization that cannot be realized. Once we have accepted this reality, the theories can be utilized, and modified, to fit real situations. In other words, the base assumptions may be wrong, but used with discretion, they are still a useful tool.

To a certain extent, an assumption is little more than a belief. Its strength is that it provides you with a place to start without the necessity of actually being true. Its weakness is that repeated use or excessive rationalization can make it seem to be true. In the cases of religion or politics, belief can lead to debate. At times design assumptions can also cause disagreement.

Most assumptions provide boundaries within which we can operate. They provide a way to simplify a complex situation or create boundaries within which we can work. They are a familiar tool that we use in design every day. However, that familiarity can lead to problems.

Subsequent analysis of the March 11, 2011 earthquake and tsunami in Japan has brought a series of assumptions to light. We all saw videos of the actual events and their physical consequences. We all saw pictures of the nuclear power station with the ominous "clouds" emerging from the containment buildings. Miraculous rescues, grief stricken and/or resilient survivors, apologetic authorities and international "experts" became regular newscast features. But only in the "engineering" press did people start pondering the assumptions, both good and bad, that provided the foundation for design and construction many years ago.

The first of the "what were they thinking" question was "why would they put a nuclear power plant in that location?" Obviously the answer to that is the Japanese design engineers assumed they could design and build a system that would survive a major earthquake. In retrospect, and considering only the structural performance, this was a good assumption. Until the seawalls were overtopped and the impacts of the tsunami were experienced, the reactor building/system survived.

However, the seawalls were overtopped. Clearly the engineers responsible for that system based

their design on some assumed maximum tsunami magnitude. But assumptions respecting natural occurrences are based on best available historical data and statistical probabilities. They are a "best guess" as to what we might experience. So maybe it is unfair to call the design assumption "wrong" and simply accept the risk inherent in attempting to predict nature.

The initial tsunami effect was to destroy the electrical distribution system. Clearly the engineers had assumed the seawall would provide the necessary protection for the area, including the electrical distribution system. Someone did, however, assume that some sort of electrical outage could occur and they installed backup systems to deal with such an occurrence. Unfortunately the backup systems were installed at ground level. This placement was a good assumption with respect to earthquake resistance, but a bad assumption with respect to the potential impact of an unanticipated tsunami. If the tsunami had not occurred, or if the seawall system had been adequate, the reactor structure would not have been compromised.

From the perspective of the general public, the problem was that the atomic reactors began to over heat because there was no electricity to operate the pumps that were needed to provide adequate cooling water replacement. Without adequate cooling water the reactor began to overheat and a partial melt down began. Steam build up led to explosions causing structural damage to both the reactors and the containment buildings and ultimately allowing release of radio active materials.

Actually the assumptions that led to the melt down were made many years earlier at GE when the original reactor designs were carried out. The reactors were assumed to be "safe" as long as the "rods" were covered with cooling water. It was assumed that cooling water could always be supplied. That being the case, there was no need for the complexity or cost of an automatic shut down system. Apparently this later assumption was hotly debated at that time and a number of senior engineers resigned in protest. Now almost a half century later, their concerns were justified. And "Houston, we have a problem".

Clearly I was not a part of the design process and I have been a distant, if interested, observer of the disaster. The assumptions I have identified are my assumptions based on information that I have been able to find. But they do illustrate the potential, and in this case realized, domino effect of assumptions and the design decisions that are based on those assumptions.

At its base, design requires that we make assumptions in order to proceed. Safe design requires that we minimize the probability of wrong/bad assumptions. System design requires that we understand potential component interactions when placed into the system, and remember that the designs of the components were all based on assumptions.

Because assumptions are so fundamental to the design process, we need to treat them with great care. Be certain that, in as much as possible, assumptions are based on knowledge rather than belief. Belief, by its nature, does not require proof.

And Chicken Little was wrong, the sky is not falling, unless the assumptions are wrong.