Thoughts on Design

. . . and learning from failure

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

The January 2010 recall of Toyota vehicles became headline news. Given that automotive recalls happen almost weekly, one has to wonder why this particular recall got so much attention.

Toyota became the largest automotive manufacturing company in the world by stressing the quality and reliability of their products. From the start their company image has been based on quality engineering, from design through manufacturing to performance. Within our profession, it has been suggested that Toyota is an illustration of what engineers can accomplish if engineering is the corporate priority.

Given the comparative awkwardness of the Toyota recall, one cannot help but suspect that the company had no plans in place to deal with a major component failure. Their competitors can, and do, deal with recalls very effectively. In fact, while Toyota was apologizing, both Ford and Honda quietly announced recalls that were literally lost in the footnotes of the “bigger” story.

Without the benefit of being part of the inner workings of a corporation, it is difficult to know what their real problems and priorities are. But regardless of the corporate priorities, all engineers know that all systems, human or mechanical, will eventually fail. In the Iron Ring ceremony we are reminded of “the perversity of inanimate objects”. Toyota engineers have just been reminded of this fact.

Engineering is founded on, and Toyota has prospered on, the concept of innovation through quality design. Henry Petroski observed that "Engineering is the rearrangement of what is", and that, to me sounds a lot like innovation. The problem is that most people, including many engineers, think that innovation is based on scientific discovery and design is simply the “sizing” of parts based on established scientific “facts”. Nothing could be further from the truth.

Scientific discovery has always followed design. The Wright brothers designed and built an airplane. That led to the study of aerodynamics. James Watt developed a steam engine. That led to serious investigation into thermodynamics. Until space travel became a reality, there was no need for studies into the effects of weightlessness on the human body. Undoubtedly scientific discovery has led to more sophisticated design, but the studies themselves are to better understand how and why some innovation works, not to create innovation.

As systems become more complex, scientific inquiry provides clues that allow the complexities to be analyzed more completely. But the system is still just a collection of “parts”.

An automobile “system” is composed of countless “parts”. Each of these “parts” is supposed to do something and then “communicate” that something to other “parts”. Each “part” is individually designed to satisfy assumptions that are based on what we know from past

experience and from recent scientific confirmation. It is analyzed and tested to determine how it, on its own, will perform. As the "system" develops interactions between and among "parts" are assessed, again based on the assumption that we fully understand what each "part" must do and how it must interact with other "parts."

Basically what happened to Toyota was that one of the "parts" failed when subjected to what was probably a unique set of circumstances. In this case failure means that it did something they didn't expect. For some heretofore unknown reason the communication from one "part" to another was faulty. And to add to the situation, only some of the hundreds of thousands of "parts" failed. Clearly the circumstances that caused that failure were not anticipated and not a part of the quality control testing program. Somewhere in the design performance specifications something was not anticipated.

Over the years, Toyota seems to have based its design specifications on past success. Design based on success will, eventually, lead to failure because refinements and "improvements" tend to move closer to the limit. Failure defines a design limit very clearly. Failure, again quoting Petroski, is an "unintended experiment".

As an academic involved in delivering a graduate class that relates to the design process, I must admit to finding a positive side in the Toyota "troubles". It has provided a valuable, current "case study" relating to failure. We were wrapping up discussions on design failures and how they affect both our understanding of system performance and the design process when the recall made headlines. The flood of informed, and other, opinion on cause and effect along with the billion-dollar cost estimates took discussions away from history and textbooks and made an engineering failure very real.

As engineers we tend to become comfortable behind the security of safety factors, standards and specifications. Fortunately major failures are not daily occurrences. But failures, major and minor, do occur on a regular basis. Failure is a part of innovation, which in turn is driven by design. And design is what engineers do. Design of parts, concepts, processes and systems, both physical and operational, is the reason our profession exists. From time to time a "Toyota recall" will occur to shake our confidence. We all need to strive to make certain the next "recall" isn't based on something we have done.