



The Product/System Failed

What did we do wrong?

Dependability and safe operation are two main requirements for any product/system. However, product/system failures have always been a problem. The complexity of modern technical and business systems adds to the number and severity of product/system failures. The question then is, "Why have traditional failure prediction methods failed at preventing product/system failures?" The sad reality is that the conventional tools themselves are not "foolproof." Moreover, the failure prediction methods are cumbersome and difficult to use.

The traditional process of failure prediction originates with a verbalization of the product or system functions and flows sequentially to what may occur if there is a breakdown in performance of these functions. As such, the line of process logic follows design intent. Once a potential failure is defined, the effect of the failure, probability of its occurrence, and the ability to detect the failure is determined. Once these parameters are quantified a calculation of risk is made. If the risk is determined to be unacceptably high, changes in product/system design are contemplated.

At first sight, the process sounds logical. However, careful consideration reveals serious logical flaws with these traditional approaches. The first weakness is a result of the very process used to define failures. The process of failure definition is a brainstorming exercise driven by probing potential failures. In other words, the process of failure determination is akin to a scientific research process. This process is limited by lack of available information and depends heavily on the knowledge and experience of the people involved in the process. In addition, the analysis of potential failures is accomplished within the same mental context that created the design in the first place. Thus, there is a question of objectivity to be raised with this approach. No one likes to admit that his or her designs are prone to fail.

A second shortcoming of traditional approaches is that analysis of failures concentrates on the absence of an intended or designed function. The issue of "unintended" functions is not considered. For example, the function of a butcher knife is to cut meat. Therefore, the failure analysis concentrates on performance according to the original design intent. The original designers of the butcher knife did not design it to be used as a weapon in a domestic dispute. This "unintended" function is not a part of conventional failure prevention process. Also, for the process to be more complete, insufficient and/or excessive, delivery must be considered.

Concept Catalysts, Inc.

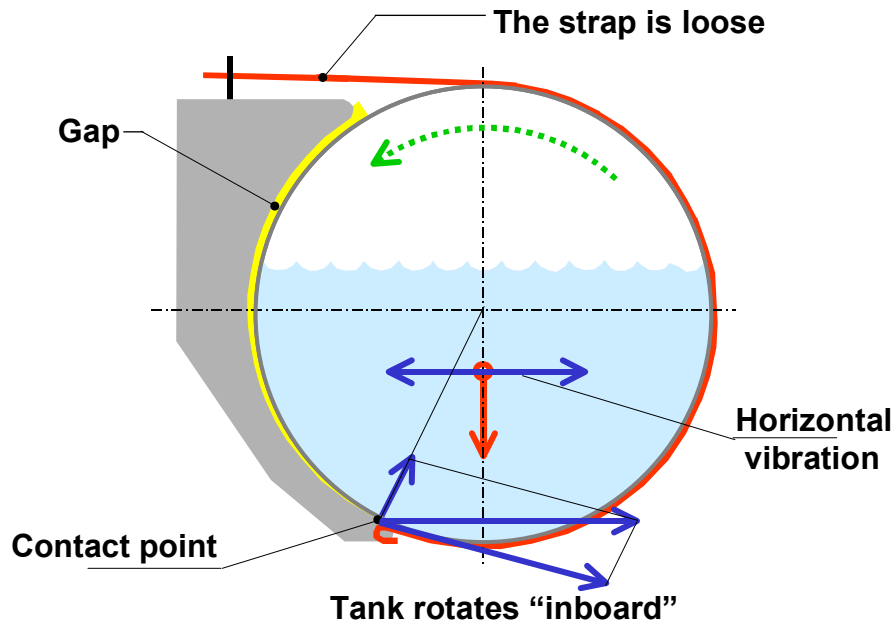
Predicting the failure rate for a business system is an even more daunting task. Here we deal with unpredictable human behavior and uncertainty associated with volatile world around the system at hand.

Also, when we fix one defect that may cause a failure, the data for that defect does not help us to predict other kinds of defects or failures. Therefore, the causes of different kinds of failures are often independent. Thus, the time spent on one failure is of no use at all when we estimate another failure.

At this point it is important to distinguish between two types of failure – safety- and performance-related. A performance failure affects the business and its financial well being, whereas a safety-related failure may lead to personal injuries and loss of life in addition to loss of facilities and equipment. Most traditional failure analysis tools are geared towards recognition and prediction of the latter. Prediction of performance-related failures is not a part of the traditional design process. In short, generally accepted failure prediction techniques are defensive in nature and not very effective.

The question, then, is what can be done differently. First, we recall that conventional failure prediction methods, just like most scientific techniques, force us to ask a research type of question: “What could happen or how did it happen?” There is very little information available to answer this question. A different type of question to ask is, “How can we make something happen?” In other words, we *invent* the problem. Thus, we move from a research type of process towards an inventive type of process.

For example, a round fuel tank on a truck inexplicably rotates inboard. For many years the question, “How did it happen?” was not answered. A different type of question, of course, is “How to make it happen?” As soon as this question is asked, one may recall that when something moves in general, a force of some kind has been exerted on it. Now there is clear direction: the system must be analyzed for a source of such force. Therefore, the process concentrates on something tangible; general knowledge of mechanical engineering enables analysis of the system. Once the source of the force was detected, the team was able to develop several readily implementable concepts to eliminate the problem.



What is different about this approach? First, the perspective from which potential failures are determined is very different. It is a vast departure from the conventional prediction process, which is similar to walking in the dark. Second, rather than taking a defensive stance, the process becomes proactive; the system resources are utilized to characterize failures and eliminate them.

For failure prediction, the process starts with definition of the main system's function, with subsequent characterization of various ways to sabotage delivery of this function. The same approach may be used for safety-related failure prediction. In fact, this process is so effective that users will often become dissatisfied with their system, be it technical or "soft", as having so many drawbacks that it is a wonder it could work at all. This is normal, since these are hypothetical failures. However, once they are perceived they can be eliminated or their impact can be greatly reduced.