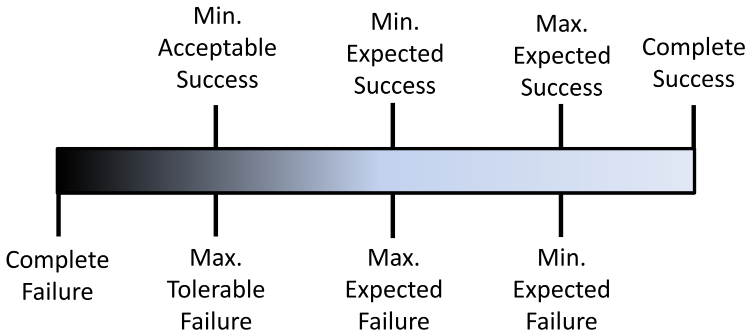
CE-395 Reliability of Engineering Systems

Instructor: Eric M. Hernandez, PhD

ENGINEERS AS PRACTICAL PESSIMISTS

Engineers are by nature pessimists, in the sense that they are always obsessed with considering all the possible different ways in which a system can fail. Engineers work (very hard) to prevent those failures in the systems they design. Although this is of paramount importance to engineering design, a non-engineer might ask, "*why so much pessimism?... why don't you look at success? If you guarantee system complete success, you don't even have to think about failure*". In the following paragraphs I will show that when dealing with reliability problems, pessimism pays off.

The typical definition is that a system has failed when it loses the capability to fulfill at least one of its intended purposes. On the other hand a system has succeeded whenever it has fulfilled its mission. By these definitions, success and failure are mutually exclusive events, however in reality this is seldom the case and significant overlap exists. Failure and success are not Boolean events, i.e. there is a spectrum of possibilities between total success and total failure which are illustrated in the figure below



- **Complete Failure**: The system did not achieve any of its intended goals
- **Max. Tolerable Failure/Min. Acceptable Success**: The system did not fulfill all the performance goals, however total failure was prevented.
- **Max. Expected Failure/Min. Expected Success**: The system fulfilled all the performance goals, however at a barely minimal survival level.
- **Min. Expected Failure/Max. Expected Success**: The system fulfilled all the performance goals with a minimal level of anticipated failure.

- **Complete Success**: The system fulfilled all the performance goals beyond the anticipated level.

From the above definitions one can clearly see that complete failure is bounded from below and this bound can be readily quantified. However, complete success is unbounded and not easily quantified. Plainly speaking, *things can always get better, but there is a point at which things can not get worse.* In addition, from a computational point of view, there is usually countable ways in which a system can reach complete failure, but there are infinite ways to achieve complete success. Thus from a practical point of view it is more efficient to compute the elements of the failure space than the success space.

Finally, avoiding complete failure is more important than achieving complete success, and moreover it is a more agreeable definition. It is always clear among different experts when complete failure has occurred, however they may differ drastically on what constitutes complete success.

To conclude, some examples are illustrated below (you may not agree with my categorization, which proves my point):

- The Space Shuttle Challenger launch in 1986: This is an example of complete failure.
- The London Millennium Footbridge: This is an example of max. tolerable failure/min acceptable success.
- The Apollo 13 Space Mission : This is an example of max. expected failure/min. expected success.
- The Ford T-Model: This is an example of max. expected success success/min. expected failure.
- The Personal Computer: This is an example of complete success.

To illustrate how these different levels can be reached in a given system/project consider the following project: “Attend a university and obtain a 4-year degree”. In this case the following levels can be defined (which some of you may not agree):

- *Complete Failure*: You are dismissed from the university due to low grades.
- *Max. Tolerable Failure/Min. Acceptable Success*: You graduate after 6 years with a GPA of 2.50
- *Max. Expected Failure/Min. Expected Success*: You graduate in 4 years with a GPA of 3.00.
- *Min. Expected Failure/ Max. Expected Success*: You graduate in 4 years with a GPA of 3.50. You are elected member of an honor society.
- *Complete Success*: You graduate in 4 years with a GPA of 4.00. You become a member of various honor societies. Your honor thesis is published in a journal and your findings result in important contributions to your field.

In this example it is clear that avoiding complete failure is significantly more important than achieving complete success. In every project it is essential to identify all the outcomes that define the various degree of failure and success.