You Can’t Paint On Reliability

Understanding the Physics of Failure and a Systems Approach are Essential

“A man’s got to know his limitations.” This is one of the more memorable lines from the movies of Clint Eastwood and it possesses great wisdom. Of course, we all are at our finest when we test our limitations. How does this relate to engineering system reliability? Well, what do we mean when we say that a person is reliable? Is it possible to say that a person is reliable in all matters or in just some matters, all the time or just sometimes, in all circumstances or in just some circumstances? The same questions need to be applied to an engineering system design, because reliability cannot be an after-thought and you can’t just paint it on!

As we become more dependent on complex mechatronic systems, it is not sufficient to understand just how they work; we must also understand how they fail. Fault-tolerant system design, not just fault-tolerant component or subsystem design, has become paramount. Reliability is the probability that an item performs a required function under stated conditions for a stated period of time. So an engineer needs to define the functions a system must perform, the boundary conditions under which the system will operate, and the time duration during which reliability is required.

To better understand reliability, I spoke with Tim Kerrigan, Fluid Power Consulting Engineer at Milwaukee School of Engineering’s Fluid Power Institute (FPI), where he and his colleagues work to ensure industrial and government systems are designed for reliability.

A physics-of-failure approach to reliability is consistent with the model-based approach of modern mechatronic system design. It uses modeling and analysis to design reliability into a system, perform reliability assessments, and focus reliability tests where they will be most effective. The approach involves understanding and modeling the potential failure mechanisms (e.g., fatigue, wear, temperature), the failure sites, and the failure modes (the activation of the failure mechanisms). The failure modes of a mechatronic system include those of mechanical, electrical, computer, and control subsystems, i.e., hardware and software failures. A physics-of-failure approach can substantially improve reliability, reduce the time to field systems, reduce testing, reduce costs, and significantly increase customer satisfaction.

As mechatronic systems become more complex, the interactions among the subsystems – mechanical, electrical, computer, and control – become more difficult to manage and the overall system reliability goes down due to this integration. Therefore an assessment of overall system reliability must have an adequate margin for safety. An analogy here is the feedback control system. It provides great benefits, e.g., command following and disturbance rejection, but feedback control systems can go unstable if there is an imbalance between strength of corrective action (gain) and system dynamic lags (phase lags). Model uncertainty is quantified by assuming that either gain changes or phase changes occur and the tolerances of gain or phase uncertainty are the stability margins, gain margin and phase margin. Real systems must have adequate stability margins! Real systems must also have adequate reliability margins!

Mechatronics can enhance the reliability and fault-tolerance of a system with prognostics, diagnostics, and built-in test capabilities. The additional sensors and control elements must be very reliable and do add additional cost. But the long-term cost of unreliability is huge compared to the initial design cost of reliability. In addition, designing for reliability enhances energy efficiency and sustainability. Reliability and fault-tolerance is a competitive advantage in the commercial market and an absolute requirement in the healthcare, military, and transportation sectors.

Kevin Craig
December 2010