Applying Human Space Flight Experience to Identify and Reduce Risk in Dynamic Environments

Phil Lewis
Chief Engineer – J&P Technologies

It is said that we are doomed to repeat the failures of the past unless we learn from them. Well that is not the whole truth, the past will still repeat, it's just that now we have the opportunity to effectively plan for and control the effects of such occurrences, i.e. "Learning from the Past". One more small, but interesting fact, those repeated failures would have the most detrimental effects in a completely different industry, in a seemingly new application. Therefore we must not just learn from our own failures, but look outside our technical comfort zones and investigate significant events in what may seem like totally unrelated, or near impossible failures in other applications and industries.

While on the surface space flight and petrochemical industries appear technically unrelated, the ascent phase of space flight is a very high-energy endeavor, much like deep-water oil exploration. In both cases the environment changes rapidly and the effects of failures catastrophic, which is why we not only minimize our risk by utilizing design solutions, we must also plan our responses to rapidly changing environmental and system vulnerabilities. Another example of similarity is a refinery and long-duration space flight, such as that experienced aboard the International Space Station. Just like with a space station, a refinery relies on a "Control Center" and "System Operators" to maintain an efficient production environment by responding to "Off-Nominal" situations. Additionally both systems, while dynamic in nature, were designed with significant automation in place to assure a level of sustained safe operation with minimal human interaction. In many cases, the time-to-effect for "Off-Nominal" situations may be such that automated responses are the only effective means to maintain a safe system.

J&P's system and software safety engineers are very familiar with minimizing risks to an acceptable level, and fully understand what it takes to design, deliver, and operate complex engineering solutions in dynamic environments. Our experience with the complex dynamics of space flight is directly applicable to the offshore and refining industries. The increasing use of computer control systems offers significant productivity gains while at the same time minimizing human exposure to hazardous operations. With this benefit comes the paradox that a single software module of the control system can be more complex than the entire mechanical system. In addition, these advanced computer controls contain safety-critical fault handling functions that can be dangerous and cost prohibitive to fully test, resulting in systems the true performance of which is only known during an emergency situation. This scenario is common in space flight also and J&P's System and Software Safety Engineers are ready to apply our space flight proven methodologies as an important contribution to improving safety in dynamic environments such as offshore and refining operations.