NASA Flight Safety Experience
Translates Directly to Process Safety

Phil Lewis
Chief Engineer – J&P Technologies

One of J&P's more challenging tasks is providing assurance that our Nation's Astronauts and Critical Space Assets (i.e. the International Space Station, Space Shuttle, etc.) are not exposed to an unacceptable level of Risk. To achieve this we use tools such as Hazard Analysis (HR), Failure Modes and Effects Analysis (FMEA) / Failure Modes, Effects, and Criticality Analysis (FMECA), Reliability Block Diagram Analysis (RBDA), Criticality Assessments (CA), Fault Tree Analysis (FTA), and even Probabilistic Risk Analysis (PRA) to name just a few. There have always been two key aspects to Human Spaceflight; the first is assuring the safety of the crew, the public and the environment, the second is providing a level of assurance that the mission will be a success. If you substitute "Human Spaceflight" with "Process Industries" the rest of the statement still rings true. Process Safety Engineers are responsible for assuring the safety of their "crew", the "public", and the "environment", while at the same time assuring that the "plant" will operate in such a manner as to maximize productivity and profitability, essentially what we call "Mission Success". The only real difference between these "missions" is the nomenclature / language used in each industry, the tools and techniques are very similar, and even the basic methodologies for achieving their desired goals are essentially the same.

When developing a "new system for spaceflight" we would normally perform a Preliminary Hazard Analysis (PHA), with the objective to identify potential hazards in both the design and operation of the system. When developing a "new processing system" the entire process team commonly undertakes a brainstorming session called the HAZID (Hazard Identification) to identifying high level potential threats along with causes & consequences in a system that could lead to major accident hazards. Hazard and Operability Analysis (HAZOP) is the hazard identification technique that is done when the plant is in operation and involves hazardous operations that could affect day-to-day operations. In many cases feedback from the PHA/HAZID/HAZOP results in refinement to the system requirements and specifications documents.

Depending upon the complexity and criticality of the flight system being developed we may perform an initial Probabilistic Risk Assessment (PRA) or develop a functional Reliability Block Diagram Analysis (RBDA) to determine the level of risk inherent in the proposed system. Taking a cue from the Nuclear Power Industry, the use of PRA's for spaceflight is becoming much more common place. As the design matures, so do the products. At J&P we constantly update our PRA's, RBDA's, FMEA's, and Hazard Analyses so that informed risk-based design occurs.

A key safety process exercised during the design phase for spaceflight is the identification of hazards and proposed controls. This is very similar to what happens during the design of a Process Control System. Both Spaceflight and Process Systems utilize similar strategies to minimize risk. In spaceflight we follow a safety order of precedence, 1st we try to eliminate the hazard by design, 2nd we try to minimize the effect of the hazard through a series of controls, alarms, automated and human responses, and finally we design escape and safe-haven systems should a really "bad day" occur. In Process Engineering you 1st try to minimize the risk using safe process design (elimination of the hazard via design), 2nd is a perfect corollary to spaceflight in that the Basic Process Control System / Safety Instrumented Systems (SIS) is designed such that responses, both automated and human, are used to control the hazardous effects and bring the system back to nominal operation [Note: The SIS is nominally designed for plant shutdown safely. It usually takes manual intervention to bring the plant back to full operation]. Finally, the process designers include plant (including shutdown) and community responses (evacuations and shelter in place) for those "bad days" when the hazard cannot be controlled. The process industry commonly uses Layers of Protection Analysis (LOPA) to assure that the Independent Protection Layers (IPL's) are effective and independent. LOPA based design also identifies an order of precedence from safe process design to emergency response, essentially identical to that used for Space Flight. The space flight engineer utilizes PRA's, RBDA's, risk appropriate fault tolerance allocations (i.e. similar to allocating Safety Integrity Levels), verification that hazard controls are truly independent, and emergency response plans to achieve a similar objective; part of what we call Flight Certification. Both industries strive to maintain an optimal balance between Risk and Mission Success. NASA Space Flight Safety Experience is a great addition to Assuring Process Safety.