MODELS AND SIMULATIONS: RISKS AND LESSONS LEARNED

Terry L. Hardy

Great Circle Analytics, LLC, 899 Pearl Street #21, Denver, Colorado, 80203 USA, thardy@gcirc.com

ABSTRACT

Organizations throughout the world are developing and operating space launch vehicles and systems for the purposes of furthering exploration, delivering services, and facilitating commercial human spaceflight. The operation of the launch vehicles and space systems creates the potential for harm to the crew, to flight participants, and to the uninvolved public. Therefore, it is imperative that comprehensive risk assessments be performed to characterize, evaluate, and reduce the risks of these endeavors. Analytical models and simulations are used in complex space systems to support decision making during development and operations. However, the risks associated with the use of models and simulations are often underestimated, and the hazards are often misunderstood. The failure to understand and address model and simulation risks can lead to poor decisions that may result in mishaps. This paper provides real-world examples and lessons learned to illustrate common concerns with the use of models and simulations.

1. INTRODUCTION

Analyses, models, and simulations play important roles in identifying and controlling space system hazards and reducing space system risk. Analysis is typically defined as technical or mathematical evaluation using mathematical models, simulations, and algorithms. A model is a physical, mathematical or otherwise logical representation of a system, entity, phenomenon, or process. Data that goes into a model is considered part of the model. A simulation is a method for implementing that model, and is typically considered to be an imitation of the characteristics of a system, entity, phenomena, or process using a computational model.

Critical risk decisions are often made on the basis of the results from models and simulations. Analyses and models may be used in the design of space systems, for example, to determine propellant requirements or to calculate launch vehicle trajectories. Models and simulations may be used to verify that safety requirements have been met, for example, to determine structural design margins or to calculate expected thermal loads. Simulations can be used to identify whether systems meet requirements and to allow operators to interact with the system prior to operation. Examples include the use of simulation tools to imitate cockpit conditions prior to flight or to analyze guidance, navigation and control system performance during reentry of a crew capsule. Models may be qualitative, such as system safety risk assessments, or quantitative, such as expected casualty analyses.

All analyses, models, and simulations contain assumptions and uncertainties which impact their usefulness. However, the analysis assumptions are not always understood, and the models and simulations may not be applied appropriately. While the use of any model or simulation requires judgment, safety assessments often do not consider the impact these analyses can have on the risk. Using accident reports from various industries, this paper describes safety risks applicable to analyses that support space system decision making, and provides lessons learned from those incidents.

2. LESSONS LEARNED

This section discusses a number of lessons learned related to analyses, models, and simulations, with corresponding accident examples to show where a flaw in the analysis process led to an undesirable outcome. These accidents are described in reports and investigative summaries from multiple industries and organizations, including those outside of the aerospace industry. This is done to broadly illustrate hazards and risks in models and simulations and to stress the importance of learning from other industries. Note that in discussing these accidents, this paper does not intend to oversimplify the events and conditions that led to the accidents or blame any individuals or organizations. There is rarely a single identifiable cause leading to an accident. Accidents are usually the result of complex factors that include hardware, software, human interactions, and procedures. Readers are encouraged to review the full accident and mishap investigation reports to understand the often complex conditions and chain of events that led to each accident discussed here.

2.1. Failure to incorporate the appropriate models in hazard identification and risk decision making

On January 31, 2006, an explosion occurred at a chemical manufacturing facility located in Morganton, North Carolina, in the United States. This company manufactured paint additives and polymer coatings, and conducted its operations in a large 1,500 gallon reactor. One worker was killed by the explosion, and 14 others were injured in the aftermath. The U.S. Chemical Safety and Hazard Investigation Board (CSB) determined that the cause of the accident was a runaway reaction. To meet a sudden increase in demand, plant managers had scaled up the normal process by adding more constituents. Unfortunately, the managers failed to understand that scaling up the process resulted in an increase in energy release, leading to tank heating above what the cooling system could handle. The pressure inside the reactor increased due to the increased heating, leading to the venting of solvents inside the building. The vented solvents ignited, leading to the explosion. The CSB faulted the company for its lack of recognition of the hazards from scaling the process and its lack of safeguards to protect against a runaway reaction. The CSB stated that the company had not identified hazards in its operations and had not conducted formal hazard analyses. The CSB noted that safeguards were primarily procedural, but the company could have used high pressure alarms, automatic shut offs, and venting to mitigate the risk. CSB also stated that the company “had minimal safety information on its polymerization process, even though this was the core of its manufacturing business.” Although analytical techniques were available, the company did not use analytical models to characterize the reaction process and the thermal aspects of that process, and the plant manager had relied on past experience to estimate batch sizes. This accident shows that, while past experience is important, that experience should be supplemented with data and analysis, especially when making changes to a system [1].

2.2. Failure to provide adequate training in the limitations of models

On August 6, 2007, the Crandall Canyon Mine in Emery County, Utah collapsed, trapping six workers. On August 16, 2007, the mine collapsed again when one of the walls of a tunnel exploded, killing three rescue workers. The original six workers trapped in the explosion were never recovered. According to U.S. Mine Safety and Health Administration (MSHA) investigators, the original collapse was caused by a flawed mine design. The investigation report stated that the stress level exceeded the strength of the pillars such that when one small failure occurred it created a ripple effect that caused widespread collapse, leading to the loss of the miners. The MSHA stated that the mine was “destined to fail” because the company failed to heed early warnings and previous failures. For example, on March 10, 2007, one of the pillars burst leading to a partial collapse of the mine. According to the MSHA the mine’s design was based on improper analysis and models. The report stated that the operator’s mine design incorporated flawed design recommendations from its contractor. The investigation team discovered that managers and mine safety personnel did not review input and output files for accuracy and completeness and were not appropriately trained in the details and limitations of the models. Therefore, evaluators could not provide adequate assessments of the risk. This accident illustrates that even valid models and simulations can be misused if those using or reviewing the models are not trained to understand the model’s limitations [2].

2.3. Failure to document model assumptions and limitations

The Space Shuttle Endeavor was launched on September 7, 1995, on mission STS-69. One goal of the mission was to deploy and then retrieve the Shuttle Pointed Autonomous Tool for Astronomy 201 (SPARTAN-201). SPARTAN-201 was a spacecraft designed to provide short-term scientific observations related to solar winds and the solar atmosphere. During one of the first on-board targeted burns in the rendezvous sequence, ground crews noted that the Shuttle had used 4.3 times as much propellant as predicted. This propellant usage may have threatened the ability to retrieve the spacecraft. However, all burns after this maneuver were ultimately completed successfully and the spacecraft was successfully retrieved. Analyses after the mission found a performance limitation in a rendezvous software algorithm that led to the excess propellant usage. Apparently, this algorithm had been used on Apollo missions in the 1960s and adopted for use on the Space Shuttle. However, the limitations in the algorithm were not passed down to personnel on the Space Shuttle program, and had not been encountered on any previous missions. After the mission, the algorithm functionality and performance were documented and incorporated into flight rules, training, and procedures. This incident stresses the importance of documenting all model assumptions and limitations [3].

2.4. Analysis substituted for testing to reduce costs

The Mars Polar Lander (MPL) spacecraft was launched on a mission to the planet Mars on January 3, 1999. Upon arrival at Mars, communications ended according to plan as the vehicle prepared to enter the Martian atmosphere. Communications were scheduled to resume after the Lander and the probes were on the surface. However, repeated efforts to contact the vehicle failed, and eventually the program managers declared that the spacecraft was lost. The cause of the MPL loss was never fully identified, but the most likely scenario was that a failure occurred upon deployment of the three landing legs during the landing sequence. Each leg was fitted with a Hall Effect magnetic sensor that was designed to generate a voltage when the leg contacted the surface of Mars. The flight software issued a command to shut down the descent engines when touchdown was detected by this sensor. The MPL