Gains from Losses

John Livingston

The Importance of an Active and Robust Working Relationship Between System Safety and Engineering

The next few columns will address the importance of an active and robust working relationship between system safety and engineering. While the importance of this relationship is an often-stated axiom, post-accident assessments continue to cite causes reflecting shortcomings in system safety and engineering efforts that are rooted in either a lack of the basic exchange of knowledge or in the mutual utilization of that knowledge for the identification and control of project hazards and safety risk assessments.

These columns will take an ephemeral look at the key relationships between engineering and system safety efforts during a project's lifecycle. The references cited provide more detailed insight into each discipline, and I welcome the contribution of additional sources. Because of the nature of my personal experience and the references that will be used for examples and source information, these columns will have a strong aerospace flavor. In general, it is not the nature of the enterprise, but the complexity of the individual projects that fuels the challenges to the system safety/engineering relationship.

Highly complex systems are becoming more common, which only increases the need for a truly integrated effort. Areas of specialized knowledge and discipline expertise must be molded into one joint effort that addresses all aspects of the project, its hardware and its operation.

These columns will be divided into three general project phases: concept development, design definition and program operations. This column on concept development will offer an overview of the respective roles of each discipline and suggest areas of mutual interest, as well as the advantages of coordinated efforts.

Concept Definition Goals and Objectives

There are many important goals and objectives for engineering and system safety during the concept definition phase. Engineering plays a key role in the development of the system architecture, defining technical requirements, leading the evaluation of design trade-offs, including associated technical risk of the different options, and the establishment of the roles and tasks that engineering will perform for the balance of the project lifecycle [Ref. 1]. Major tasks for system safety include the development of initial safety requirements and risk management criteria, the performance of trade studies that evaluate hazardous conditions or concept options with high risk sensitivities (with recommended alternatives) and the identification of safety tasks that will become the core of the system safety and risk management efforts during system definition, design, manufacture, test and operations [Ref. 2].

While each discipline's approach and specific objectives may vary, the commonality of the major tasks allows us to structure our discussion into three general topics: development of discipline requirements, discipline trade studies, and planning for the next stage of the project development.

Requirements Development

System Engineering — The initial engineering requirements based on the assigned project objectives should be part of the project lifecycle kick-off. These top-level engineering requirements lead to a set of baseline requirements, which include supporting derived requirements. For most efforts, the derived requirements will make up the great majority of the engineering requirements on the project. Project engineering requirements should address the total lifecycle and cover all design aspects. The details of the derived requirements closely interact with the development of the concept details. The "established" concept should be based on a "converged" set of engineering requirements that are both understandable and verifiable. It is also important that they are placed under program control and that traceability of their origin is maintained. It is not usual for conflicting project engineering requirements to occur, necessitating project -level trade studies to assure that resolutions provide the best possible balance between project goals and sound engineering principles [Ref. 3].

System Safety — The first step in developing project safety requirements is the definition of what

is an acceptable safety risk, along with the factors and conditions that present unacceptable accident/mishap risks. These definitions provide a program baseline for forming design criteria and assessing the suitability of proposed candidate solutions. Requirement sources include (but should not be bounded by) historical experience with similar systems, associated trade studies and related hazard analyses. Requirements may be inherited (or imposed) from outside sources, but all should be carefully evaluated for applicability to the concept under development.

The basic safety philosophy and associated design requirements should be established prior to initiation of any hazard analysis tasks. A lack of standard or benchmark safety requirements can lead to reactive (operational) controls, rather than design "corrections." Opportunities to develop solutions that offer the most productive reduction in potential risks are generally the greatest at the concept development stage with minimum impacts [Ref. 4]. As the project progresses, design options decline and costs increase.

It should be remembered that safety requirements include both deterministic and risk-informed requirements: "A deterministic safety requirement is the qualitative or quantitative definition of a threshold of action or performance that must be met by a mission-related design item, system, or activity in order for that item, system, or activity to be acceptably safe. A risk-informed requirement is a safety requirement that has been established, at least in part, on the basis of the consideration of a safety-related risk metric and its associated uncertainty" [Ref. 2].

Trade Studies

In this series of discussions, we will use the general definition that "a trade study is an objective comparison with respect to performance, cost, schedule, risk, and all other reasonable criteria of all realistic alternative requirements; architectures; baselines; or design, verification, manufacturing, deployment, training, operations, support, or disposal approaches" [Ref. 5] with the important caveat that "risk" evaluations include system safety trade assessments. The trade study effort is an important part of any project and evolves as the project moves through its lifecycle. As the details of the system emerge, the resolution of the trades becomes more specific and the linkage to the project more complex. At any stage of development, the quality of the trade studies is directly dependent on the knowledge, skill and range of expertise of the participants. Also important is the leadership of the trade study efforts and their role in the progress of the project toward an optimum system design.

Engineering — Design concept trade studies are an important part of the engineering process used to support the development of a concept that provides the best combination of effectiveness and cost.

In this discussion, we will use the following NASA definitions [Ref. 1]:

- **Effectiveness:** The effectiveness of a system is a quantitative measure of the degree to which the system's purpose is achieved. Effectiveness measures are usually dependent on system performance.
- **Cost:** The cost of a system is the value of the resources needed to design, build, operate and dispose of it.
- **Cost-effectiveness:** The cost-effectiveness of a system combines both the cost and the effectiveness of the system in the context of its objectives:
  - While it may be necessary to measure either or both of those in terms of several numbers, it is sometimes possible to combine the components into a meaningful, single-valued objective function for use in design optimization
  - Even without knowing how to trade effectiveness for cost, designs that have lower cost and higher effectiveness are always preferred

In the most favorable situation, the design trade studies will start within the project-acceptable cost/effectiveness envelope. There are design options that either reduce cost while still maintaining the project effectiveness requirements or improve the project effectiveness while staying within the cost boundaries. In the best of both worlds, there are design solutions that improve project effectiveness and reduce costs at the same time. Much more likely are project design alternatives that trade cost for effectiveness or effectiveness for cost. The most challenging outcomes are presented by trades that have only alternatives that fall outside the cost or effectiveness boundaries.

Additional factors that must be considered include the fact that for most complex systems, the total design effectiveness is composed of system, sub-system and component factors that may have conflicting attributes. With any option, the quality of the supporting knowledge must be considered. These potential uncertainties add another dimension to the trade studies. It should be no surprise that numerous trade studies are required for major projects.

System Safety — System safety trade studies should be a part of the process of concept development and a factor in concept selection. The objective of the safety concept trade studies is the evaluation of potential hazards associated with concept candidates both in terms of the hardware and the operational characteristics. This

evaluation should include associated risk sensitivities for the different options and the safety recommended alternatives. The evaluation also provides support for any formal concept hazard analyses and risk assessments that assess potentially hazardous systems. The trade studies provide insights that aid in the development of the initial safety requirements and risk management criteria. The effort should also identify any follow-on special safety studies and risk assessments that may be required during system definition or design.

Project Development Planning

Engineering — Engineering has a major role in planning the technical effort for the balance of the project, based on the results of the project concept definition phase and traditional engineering roles. Project activities that should be addressed in the planning for the continuing engineering support include [Ref. 1]:

- The identification and definition of the technical effort required to satisfy the project objectives and lifecycle-phase success criteria
- The engineering roles in the project technical reviews and technical issue assessments
- The validation of the project technical requirements
- Support for the development of any enabling new technology associated with the concept selected
- The engineering role in the project technical risk management activity, including risk tracking and control functions (risk mitigation actions)

While some of the activities are extensions of the concept definition phase engineering efforts, it is important that all engineering support efforts are addressed in terms of the project lifecycle effort. For example, the verification and validation (V&V) of project technical requirements is a fundamental part of the project technical integration that has roots in the concept development. The details of the process (test, analysis, demonstration, inspection or similarity engineering) will emerge as the project design matures. Proper planning is important because of the relationship with the selection of specific technical requirements and its role in other project aspects, including cost and schedule. Because V&V will be required at the component, sub-system and system levels, it is important that the systems engineering team develop a top-level verification plan early in the project development cycle [Ref. 3].

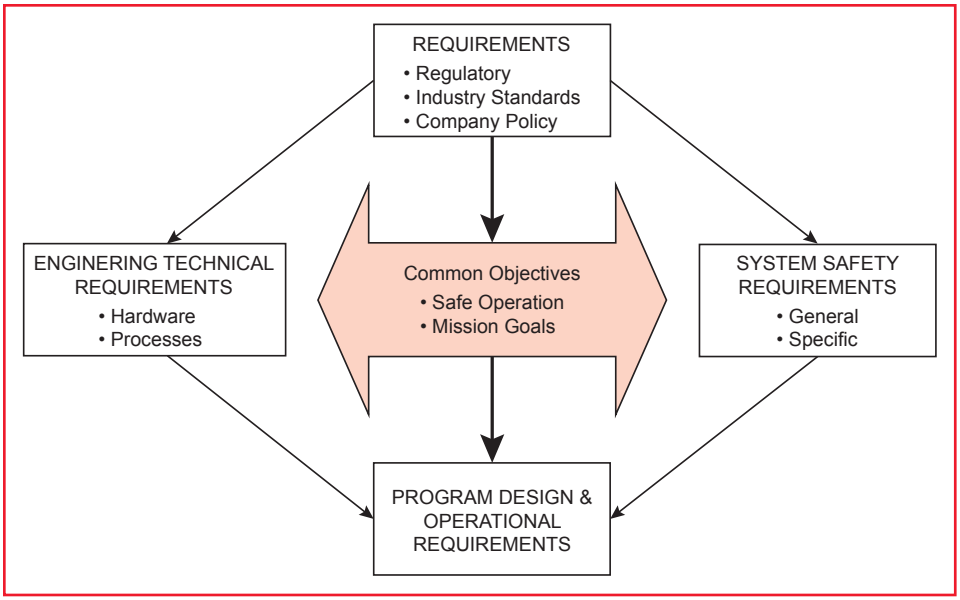

Figure 1 - Concept Requirements Development.

System Safety — System safety planning for the next stage is an important part of the concept development activity. Planning for the project development stage should reflect the project system safety program requirements that originate from many different sources. Government regulations, company policies and customer requirements all play a role. The knowledge gained from the concept definition activity should also be factored into the planning. Part of the planning activity should be the establishment of safety and risk goals and objectives that will be used to determine the safety and risk inputs for the overall program. The goals should be measurable, and the related safety tasks and risk management tasks should be clearly identified. Each task should be constructed in a manner that will demonstrate that its respective goals have been met. The development of the planned safety activities should also include estimates of the personnel requirements for the safety program for the balance of the project lifecycle [Ref. 2].

Common Interests

Early and direct involvement in any project or program is critical to the success of project support for the engineering and system safety disciplines. The three major concept development efforts discussed have activities that have strong parallels (and interfaces) between the two discipline efforts. These common interests offer the opportunity to improve each effort and the overall welfare of the client project.

Figure 1 illustrates the general flow of concept requirements development. While each discipline provides unique contributions to the requirements development, they share the common objectives of assuring

safe operation and the achievement of the project's mission goals.

Many of the project technical requirements are drivers for system safety requirements. It is important that system safety practitioners have knowledge and understanding of project technical requirements. This knowledge can be enhanced by direct contact with the engineering discipline experts and the project system engineering staff. It is also important that the project engineering side of the project has the appropriate understanding of the design requirements driven by system safety discipline sources.

Less obvious is the interrelationship of the respective quality for both efforts. For example, both disciplines face the challenge of providing the best products with the resources provided by the project. The general lack of communication about program design requirements (and implementation) between program engineering and system safety was one of the findings of the Space Shuttle Challenger accident investigation [Ref. 6]. One could argue that system engineering shortcomings in the establishment of technical requirements and their validation cited in the Mars Climate Orbiter Mishap Report [Ref. 7] and the Genesis Mishap Report [Ref. 8] might have been diminished by a strong interface with system safety (and quality assurance) requirements efforts.

Figure 2 illustrates some of the major objectives of the trade studies that support concept definition. Again, both disciplines have different focuses based on their assigned responsibilities; they share the common objective of assuring that the "best" concept is developed in terms of the candidate hardware and the associated operational characteristics.

For major projects, a number of technical trade studies will be conducted in parallel. While system safety should have insight into all of the trade studies, it is a must that system safety engineering personnel participate in all trade studies that have been identified as being safety related. This direct involvement ensures that safety impacts are addressed and technical risk assessments have system safety factors as part of the trade study decision drivers. From a system safety perspective, it is important that the trade study results show that the safety risks for the recommended solution are equal to or less than the other alternative being traded, or provide sufficient justification (safety margin) for the recommended option [Ref. 4].

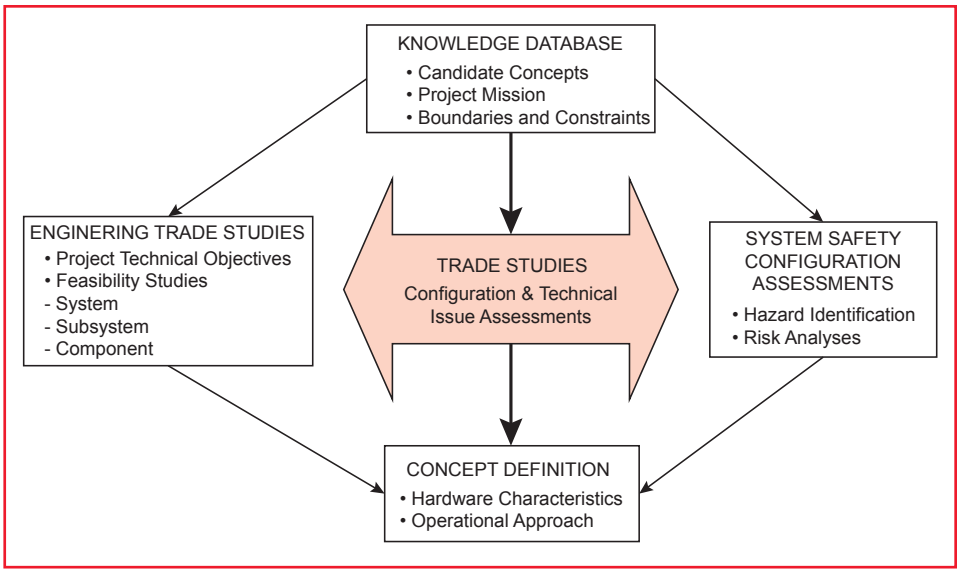

Figure 2 — Concept Trade Studies.

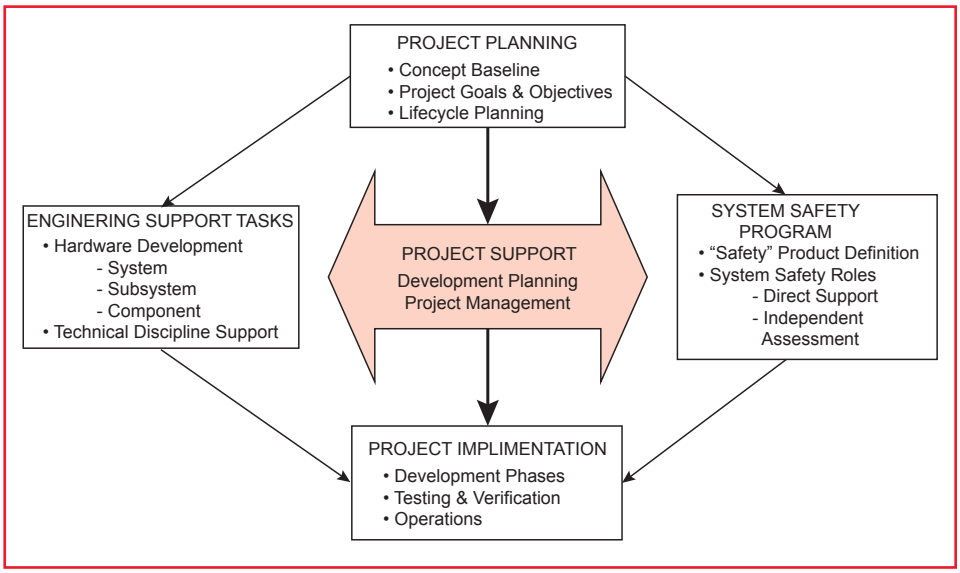

Figure 3 — Project Planning Tasks.

There should be linkage between the technical trade support activity and any related system safety trade analyses. This linkage provides support to the system safety team member's efforts to assure that there are optimum safety provisions developed for each option and inputs to the establishment of the system safety position on trade study recommendations. The effectiveness of this imbedded approach is driven by three factors: the ability to identify safety-related trade studies, the resources necessary to support trade studies, and the necessary system safety role in the project concept selection process.

Figure 3 illustrates the planning for the movement of the project from the concept definition stage into the project development stage. Each discipline has an important role in the planning of project implementation and management activities.

It is important to both disciplines that the proper "go forward" planning is done. Planning is based on the expected roles of each discipline in the project development stage and should utilize the experience gained during the concept definition stage. Each discipline should acknowledge the role of the other discipline in the development of project support activity plans. Acknowledgements that are not mutual or are not consistent should be subject to question and inquiry.

"It is important to both disciplines that the proper 'go forward' planning is done. Planning is based on the expected roles of each discipline in the project development stage and should utilize the experience gained during the concept definition stage. Each discipline should acknowledge the role of the other discipline in the development of project support activity plans. Acknowledgements that are not mutual or are not consistent should be subject to question and inquiry."

The benefit of mutual planning is illustrated by the following example. For any crewed launch vehicle, the provision of a launch pad escape system is of primary importance. Planning for the development of such systems requires the consideration of many factors (hardware and system characteristics procedures) and inputs from many contributors (vehicle designers, pad system developers, human factors experts, system safety engineering and system engineering). Even specialized analyses like the development of the minimum timeline for the flight crew to escape to a place of safety requires input from many sources to provide a complete assessment. Engineering studies that address only the quickest path in terms of the functions of the different subsystems (stairs, pathways, chutes, transporters, etc.) still need input from the human factors evaluations and system safety analyses to determine if the optimum technical system will meet the crew egress survival requirements. Conversely, the system risk analysis needs the inputs of the system engineering analyses and system safety assessments to determine the risks associated with the baseline system and potential alternative solutions. True mutual efforts are based on plans that address all information sources and their application to the system definition development. Such plans should describe an iterative approach that encourages interactions among the contributors to the different aspects of the system during its development.

In the next column, we will address engineering and system safety relationships during the project development phase. Attributes introduced in this article will be expanded and a few new "wrinkles" will be added.

References

1. "Systems Engineering Handbook," National Aeronautics and Space Administration, NASA Headquarters, Washington DC, December, 2007, http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20080008301_2008008500.pdf, accessed on July 31, 2013.
2. NPR 8715.3C, NASA Safety Manual, January 24, 2000. Change 6 as of February 3, 2011 Source: NASA Online Directives Information System (NODIS) Library, http://nodis3.gsfc.nasa.gov/, accessed on July 31, 2013.
3. Blair, J.C., R.S. Ryan and L.A. Schutzenhofer. "Engineering the System and Technical Integration," NASA/CR—2011–216472, NASA Scientific and Technical Information (STI) Program Office, http://www.sti.nasa.gov, accessed on July 14, 2013.
4. "Air Force System Safety Handbook," Air Force Safety Agency, Kirtland AFB NM, http://www.system-safety.org/Documents/AF_System-Safety-HNDBK.pdf, accessed on July 31, 2013.
5. "Space Systems Engineering Course: Chapter 12, Trade Studies," http://spacese.spacegrant.org/index.php?page=trade-studies, accessed on August 6, 2013.
6. Report of the Presidential Commission on the Space Shuttle Challenger Accident, National Aeronautics and Space Administration, Washington, DC, 1987, http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/table-of-contents.html, accessed on August 9, 2013.
7. Mars Climate Orbiter Mishap Investigation Board Phase I Report, National Aeronautics and Space Administration, Washington, DC, 1999, ftp://ftp.hq.nasa.gov/pub/pao/reports/1999/MCO_report.pdf, accessed on August 9, 2013.
8. GENESIS Mishap Report, Volume I, National Aeronautics and Space Administration, Washington, DC, 2005, http://www.nasa.gov/pdf/149414main_Genesis_MIB.pdf, accessed on August 9, 2013.