N72-25977

SYSTEM SAFETY IN THE OPERATIONAL PHASE

By

Mr. John Gera, Jr.
Manager, Division Safety
North American Rockwell

PRECEDING PAGE BLANK NOT FILMED

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

SYSTEM SAFETY APPLICATION IN THE OPERATIONAL PHASE

The operational phase of a program assures completion of flight test programs and demonstration of operational capability. It is mission performance. Support of this activity from a System Safety standpoint is failure analyses, hardware changes, procedural changes, accident/incident analyses, and a great amount of involvement in ground operations. However, the operational phase really starts further back than at mission performance. I say this because one never finishes designing and manufacturing the system since requirements seem to change calling for improvements in the system. In this respect I consider the manufacturing, testing and material handling an important element of the operational phase and should be treated as such.

No one disagrees with the concept that a good, safe product starts with the designer. System Safety effectiveness also starts there. During its short life, the major emphasis of System Safety has been in engineering and we can find voluminous material on System Safety engineering management, System Safety engineering, System Safety analysis, and so forth. With the emphasis on engineering, we sometimes forget that System Safety is a totally encompassing task, as the word system implies. As a result, important processes in the total system go unattended. What good does it do to engineer a functional, safe product; build it on time within budgeted cost; then have it damaged by inattentive handling or worse yet by not having handling equipment because the interface was not there. Someone forgot -- someone overlooked. We need to stop and evaluate the total System Safety process to assure we really are talking about a "system" oriented program.

I'll cover System Safety concern in manufacturing, test operations, material handling, and flight test and flight operational phases. The reason for including manufacturing, test operations, and material handling is that is an area that has lacked proper System Safety concern.

Most manufacturing people do not have the luxury of knowing why certain hardware is designed a certain way. The engineer can only reflect the design in drawings and specifications after the thinking process had culminated in an end concept. The manufacturer could easily envision the end product differently from a process standpoint and, gentlemen, this process analysis from a System Safety standpoint desperately needs to be accomplished early in the program.

We need to:

1. Look at facilities for emergency backup power, electrical protection against main power fluctuations, work platform locations, deluge systems, lighting, noise, accessability. The relationship of this equipment on the end product.
2. Develop requirements for support items such as work stands, hoisting, confined entry, emergency procedures, safety critical operations such as welding and pressure tests.
3. Conduct hazard analyses o. the manufacturing flow and develop disciplines to eliminate or reduce these hazards prior to the start of manufacturing operations.

We have learned the hard way tnat playing "catch up" is expensive and very hard on the nerves, I might add. Lack of analysis has been the culprit in many instances, leading toward destruction of space boosters, test articles and components. Lack of process control has led to untold embarrassing situations. The accidents are often times shrugged off under the umbrellas of statements that "to err is human," "Murphy's law," and the like. It is often said, "We have time to do the job over, but never enough time to do the job right the first time." All of these so-called explanations are, in my opinion, unacceptable crutches and ways to avoid the basic problem. Many times we design traps for the men in manufacturing, test, and material handling. They need a good process analysis that can identify for them situations that are hazardous to the product as well as ways to protect them from personal injury. They need to be reminded about safety features required to assist them in doing the job right the first time.

Let's back up a little and ask ourselves why not let the builders and users work closely with the designer in the early stages of design. Not just involvement in the design review but during the criteria development phase and the

actual design. The outcome will be a safer and more efficient process along with being cost effective; the ground support equipment and handling equipment can be brought into the picture much earlier; and the transportation or movement of subassemblies and delicate parts can have parts protection considered during the design phase. You can already see that part of what we consider System Safety is getting everyone into the act not merely the system safety engineer but the people that are building, handling, and testing the product. System Safety, then, is part of the labor that goes into the product -- a direct labor function that is looked at very carefully as to its contribution. The payoff is accident prevention as opposed to cure.

(Refer to Chart)

Early analysis in the manufacturing process identifies not only what is required to build the product but also the required skills. Training and certification of personnel helps assure that the job starts correctly. The next step is to match the process against System Safety standards. Those of us who are fortunate in having active standards know many of the pitfalls in process delays are avoided by assuring standards are satisfied. If some standards cannot be satisfied, our job in System Safety is to work with respective departments and keep the process moving in a safe manner. This is our contribution that is looked at very carefully. Don't misunderstand me here -- I am not advocating disregard for standards by merely signing a waiver. What I am saying is that we in System Safety should not use the standard as a shield and say, "You can't do that!" The approach is -- "we have a problem!" and our job is to help get the program out of that problem.

Review of documentation comes next. These reviews require approval of safety critical systems. That is of systems that need tighter monitoring because of damage potential. Certain installations, pressure tests, major hardware moves at times require that extra pair of trained eyes from System Safety. So in these reviews we assure ourselves that planning documentation and process documentation have proper back-out procedures in case of problems; safety cautions and warnings are identified. Here again, we shouldn't only act as a filter -- we should be helpful in making constructive comments to make the process better and safer. Another word of caution -- the responsibility for safety must remain in each department with each supervisor and with each employee.

Testing operations provides a unique situation for System Safety. Testers must understand manufacturing since there always seems to be some finishing up to do after the hardware is manufactured. This discipline must understand handling techniques and adapt them to the hardware being handled while undergoing checkout. They must also understand launch checkout and launch procedures since testing attempts in every way possible to duplicate the launch conditions. The concept that is followed is manufacturers build and testers test, resulting in a better product.

Closing the loop is an element that many people overlook.

Along with the imposition of standards and reviews, a key element is monitoring, audits and surveys. This gives Safety the opportunity to evaluate whether or not operating departments are, in fact, living up to the safety standards. Modifications can be proposed through this performance monitoring, coupled with new methods, ideas, and worker behavior. We also have other sources; an important one being customer experience. Additionally, internal and external experience can be evaluated. The final element of the action or monitoring loop is feedback from the departments themselves in the form of communication monitoring and direct communication. When we combine all these elements of experience, performance monitoring, and communication, the next big step is to see if the resources we have available support the recommended changes and if these changes support the goals. We have to be practical here. System Safety has to consider the safety aspects but also cost effectiveness. Our talents are put to the test in walking the fine line between the two. An unbending, non-innovative, to-the-book System Safety department is worthless in this situation.

Our final step is to take the results of the analysis and feed them back in the form of constraints within the operating departments which can take the form of additional checks and balances in the control and procedural

documentation; in modifications to the system safety standards. I might add that these modifications can take the form of either being more stringent or in easing of requirements. This is a constant learning process. The other constraint is a feedback into the engineering world by way of requirements, specification changes, retest requirements, hardware protection, and the like.

In a short period of time, I have attempted to show a closed loop flow which includes the impact of good System Safety involvement in the early portions of the program as well as the very important feedback loop. It is obvious, if the involvement comes at some time after start of the program, we play "catch up" for the remainder of the program. You don't have enough trained safety personnel to go back and review every drawing that was pumped out, every drawing that is being pumped out now, and attempt to monitor and take action on the feedback loop. Gentlemen, you chase your tail and never catch it.

I indicated to you earlier that I consider manufacturing, test, and material handling a part of the operational phase. There are two elements of operations that fall within my definition of operational phase. The first has to do with manufacturing operations, test operations, and material handling operations. This is the potential damage from people, processes, procedures, checkouts, and the like. The second element is the hardware operation with potential damage to mission and crew from insufficient primary or secondary systems. In the latter, the safest possible approach for overcoming hardware operational problems or emergencies would be to develop all the equipment and procedures so that the crew would have the option to select the most applicable from the protocol of emergency actions. These emergencies could be single or combinations of explosion during boost or orbit; severe instability during boost or orbit; loss of thrust during boost; fire; trajectory deviation; capsule decompression; life support system failure; power failure; subsystems failure; and loss of retro thrust. And there are many more to consider in separation, docking, maneuvering and the like. However, recognizing the limitations in time, money, and manpower, there must be a reasonable investment in study analysis and development testing to determine what is practical. This activity provides a rationale for setting design requirements.

The several occurrences of failures in flight, both major and minor, serve notice, in view of space hazards and more ambitious programs, that added attention to the potential requirements for operational safety can be justified. These operational emergencies are serious incidents which interrupt, either temporarily or permanently, the normal course of the mission plan. As indicated, such incidents may be anticipated or may occur unexpectedly. Anticipated emergencies can be countered by careful planning and implementation of action prior to the event, redundancies, and rapid and efficient action following the event. These actions all fall under the category of analysis that takes place early, prior to the design phase. The unexpected emergencies are those that were not thought to exist or were overlooked. During the hardware operational phase, these are the ones that bother us the most. What did we forget. The number of possible operational problems is virtually endless. No situation or system can be seen that is entirely immune to all such events. We must select the credible accidents or emergencies and act on them. So from my introductory definition, I find it difficult to separate the "people building" from the "people operating" phase. Considerations must be there for both, early and continually. The actions taken early, prior to and during design phases, helps us get prepared to prevent emergencies and provide recovery actions. There is ample opportunity for Safety to become involved, to be able to raise questions as to readiness. The review process has matured and includes: the preliminary design review; the critical design review; the first article configuration inspection; flight readiness review; and the design certification reviews.

In summary, a continuing emphasis placed on preventing accidents or emergencies through hardware design, manufacturing, test operations, handling, and operational mission analysis can give us the greatest return possible in the area of safety for the resource expenditure devoted to that end.

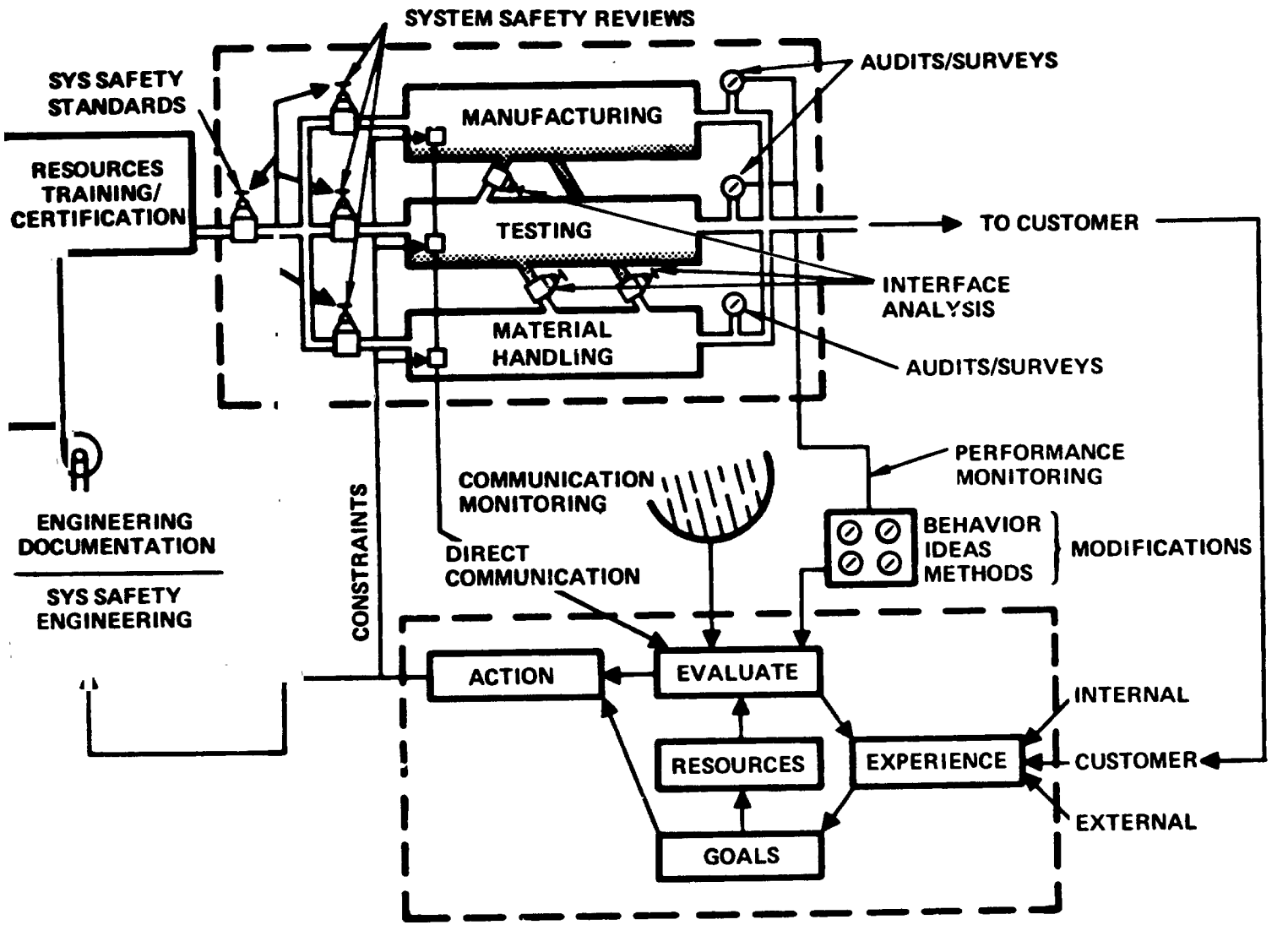
SYSTEM SAFETY REVIEWS
SYS SAFETY STANDARDS
RESOURCES TRAINING/ CERTIFICATION
MANUFACTURING
TESTING
MATERIAL HANDLING
AUDITS/SURVEYS
TO CUSTOMER
INTERFACE ANALYSIS
AUDITS/SURVEYS
PERFORMANCE MONITORING
COMMUNICATION MONITORING
BEHAVIOR IDEAS METHODS
MODIFICATIONS
ENGINEERING DOCUMENTATION
SYS SAFETY ENGINEERING
CONSTRAINTS
DIRECT COMMUNICATION
ACTION
EVALUATE
INTERNAL
RESOURCES
EXPERIENCE
CUSTOMER
EXTERNAL
GOALS

FIGURE 1