X.15

SAFETY ENGINEERING FOR THE MAN

Presented by

E. B. Gallant, Director
Administration and Engineering Operations
Rocketdyne, A Division of North American Aviation, Inc.
6633 Canoga Avenue
Canoga Park, California

at

Safety Engineering of Missile/Space Systems
53rd Air Force-Industry Conference
Hotel Miramar, Santa Monica, California

19-21 June 1963

SAFETY ENGINEERING FOR THE MAN

During the past 2 years, Rocketdyne has participated in the field evaluation of a complex operational weapon system, namely, the Atlas. Trained specialists observed every job operation from receipt of the missile until actual launch. Interviews were conducted with operating personnel to determine all potential problem areas. Each deviation from the established or standard procedures was carefully investigated. All interruptions or time delays were checked to determine cause and effect. This field evaluation was a systematic attempt to determine and isolate areas where improvement would be required to achieve the maximum possible safety, system effectiveness, and operational capability.

Our specialists were able to identify 303 problem areas involving some 1500 incidents in which human performance could adversely affect the Rocketdyne engine system with respect to safety, system effectiveness, and operational capability. To better evaluate these problem areas, we have placed them in specific categories most appropriately descriptive of their nature. A summary of these categories and the number of times each problem category occurred is shown in Table 1.

The problem category that occurred most frequently involved deficiencies relating to technical data necessary to furnish guidance or support for the required job performance. Specifically, this category includes the use of aids such as technical manuals and operation and maintenance check lists. The problems were those in which difficulty was experienced because of an omission, technical error, or lack of clarity. As a result, the specific task was improperly or incompletely performed.

The second area concerns organizational controls. Problems observed involved methods used for personnel control in the work area as influenced by regulations, job practices, and use of equipment.

The next category, safety per se, turned out to be one of the three major problem areas. Approximately one out of every five problems directly involved safety. The cause of the hazards could be traced to hardware design, system configuration, task sequence, procedures, material, operations, and common personnel practices.

A substantial number of maintainability problems occurred during the earlier maintenance demonstration exercises, but this number decreased rapidly as the operational system testing continued.

Poor job environment in the work area adversely affected personnel performance. These conditions were attributed to excessive noise, poor illumination, psychological pressure, inadequate tools, inappropriate test equipment, and crowded work space. (I might mention that this study did not involve Silo operations.)

Problems involving the prior training of individuals in the performance of various work tasks increased in relative importance during the conduct of operational system testing. These problems were related to deficiencies in skills, job knowledge, work habits, and attitudes traceable to either individual or integrated system training environments.

Operability problems were those observed which related to the activating, monitoring, regulating, or changing the performance of an item of equipment be means of control devices.

Comparatively few personnel selection and manning problems were observed or reported. These problems related to the selection or assignment of personnel to various job operations, the number of persons assigned to do a job, and the requirement for special aptitudes or talent.

In Table 2, the 60 safety problems are categorized to more clearly define the contributing or causal factors, i.e., job environment; organizational controls; equipment design; training; provisioning; technical data; personnel selection and manning, and manufacturing error. Now, using specific examples, it may be possible to more clearly indicate the type of problem with which we are confronted. For example, let us take an incident which involves both job environment and organization controls. On at least 20 different occasions, 4 to 15 people were observed in the missile thrust section where there is only room for 2 or 3 to work efficiently. This was a safety problem because the exit routes were obstructed during the installation and removal of live pyrotechnics and hypergolics. The cause of the problem was determined to be the simultaneous scheduling of three work tasks, each of which involved crews of three to eight individuals. Obviously, under such conditions, only one work task should be scheduled at a time.

Now, let us look at an incident which involved an equipment design problem. During the leak testing of a gas generator system, it is necessary to install a test plate to contain the pressurant. The test engineer ordered the leak check accomplished with the shipping cover instead of the test plate. He claimed that the test plate took too long to install. The practical solution was to redesign the shipping cover to provide the safety factor necessary for leak testing, or require adherence to the established procedure.

In an incident that involved training, the No. 1 mechanic attempted to hand the solid propellant gas generator through the turbine spinner access door to his helper outside the missile thrust section. He bumped the solid propellant gas generator against the turbopump and dropped it. The mechanic claimed that he had not been instructed in the proper routing for solid propellant gas generators, which is through the boattail.

Another incident illustrates a technical data error. A mechanic was slow in performing the steps for which he was responsible during the removal of the missile battery and explosives. He studied his check list procedures for a long time, but was not too sure that he was doing the right thing, particularly in regard to turning the power off. The check list did not indicate which power, how many places, or where. In this case, it was necessary to revise the check list to provide complete, clear, and correct information.

Manufacturing errors occur. A mechanic was observed having difficulty installing the sustainer hypergol cartridge. Before the cartridge was properly aligned with the container so that it could be inserted, the aft end struck a welded bracket used for attaching the shipping strut. The mechanic finally found a position in which he could exert sufficient pull on the container to spring it about 3/16 inch, allowing the cartridge to clear the bracket and enter the container. A slip of the hand at the wrong moment could have resulted in a ruptured cartridge and a devastating fire. A new inspection procedure was established which required utilizing a dummy cartridge to check clearance prior to shipment.

The application of safety engineering principles in system design must ensure optimum freedom from inadvertent and destructive mishaps which result from facilities, equipment, procedural, or personnel deficiencies. Important factors in ensuring the appropriate application of such system safety effort are the phasing, timing, and allocation of effort in accordance with the system development stages and technical processes.

Table 3 shows eight commonly accepted stages of system development requiring the allocation of system safety effort. The second column lists the general reliability milestones relating to these eight stages as specified in Air Force Regulations. The next column correlates system development functions to these reliability milestones. The last column indicates the type of quantitative estimate of system safety that could be made at each stage of systems development. For example, at Stage 6, the type of operational system testing which would provide the data shown in Table 1 and 2 is performed. It is at this stage that data can be accumulated which reveal the degree of system safety actually achieved relative to the operational environment. The information in Table 3 should be interpreted to mean that some of pretest analysis or systematic test activity must occur during each stage of system development. System testing must be conducted periodically on various equipment or subsystems during all phases of use, from factory to static firing for launch operations. Equally important is the necessity for system re-evaluation tests to ensure suitability of modification kits, procedural changes, material changes, or source of supply. The basic objective will be the evaluation of the operational safety and reliability of the system under field conditions.

Obviously, the extent of such effort would vary from sampling in areas of maximum likelihood to an exhaustive reliability and safety assurance effort. The extent of such effort would be affected by budgetary restrictions and the unique needs of a particular program.

How do we accomplish a sound systems safety engineering effort at the lowest possible cost? It is our belief that a major factor in the avoidance of safety problems is in the relationship between a reliability concept or practice and system safety. A review of the required, proposed, and suggested system safety engineering functions reveals a marked similarity to the activities already being conducted by many engineering reliability organizations.

Table 4 shows the reliability functions which now exist in Rocketdyne and other similar organizations. It also shows similar system safety functions now being called for in various system safety engineering documents. For example, the function entitled "Identification of Human Error" and the function entitled "Identification of Personnel Error" are basically the same. The Reliability Design Review already includes safety as well as maintainability, value, producibility, and other design criteria. A separate review for each of these criteria could be conducted, but it would only increase costs, delay schedules, and make design tradeoffs more difficult to accomplish.

In general, an organized and planned system safety engineering function serves to emphasize safety factors during the early design and development of each system. Its approach is characterized by rigorous, step-by-step methods or controls to ensure that safety criteria cannot be inadvertently overlooked. The activity should cover all stages of product design, development, fabrication, inspection, test, maintenance, and use.

The focus should be on the early identification and resolution of potential problems (i.e., on preventive action rather than corrective action following the occurrence of a mishap).

In conclusion, a system safety engineering effort which we consider to be effective is emphasised at Rocketdyne. During the past few years, we have been conducting systematic field evaluations to identify and resolve all system safety problems which could develop as a result of the operational use of our engine and ground support equipment. We believe that we have developed an effective and economical means of implementing the system safety engineering requirements by focusing the talents and energies of various technical disciplines on this highly important system development objective. Our system safety engineering effort is so integrated into the matrix of our in-plant procedures that we are assured of the full attainment of the system safety objectives that have been established.

TABLE 1

VARIABLES AFFECTING HUMAN PERFORMANCE

(303 Problems)

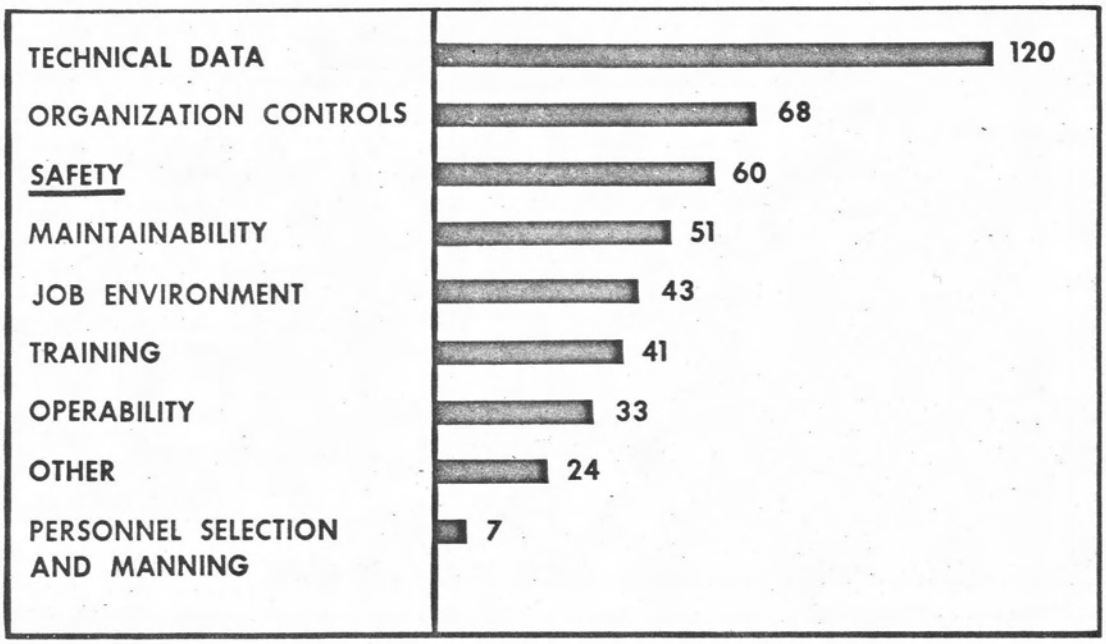

TABLE 2

SAFETY PROBLEMS

(60 Problems)

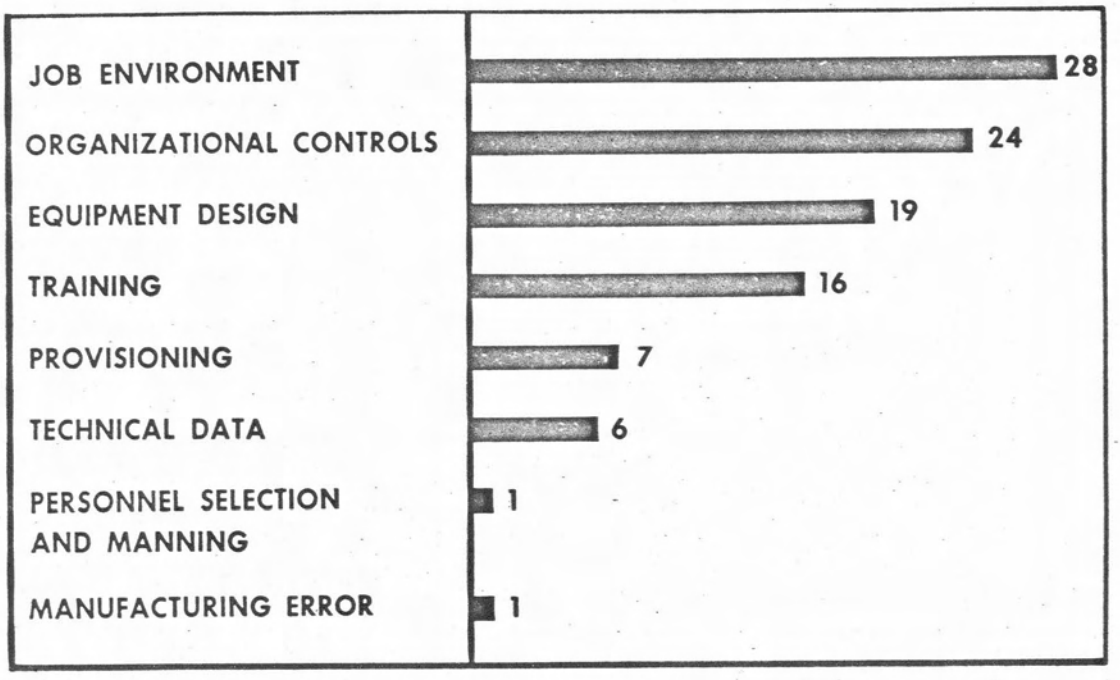

TABLE 3

ALLOCATION OF SYSTEMS SAFETY EFFORT

STAGE	RELIABILITY MILESTONE	SYSTEM DEVELOPMENT FUNCTION	SYSTEM SAFETY ESTIMATE
1	DETAILED DESIGN STUDY	SYSTEM ANALYSIS	PREDICTED
2	PREPROTOTYPE	STATIC MOCKUP, MODEL, DRAWING, AND SIMULATION STUDIES	INTERPOLATED
3	PROTOTYPE	DYNAMIC SIMULATION AND PROCEDURES DEVELOPMENT	EMPIRICALLY DERIVED
4	PRODUCTION DEMONSTRATION	VERIFICATION AND VALIDATION	REFINED
5	DEMONSTRATION OF SERVICE READINESS	CATEGORY I, PERSONNEL SUBSYSTEM TEST AND EVALUATION	DEMONSTRATED
6	SERVICE EVALUATION	CATEGORY II AND III, PERSONNEL SUBSYSTEM TEST AND EVALUATION	ACHIEVED
7	FULL-SCALE PRODUCTION	MONITOR PROCESS, PRODUCT, SYSTEM APPLICATION AND USE	SURVEILLANCE
8	DEMONSTRATION OF MAJOR PRODUCT IMPROVEMENT	MODIFICATION AND SPECIAL SYSTEM TEST AND EVALUATION	VALIDATION OR REVALIDATION

TABLE 4

INTERRELATIONSHIP BETWEEN RELIABILITY AND
SYSTEM SAFETY PROGRAM ELEMENTS

	RELIABILITY FUNCTION	SYSTEMS SAFETY FUNCTION
1	IDENTIFICATION OF HUMAN ERROR	IDENTIFICATION OF PERSONNEL ERROR
2	DESIGN REVIEW	SAFETY DESIGN REVIEW
3	HUMAN ENGINEERING HAZARDS AND SAFETY	DESIGN FOR MINIMUM HAZARD POSTANALYSIS ACTION
4	FAILURE EFFECT ANALYSIS MALFUNCTION ANALYSIS	CATASTROPHIC ANALYSIS
5	SYSTEMS ANALYSIS PERSONNEL SUBSYSTEM ANALYSIS	SAFETY ANALYSIS DEFINITION OF SAFETY CHARACTERISTICS FUNCTIONAL FLOW DIAGRAMS
6	SYSTEM TEST ACCEPTANCE TEST DEMONSTRATION EXCERCISE CATEGORY I, II, III EVALUATION	SAFETY TEST
7	RELIABILITY TEST ENVIRONMENTAL TEST OVERSTRESS TESTING SIMULATION STUDIES	SPECIAL SAFETY TESTS
8	RELIABILITY TRAINING AND MOTIVATION	SAFETY TRAINING
9	RELIABILITY DATA OPERATION AND FAILURE REPORTS	SAFETY DATA ACCIDENT/INCIDENT REPORTS
10	RELIABILITY ANALYSIS	SAFETY RESEARCH