27/1-29-79

SAND78-2176
Unlimited Release

MASTER

A Study of the Application of Quality Assurance Human Factors and Reliability Principles to the Prevention of Major Environment, Safety and Health Incidents

Charles A. Trauth, Jr., Andrew C. Ellingson, Donald E. Farr, Leo M. Jercinovic

Sandia Laboratories

SF 2900 Q(7-73)

ACKNOWLEDGMENTS

We acknowledge, with pleasure, our debt to the members of the Safety Standards and Engineering Department for their assistance in obtaining much of the information on which this study is based.

CONTENTS

ILLUSTRATIONS

TABLES

A STUDY OF THE APPLICATION OF QUALITY ASSURANCE, HUMAN FACTORS AND RELIABILITY PRINCIPLES TO THE PREVENTION OF MAJOR ENVIRONMENT, SAFETY AND HEALTH INCIDENTS

Introduction

Sandia Laboratories, under contract to the Division of Operational and Environmental Safety of the Department of Energy (DOE), is investigating how the principles and techniques of Quality Assurance (QA), Human Factors (HF) and Reliability (R) might be adapted or modified to support Environment, Safety and Health (ES&H) programs. This report describes one facet of this investigation: A study to determine whether accidents and incidents which had occurred might have been prevented, or rendered less likely, if the principles or techniques of QA, HF and/or R had been applied. Most, but not all, of the incidents studied involved Sandia Laboratories personnel and occurred at Sandia over the past ten years or so.

We would like to stress that no criticism of the ES&H program at Sandia, or elsewhere, is intended. That the ES&H record at Sandia is excellent is demonstrated in Figures 1 and 2 which compare Sandia both within a selected group of DOE contractors and within selected national industrial categories.

There is one well-known generic way in which QA, HF, and R principles and techniques might be used to support the achievement of ES&H objectives. Over about the past three decades, the field of systems safety has focused on insuring that the failure rate of hardware systems is adequately low when such failures have potentially undesirable safety consequences. Systems safety activities emphasize QA, HF and R of hardware systems (Figure 3). For a complex hardware or facility system design, the first step is to analyze the ways in which it may fail and cause death or injury. This step is typically, but not exclusively, an R study. Also, ways in which the system design may promote or encourage human error - which may lead to undesirable ES&H consequences - are determined through HF studies. Requirements to decrease the likelihood of these failure and error modes are incorporated into the system design. Quality Assurance actions are then taken to verify, independently, that, among other things

- the design is, indeed, adequate to achieve desired levels of ES&H protection,
- the design is truly implemented, as production is undertaken, and
- the final hardware or facility does truly perform as intended.

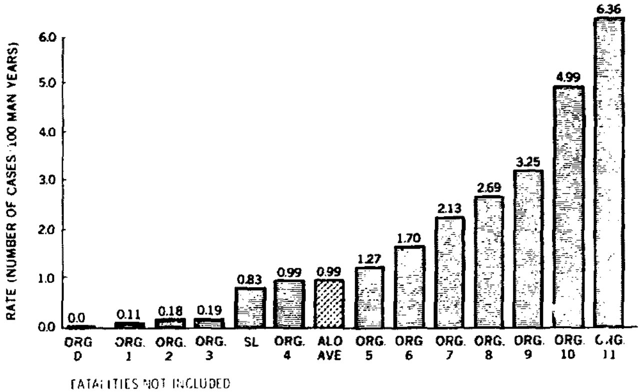


Figure 1. Lost Work Day Cases. This Compares Sandia Performance to the DOE Contractors Complex Managed by the Albuquerque Operations Office (ALO of DOE)

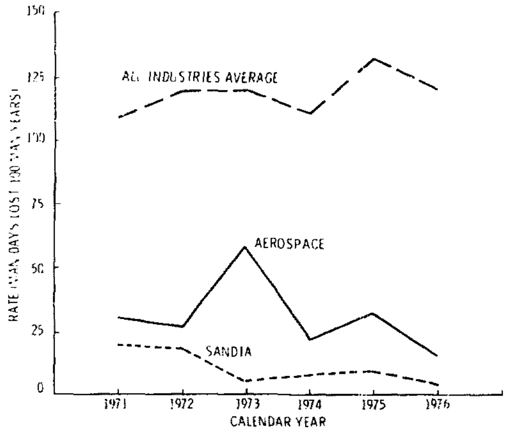


Figure 2. Disabling Injury Severity Rates

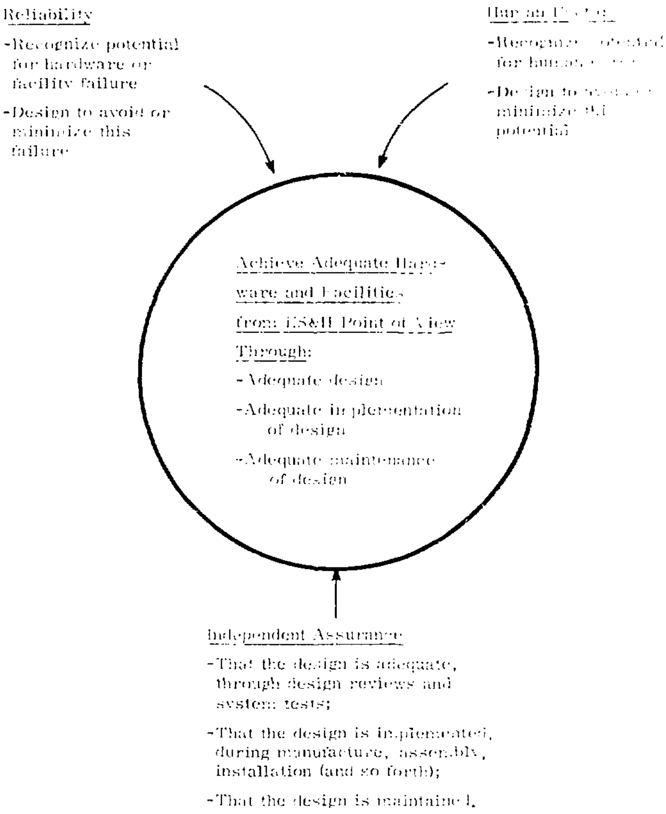


Figure 3. Simplified View of Systems Safety Functions

Thus, to achieve safety objectives, R and HF activities are used in defining both the needed design objectives and the actions needed to achieve them while QA provides independent verification that the design-related actions are "adequate" and are actually "used." Some of the traditional functions often found in systems safety activities include

- early involvement of QA, HF and R, at the design stage,
- use of modes and effects analyses, fault trees, and so forth,
- identification of failure modes that lead to unsafe conditions,
- identification of critical items on which these failure modes depend,
- implementation of appropriate actions to eliminate these failure modes or to decrease significantly the likelihood of their occurrence through the proper design or control of critical items,
- determination and documentation of the risk associated with the final design,
- review of the adequacy, manufacturability, assurability and maintainability of the design,
- assurance that the design is implemented or that the consequences of changes are understood, and acceptable,
- performance of system and subsystem tests,
- assurance that the necessary controls are exercised when the system is operational.

Hence, in the traditional setting of hardware and design, QA, HF and R can, indeed, support ES&H objectives - and do so in ways that are now well-understood. This study is not aimed at further justifying such activities, but is for determining if these disciplines have techniques or principles which may be "borrowed" or adapted to address ES& H problems in operational activities -- and to judge, with qualifications (discussed later), the worth of developing the needed techniques for such adaptation.

There are many definitions of "systems safety," but the current tendency is to regard system safety activities or practices as integral parts of any total effort to achieve "systems performance." In this context, "ES&H requirements" are an integral part of "performance requirements," and actual efforts to meet them are not visibly separated into "safety" and "other." The derivation of requirements still involves those functions from the above list that are appropriate to a particular system. Beyond the definition of requirements, emphasis is placed on total design -- which will include consideration of design allocation, evaluation, and engineering trade-offs. We have chosen to emphasize the ES&H component because of the nature of the current study.

Two In-Depth Pressure Safety Incidents Illustrating
Ineffective Application of Principles QA, HF and R

Example 1

Inadequacies of a large "gun" facility in the DOE complex, designed to investigate phenomena associated with high-velocity impact (Figure 4)

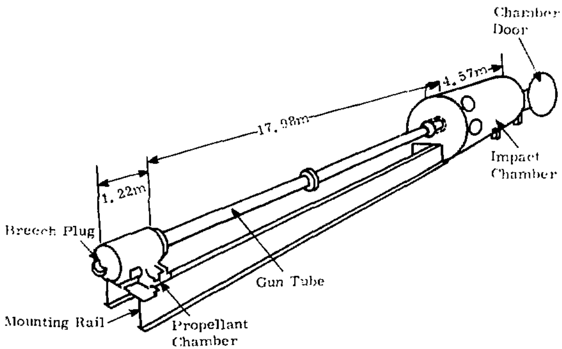


Figure 4. A High-Velocity Propellant Gun System. In the accident discussed, energetic gases escaped from the impact chamber at the right.

The impact chamber is partially evacuated during an experiment and may contain quite sensitive instrumentation to record characteristics of the impact upon a target material from a projectile fired from the gun tube. Explosive charges of up to about 9.1 kg of a mixture of naval propellents are used to accelerate the projectile into the target. When the projectile leaves the gun tube, the expansion of the products of "combustion" of the explosive (hot gases) expand into the impact chamber and cause a force to be exerted on the rear door of the chamber. New personnel probably would not adequately appreciate that the impact chamber, for a short time after firing, becomes a pressure vessel. Figure 5 illustrates this condition and also shows the force exerted by the impact of the target (fragments) on the catcher mounted on the rear door. The catcher is a shock-absorbing device composed of layers of aluminum honeycomb and steel plates. The rear door is hinged and designed to be closed against the chamber body with 48 one-inch-diameter bolts.

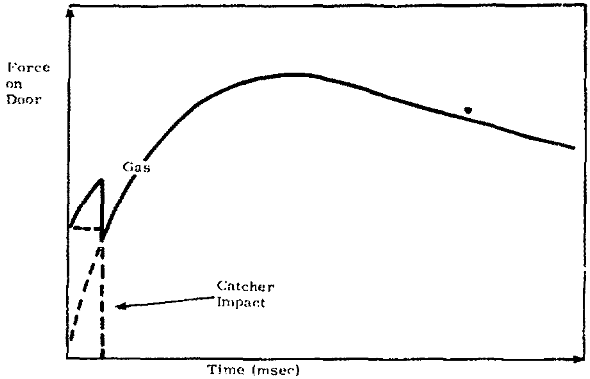


Figure 5. Force Exerted on Chamber Door After Firing When the Catcher is Mounted on the Door

The design configuration of the impact chamber is shown in simplified form in Figure 6. Over about 15 years, experimenters gradually reduced the number of bolts used from 48 to 7. During the same period, instrumentation grew more sophisticated and hand torquing rather than pneumatic torquing of the bolts was instituted to avoid disturbing the alignment of the instrumentation. Safe operating procedures made no mention of the use of fewer than the 48 bolts that the design intended, and the relationship between over-pressure and charge was never examined.

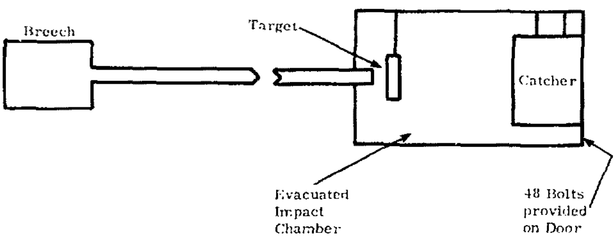


Figure 6. Schematic of Gun Assembly in Original Design Configuration

In 1977 a design change moved the catcher forward from its location against the rear door to a position just behind the target (Figure 7). This change was made to help confine the products of impact to the target area for a longer time. When the gun was fired with a nearly maximum charge, the catcher, upon impact of the target, was torn loose and impacted in the rear door. The force pulse from this impact occurred later in the time sequence than it ordinarily had done when the lighter target was propelled into the catcher fastened to the door (Figure 5). Figure 8 is a schematic of the resulting force-curve for the rear door compared to the theoretical ability of the door to withstand that force when held with 7 bolts.

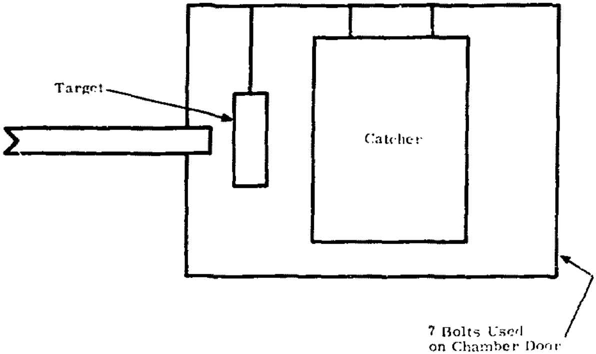


Figure 7. Impact Chamber Condition at Shot Time Shown Schematically

The result was that the nearly 2400-kg rear door of the chamber was blown open with sufficient force to rupture the approximately 15-cm-thick steel hinge brackets. The angular momentum of the door caused severe misalignment of the whole, massive system, and the overpressure released into the building housing the gun caused wall and roof sections to be blown out damaging the equipment in the area. Total damage was estimated at $133,000. No personnel were injured because, as required by safe operating procedures, they were in a blockhouse located externally to the gun facility at the time of firing.

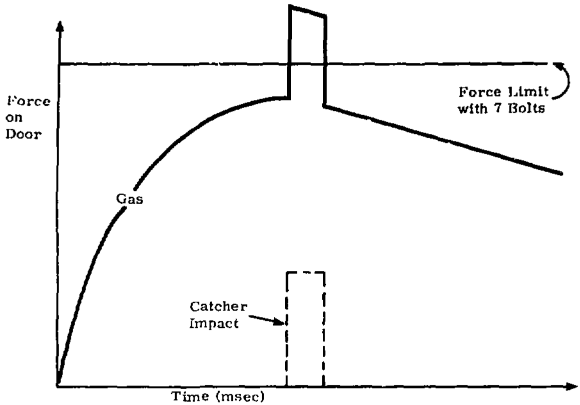


Figure 8. Force on Chamber Door in Design Change Configuration

Looking at this incident from the point of view of a systems safety analogue, which also addresses operational questions, we structured our study of it to determine whether the incident could be attributed to "inadequacies" in any of the following:

- design,
- "use" (implementation or maintenance) of design,
- safe operating procedures or practices, and/or
- the "use" of safe operating procedures or practices.

We also tried to determine whether there was sufficient assurance that no inadequacies in these areas existed. Here, "procedures and practices" were used as operational analogues of designs since they were the primary documented materials relating to how operations were to be conducted to promote safety. "Practices" is used to denote institutional-wide requirements of a general, or programmatic, character, whereas "procedures" denotes project-specific requirements generated by the organization responsible for the facility, as required by institutional policy.

In this framework, we drew the following conclusions:

1. There were "inadequacies" in the design.

   - The original design was adequate from a reliability point-of-view, but was considered deficient from the point of view of human engineering. It is unreasonable to believe that persons will routinely fasten, by hand, 48 one-inch bolts -- particularly if it seems unnecessary. An "autoclave-type" hatch would have been preferable, and with such a hatch, the incident would not have occurred.
   - The design configuration actually used (as a result of the decreased number of bolts and the change in location of the catcher) was clearly inadequate. The probability of failure was equal to "one" (Figure 8).

2. There were "inadequacies" in the "use" of the original design. The original design called for the use of 48 bolts and a lesser number was used. In addition, the original design called for the catcher to be against the rear door of the chamber, which also was changed. Without these changes the incident would not have occurred. This was a reliability inadequacy.

3. There were "inadequacies" in safe operating procedures. Written procedures designed to define actions necessary for safely operating the facility did not define precisely the number of bolts to be used or give the qualification for using fewer than the specified 48. As a result, reviewers of the procedures assumed that all bolts were being used, but did not audit "use" of the procedures. The procedures failed to state any correlation between the explosive charge and number of bolts used. A simple failure modes and effects study for the design changes could have revealed these deficiencies. The procedures made no reference to the type or amount of training needed by operational personnel and made no provision for obtaining it.

   In part, this is a human factors deficiency because it is unrealistic to expect new personnel to recognize problems without training. In part, this problem is due to administrative factors since institutional requirements for pressure safety and explosives safety training existed. Had personnel been trained in pressure safety and explosives safety, they should have been more questioning about the adequacy of design changes and their lack of inclusion in safe operating procedures.

4. There were "inadequacies" in the "use" of safe operating procedures. The "use" of safe procedures was inadequate because the facility was not treated as a pressure facility as it should have been, and was therefore not subject to mandatory laboratory-wide pressure safety practices by which significant design changes are reviewed.

Even though the design had been altered, the safe operating procedure was adequate to prevent any injury.

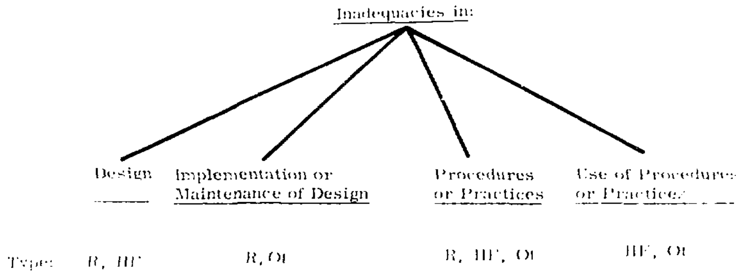
5. Finally, there was no adequate independent assurance that the design, its use, procedures, and the use of safe practices were adequate. Had there been such assurance (in any of these areas), the authors feel that the likelihood of the occurrence of the incident would have been appreciably lower. In this case a review of designs and procedures by human factors, reliability and quality assurance personnel would have been desirable. On-site audits of procedure "use" would probably have uncovered the 7- vs 48-bolt discrepancy and may well have led to a discovery that new personnel lacked knowledge of pressure safety practices.

Discussion -- In this example, inadequacies in design, its maintenance, safe operating procedures and practices, and the use of safe practices are observed. The original "inadequacy" of design was an HF problem. Lack of maintenance of the design was due to HF considerations (tendency to use fewer than the maximum number of bolts), to R "inadequacies" (a pressure failure analysis would have uncovered the inadequacies) and to other administrative factors relating to training. The inadequacies in safe operating procedures arose primarily because of the bolt issues (HF, R) and because design changes were permissible without adequate review (administrative and operational factors). Fundamentally, the safe operating procedures were not based on an adequate failure analysis for the design changes -- a "reliability" related question. The inadequacies in the use of safe operating practices stemmed from a lack of adequate recognition on the part of relatively new personnel that the system should have been treated as a pressure system (an administrative or operational problem). This lack of appreciation of the system as a pressure system led to failure to perform proper analyses and to update operating procedures to reflect their results (change the number of bolts, or don't change the material position). Finally, assurance of adequate design and procedures, through reviews, and of their use, through audits, was clearly not present. All of these inadequacies are summarized in Figure 9.

Example 2

A "continuously" operating hydrogen-burning furnace system which includes a hydrogen generator, compressors, surge tank, furnace and various valves (Figure 10). The original system is shown in solid lines, and a later system addition in dashed lines.

In the original system, the furnace was operated continuously until the compressor failed, a matter of months, because of continuous operation. The second parallel compressor was added to minimize down-time. Periodically, or if the original compressor failed, it was removed and serviced and the second compressor was used.



Legend (see text):

"R" - consideration of failure modes and consequences,

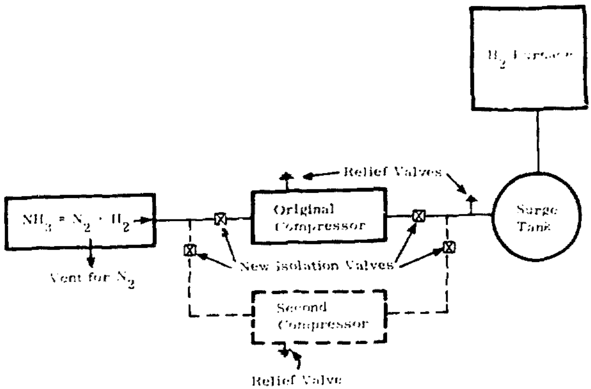
"HF" - consideration of situations which involve predictable human behavior that could lead to undesirable ES&H consequences.

"Ot" - provision of administrative support (in training, for example, or control actions or policy) or the operational situation itself

---

In addition, where inadequacies of R-, HF- or Ot-type existed, there was a de facto lack of assurance that the corresponding areas (design, etc.) were handled adequately (see text).

Figure 9. Summary of Inadequacies in Example 1.



Legend:

——— Original system.

– – – Parallel compressor added to facilitate replacement. This included isolation valves, as shown (⊠).

Figure 10. Simplified Schematic of a Hydrogen Furnace Facility

When the compressor failed one night the first person to arrive at work recognized the problem. Following safe operating procedures, he first shut off the system, then closed isolation valves at each end of the failed compressor (Figure 10). He then tried to open the isolation valves (gate valves with threaded stems) on either side of the parallel compressor. When he couldn't turn these latter isolation valves counter-clockwise, the employee assumed that they were open and energized the compressor. Both valves, however, were stuck shut. Returning later, he found the hydrogen furnace again cold and once more tried to turn the isolation valves on either side of the second compressor--which he left running. Unfortunately, he managed to free the stuck valve on the intake side of the running compressor first. The second stage of the compressor rapidly built up internal pressure. The pressure relief valve on the first stage of the compressor failed to function, and the pressure relief valve on the output side of the compressor was still isolated from the compressor by the stuck isolation valve. A section of the compressor head blew off, scattering shrapnel around the area. The compressor noise prior to this "explosion" alerted the individual, causing him to start running from the room just as the compressor "blew."

Because the potentially corrosive environment to which the relief valves were subjected was recognized, they had been scheduled, through the laboratory pressure safety program, for routine change-out with independently calibrated relief valves. New valves were routinely ordered, checked, and shipped to the organization responsible for the hydrogen furnace by the institution's pressure safety laboratory. In addition, the system was routinely scrutinized by three separate safety committees and a trained "pressure safety advisor."

When this incident is analyzed in the same format as the first example, reasons for the incident are found to be as follows:

1. There were "inadequacies" in the design. The original design was adequate, but the change, indicated by the dashed lines and legend of Figure 10, was judged inadequate from several points of view. First, gate valves, whose open/closed position was not immediately discernable by the operator, were used. In potentially critical systems, lack of a clear on-off indication is a typical human engineering deficiency. Had two-position ball valves, visually verifiable as either open or closed, been used, the accident would not have occurred. In addition, the second design (change) appears not to have been adequately documented. A "hard-to-find" design is inadequate and presents an administrative problem. Because the system was located in an area best described as a "plumber's nightmare", visual inspection of the system was difficult without, at least, a schematic as a guide. Thus, operational factors (relating to the operational configuration or characteristics) were important in this incident. Under the circumstances, labeling of the pipes would have been desirable also, as a part of the design requirements (a human engineering input). In addition, the second design should have called for the replacement of the pressure relief valve on the input side of the surge tank (see Figure 10) and two relief valves between each compressor and the isolation valve on its output side. Also, standard over-pressure, cut-off switches should have been a part of the system design. A simple failure modes and effects analysis (a reliability technique) or even a close look at a schematic diagram should have indicated possible problems. Finally, a "panic button" by the exit to shut off the entire system would probably have been of value (a human factors consideration).

2. There were "inadequacies" in the "use" of the original design. Use of the adequate first design was not maintained due to the change. Change requires adequate change control -- which in this case, was not defined. In addition, the failure to maintain properly operating relief valves is a "design maintenance" deficiency whose origin is operational (see below), with involvement of administrative and human factors.

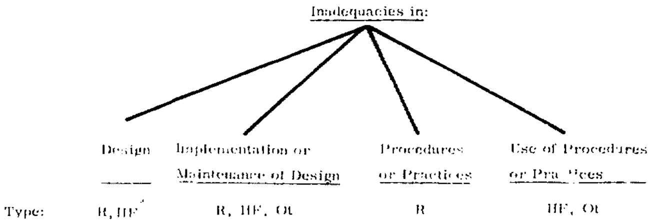
3. There were "inadequacies" in safe operating procedures. These did not address emergency procedures or procedures to be used when deviations from "normal" occurred. In particular, the procedures assumed that the parallel system would work properly, and made inadequate provision for shutting down the system when the original system failed. Since procedures did require shutdown before change-over, the system should have been shut down under these abnormal circumstances *during* change-over. Had the procedures been based on only a simple failure modes analysis, these problems would, in all likelihood, have been addressed. Safe practices were adequate.

4. There were "inadequacies" in the "use" of both safe operating procedures and practices. Both safe practices in the institution and the safe operating procedures called for a routine change-out of the pressure relief valves on the compressors. A system was set up to provide tested

valves on an adequate schedule, but these valves were never installed. They were found on a nearby shelf. This administrative problem was probably exacerbated by the "plumber's nightmare" quality of the area -- which made valve change-out difficult and, therefore, less likely to occur from the human behavior point-of-view.

5. While it is clear, with our 20/20 hindsight, that the number of reviews and audits made were adequate, they were poorly conducted and incomplete. The reviews were not of the designs, only of the system. Had audits focused on the adequacy of documented "plans" -- in this case, designs and procedures -- and their "use," and involved QA, R and HF inputs, the incident would not have occurred.

Here is just one example of the lack of completeness of the audits for "use"; there was no requirement to send the old pressure relief valves to the institution's pressure safety laboratory, nor a suitable tickler system to verify their receipt. Such a simple system could have drawn attention to the situation and prevented the accident. All of the inadequacies illustrated by this example are summarized in Figure 11.



Legend (see text):

"R" - consideration of failure modes and consequences,

"HF" - consideration of situations which involve predictable human behavior that could lead to undesirable ES&H consequences.

"Ot" - provision of administrative support (in training, for example, or control actions or policy) or the operational situation itself.

---

* In addition, where inadequacies of R-, HF- or Ot-type existed, there was a de facto lack of assurance that the corresponding areas (design, etc.) were handled adequately (see text).

Figure 11. Summary of Inadequacies in Example 2.

Discussion -- The two pressure safety examples reviewed here in some depth occurred because of inadequacies in the design, and its implementation or maintenance; and in safe practices or operating procedures, or their use. Fundamentally, there was no system to assure "adequacy" in each of these areas. A comparison of this situation with the traditional assurance role described earlier leads to the hypothesis that an assurance function like that shown in Figure 12 would be desirable in an ES&H program.[7] In the expanded setting of operations, "adequacy" of planning not only depends on technical and *human engineering* factors, but also involves administrative and operational factors, as well. Both classes of factors have been illustrated in the two pressure safety examples of this section. Perhaps the most notable administrative factor was the lack of training evident in Example 1. The most obvious operational factor was the work-setting ("plumber's nightmare") of the second example.

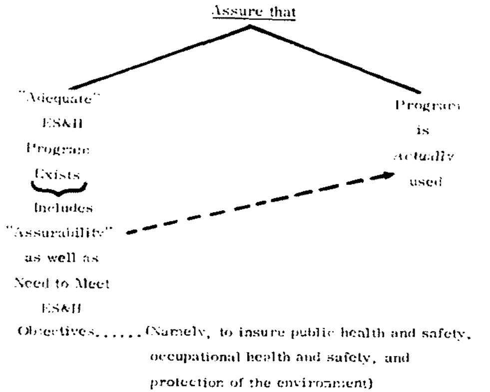


Figure 12. Two Primary Functions of an ES&H Assurance Program

Thus, we hypothesize the desirability of assurance and its general character, both of which will be tested in the next section. Again, this report does not address the feasibility or cost-effectiveness of an assurance approach to achieving ES&H objectives, it attempts to determine only whether the development of such an approach might be worth pursuing.

A Summary of Twenty-Three Other Incidents

Twenty-three other incidents were examined in somewhat the same fashion as the examples of the previous section. They are presented here in much less detail. Accident investigation reports were used almost exclusively as the source of information and the basis for judgment in these 23 incidents, whereas, in the examples of the previous section, some interviews were involved as well. Brief descriptions of the incidents and explanations of our findings follow.

Brief Incident Descriptions and Findings

Incident 1 -- A line surge in a high-pressure line occurred during a drilling operation. The line was inadequately fastened down (contrary to procedures), indicating a lack of understanding of failure modes and potential effects. The pressurized line came loose, knocking several persons forcibly to the ground. Medical attention was required. That some of the persons injured were not required for the operations in the area illustrates both an HF problem (people will be curious) and lack of administrative control. From an assurance point of view, an audit of procedures use might have pin-pointed inadequacies. Administrative policies and practices (HF) should have been reviewed for their adequacy in controlling unnecessary personnel in the area and their adequacy in assuring that procedures were being followed.

Incident 2 -- An I-beam, supporting a hoist being used to lift a 2500 lb capacitor bank, suffered a rotational force and "rolled" off the end of beams upon which it was resting. The I-beam fell into the lap of an employee. The I-beam was not adequately secured to its supporting beam because rotational forces had been overlooked; clearly a design inadequacy related to failure-mode identification. In addition, the responsible organization did not follow safe operating practices in implementing the design (an administrative issue). With respect to assurance, the likelihood that such a design fault could go unnoticed decreases significantly when "other specialties" (i.e., HF, QA, RA, Safety) review conditions.

Incident 3 -- A painter was working on scaffolding inside a 100,000-gal water tank, the top of which was 150 ft above the ground. In the last move of planks on the scaffolding before finishing the job, the painter disconnected his lifeline and plank-securing clamps at the same time. In combination, these actions violated safe practices, as did the fact that the painter was alone in the tank, unable to communicate with his helper outside on the ground. The painter fell from the scaffold inside the tank and was severely injured, a victim principally of HF, administrative, and operationally oriented deficiencies.

Incident 4 -- A person entered an exclusion target area of a high-pulse radiation device just prior to firing and was exposed to 160 mrem when the device fired. The system design permitted entry and firing in spite of interlocks, because the interlock system was inoperative during an automatic 10-s countdown period prior to firing -- a clear design deficiency. To reach the target area, the individual had to pass a gate, which was unlocked contrary to requirements of safe operating procedures. The opening of this gate prior to the 10-s automatic countdown would have actuated the interlock system, and made firing impossible, but the employee's timing was impeccable. Worst of all, the individual entered the area only because he had misunderstood oral directions (not covered in operating procedures) - a common HF concern. From the standpoint of assurance, a properly conducted design review should have caught the interlock deficiency, and audits of the use of procedures might have prevented the existence of the unlocked gate.

Incident 5 -- A workman slipped on a tanker ladder rung and injured his leg. The rungs were located too close to the tanker body to permit safe placement of feet; a design deficiency from the HF (physiological) point of view. In addition, the workman apparently had oil on the soles of his shoes, indicating poor safe-housekeeping practices.

Incident 6 -- Heavy equipment, while being loaded on a truck, went out of control and rolled from the truck, damaging a nearby fence and the equipment itself. Personnel, who were the only source of control of equipment movement during loading, managed to avoid being hit and injured. A simple safety analysis ("what if---?") would probably have indicated that some mechanical control of movement was desirable. In this case, no safe operating procedures existed for the specific operation, and safe practices were violated.

Incident 7 -- A workman, in the process of wrapping a heavy wire rope onto the drum of a hoist, unintentionally actuated a foot switch which started the drum turning. His finger was caught in the winding wire rope and mashed. The accident could have been avoided by a design which recognized error potential (a preferable approach) or through more thoroughly expressed procedures.

Incident 8 -- A material handler, transporting a 290-lb capacitor on a hand truck, slipped and lost control of the cart. The capacitor fell from the cart and struck an employee, causing a severe gash in his leg. The original slip was caused by oil on the sole of the material handler's shoes, indicating poor use of safe practices in the area. Also, the capacitor was not secured to the hand truck, a deficiency in procedures which stemmed from a lack of perception of "failure modes" and their consequences.

Incident 9 -- An instrumented manned helium balloon was being used to study atmospheric pollutants. Just prior to launch, and in accordance with plans, a man was placed on the railing of the gondola as ballast until launch time. The countdown to launch was unheard by the person, and the tether was released without warning. When the "human ballast" realized that the balloon was rising, he misjudged its height (because he was wearing biofocals) and suffered a fractured ankle when he fell. Hindsight indicates that the plan was inadequate and should have been reviewed. There were no safe operating procedures or analyses (an administrative problem), and the lack of communication at launch was a human error.

Incident 10 -- A machinist was turning a heavy, oversized part on a lathe. The mandrel failed and the part disintegrated, scattering pieces forcefully. A safe operating procedure was needed which recognized limitations on the equipment. In addition, there was a design deficiency in the mandrel, which was made of soft wood with a faceplate attached by screws that were sunk into glue joints. Although considerable energy was released no injury occurred. A design review would have been appropriate

Incident 11 -- A catastrophic failure of a self-breakdown, gas, high-power (2 MV, several hundred thousand A) switch in a large coaxial line caused the forcible separation of a section of the coaxial line and the 1.8-m movement of 1800 kg of line and attached equipment. No one was injured. The failure occurred as a result of a high-voltage breakdown in the high-pressure (11 atm) gas switch which caused a fracture of the acrylic housing of the gas chamber, permitting the force of the pressurized gas to be exerted on structural flanges which failed. The breakdown was largely due to the accumulation of dust as a result of infrequent maintenance. In addition, a lack of a pressure relief valve for the gas was a design deficiency.

Incident 12 -- The damaged head of a horizontal cask was being removed, involving the use of 16 threaded bolts as "jacks" around the periphery of the head. The use of a hydraulic jack and safety sling was planned for the final phase of removal. However, the 1100-lb head released unexpectedly and hit an employee, causing a severe bruise and minor contusions. Safe operating procedures were not prepared for the one-time operation, and work planning did not anticipate the "unexpected". "What if?" hazard considerations were lacking. Procedure and practice reviews should have reduced the probability of accident. The sling should have been installed at the beginning as a precaution. Estimating at what stage of removal it would be needed was at best an unsafe guess.

Incident 13 -- A workman was attaching a 560-lb test fixture to the lower rear ramp of a helicopter. The ramp was in full "up" position, secured by latches which were held in place by hydraulic cylinders. However, no hydraulic pressure was available because the aircraft's auxiliary power plant was not on. There was no "positive" lock under these circumstances (a design deficiency) and no failure-modes assessment had been performed (a procedural deficiency). The ramp fell with its heavy load and struck the workman, causing an acute back strain.

Incident 14 -- A small Dewar flask of hydrochloric acid at liquid nitrogen temperature used as a quench bath had been emptied of HCl, and a sample holder in the Dewar was being allowed to warm to room temperature. The sample holder was frozen to the wall of the Dewar flask, and as it began to warm, a small amount of acid trapped by the holder spurted out and struck a technician in the eye. The individual was not wearing safety glasses, as required by safe operating procedures, and safe practices were violated because no eyewash was available in the area. A safety shield was not included as a part of the equipment design.

Incident 15 -- While a machinist was grinding the cutting edge of a lathe-turning tool, the tool bit grabbed into the grinding wheel, wedging the machinist's finger between the tool holder and the grinder table. A broken bone and lacerations resulted. Investigation revealed that the tool bit had not been properly prepared and the grinder had been improperly maintained and inadequately inspected prior to use.

Incident 16 -- A workman was removing a pipe and cap from a 4 in. pipe using a 36 in. pipe wrench. The wrench slipped and the workman's fingers were mashed between the wrench and the floor. This might be regarded as uncontrollable within a reasonable safety system, or a violation of safe practices, since the workman was not pulling toward himself in acceptable practice. He may have been unable to do so due to the pipe location.

Incident 17 -- A bus driver ran into an unexpected slick spot on the road on a generally clear day. There had been a local hail storm of which he was unaware. All safe practices and procedures were followed subsequently, but the bus nonetheless overturned. The driver was seriously injured. Either this must be regarded as an "act of God", or the individual was insufficiently alert to road conditions while driving (poor practices, and an HF issue).

Incident 18 -- A quartz-ampoule, being used for the growth of large arsenic crystals, ruptured while being heated in an oven, producing a low-order explosion scattering arsenic and causing a small fire. No personnel were in the laboratory at the time, but a janitor in a nearby room reported the incident immediately. Probable causes were determined to be due either to unreliable temperature co[illegible] on the oven (no temperature-limiting controls, a design issue), or to fatigue induced in a quartz-ampoule due to an interaction with arsenic or to repeated high temperature/pressure cycling. In addition, total experimental system design lacked proper containment, and safe operating procedures did not call for it.

Incident 19 -- A commercially purchased electrolytic cell for generating hydrogen and oxygen exploded. Employee procedures followed those recommended by the equipment manufacturer, whose design and procedures were deficient. This may indicate a deficiency in equipment acceptance procedures (an assurance issue) at the laboratory involved. There was no injury.

Incident 20 -- A nitrogen surge tank became overpressurized, burst and was propelled 150 ft into the air. No injury to personnel was sustained. The overpressurization was due to system design inadequacies: inadequate regulator on the tank, no safety relief valve on the tank, and solenoid valves in the system which isolated the tank from any relief valve protection. The latter condition was the system status when the incident occurred. A "reliability" analysis had not been performed. Design reviews would have been desirable.

Incident 21 -- Three microcuries of strontium-90 were released in a laboratory due to a container failure. Contamination may have been undetected for as long as three months. Potential exposures are unknown. The basic issue was quality control for radioactive source (container) fabrication. In addition, procedures did not call for routine monitoring.

Incident 22 -- A personnel radiation dosimeter indicated a high radiation exposure, but no physiological or other evidence could be obtained to substantiate the high reading. Investigation determined that it was highly probable that the dosimeter had been exposed only as a result of "horseplay", although inattention to wearing the dosimeter might have been the cause. In any event, the issue is one of inadequate use of safe practicies in a radiation facility.

Incident 23 -- Several individuals were exposed to radiation from a small cobalt-60 source. The source was part of a portable radiation device in which the collimator was attached to a shielded source tube by a hose. The source was run from the tube to the collimator during use, and back to the source tube before personnel were allowed near the device. After operation, the return of the source to the tube was incomplete due to a defect in the source retracting mechanism, which constrained the source in the hose. Personnel assumed that the source had returned to the tube and entered the room containing the device. No radiation monitoring equipment was used. Accident analysis revealed that training, dosimetry control, safe operating procedures and administrative controls were all "less than adequate."

Summary and Conclusions

Table I summarizes our findings related to the 23 incidents investigated in this study. These incidents are largely industrial safety oriented, but do intersect the areas of fire protection, industrial hygiene and health physics as well. The primary concern, in all cases, was potential injury to the employee and to property. However, due to the nature of the incidents, these concerns, and any corrective actions, are equally applicable to public health and safety and environmental protection. In Table I, the designations of R or HF, in categories relating to design, represent inadequacies in the traditional system safety sense discussed in Section I. The use of the Ot (Other) in Examples 1 and 2 and Incident No. 11, relating to design "use," indicates a lack of change control or training. In attempting to "translate" these designations into meaningful categories in an operational setting, generally they are used to indicate inadequacies in:

"R" - consideration of failure modes and consequences,

"HF" - consideration of situations which involve predictable human behavior that could lead to undesirable ES&H consequences.

"Ot" - provision of administrative support (in training, for example, or control actions or policy) or the operational situation itself.

We readily admit that the assignment of these designations in the "Procedures and Practices" categories is highly subjective, but in our best judgment, they can be so assigned meaningfully and fully cover the generic nature of inadequacies. Finally, the use of NC in the last column of Table I indicates that, in our best judgment, no realistic control could be exercised to prevent the incident. Whether Incident Numbers 16 and 17 deserve this designation is debatable (see the previous section).

TABLE I

Categorization of Incident Causes (See text for explanation where entries occur> there was a concomitant lack of assurance)

Incident Number	Inadequacies in: Design	Implementation or Maintenance of Design	Procedures or Practices	Use of Procedures or Practices	Statistical
1				R, HF, Ot	
2	R			Ot	
3				HF, Ot	
4	R		HF	HF, Ot	
5	HF			HF, Ot	
6			Ot	R, HF, Ot	
7	R, HF		HF, Ot		
8			R, Ot	Ot	
9	R		R, Ot	HF	
10	R			R	
11	R	R, Ot			
12			R, HF, Ot		
13	R, HF		R, Ot		
14	R			R, HF, Ot	
15		R		HF, Ot	
16				HF.........(?).....	NC
17				HF, Ot......(?).....	NC
18	R	R	R, Ot		
19	R		R		
20	R				
21		R	Ot		
22				HF, Ot	
23	R		R, Ot	HF	
Ex-1	R, HF	R, Ot	R, HF, Ot	HF, Ot	
Ex-2	R, HF	R, HF, Ot	R	HF, Ot	

In all cases where inadequacies are indicated in Table I, one can argue that there was also an inadequacy in assuring proper design, its implementation, and so forth. Thus had such assurance been present, we assert that the occurrence of each of the incidents examined, with the possible exception of Numbers 16 and 17, would have been much less likely.

Carrying this a step further, Table II presents a "statistical" summary of the results shown in Table I. 96% to 100% of the incidents were "preventable" in this assurance context. Without a detailed discussion, we conclude that the development of an analogue of systems safety that addresses operational issues would be desirable. Nearly 60% of the inadequacies were found in the "operational" categories associated with procedures and practices. More significantly perhaps of the 23 incidents that were judged to be clearly due to inadequacies (that is omitting Nos. 16 and 17), 21/23, or over 91% could have been mitigated by attention to operations alone, whereas only 17/23, or about 74% would have been addressed by attention to systems safety (design) alone. These data suggest, for those willing to extrapolate from a relatively small data base, that equipment inadequacies are more likely to occur in organizations that have operational inadequacies than in organizations that have none. This finding is, perhaps, not unreasonable since assurance that design is adequate and maintained is an operational activity.

TABLE II

Brief Analysis of Inciden. Causes

	Inadequacies In:				
	Design	Implementation or Maintenance of Design	Procedures or Practices	Use of Procedures or Practices	Statistical
Totals	15	6	13	15-17	0-2
	21		28-30		0-2
Percentages	41%		55-59%		0-4%
Multiple Inadequacies - 72%					38

Finally, a qualification. Clearly, hindsight is a much better basis for analysis than foresight. While we have attempted to analyze these incidents in terms of inadequacies that we believe would be recognized by QA, R, or HF specialists, in combination with persons skilled in the ES&H related disciplines, there is little in the way of proof that this is so. With this caveat we conclude from the results of Tables I and II that an ES&H assurance program designed to assure the adequacy of

- design,
- its implementation and maintenance.
- safe operating procedures and practices, and
- their use,

would appear to be a theoretically desirable concept, and that planning for such an activity should be undertaken, and the cost-effectiveness of such plans studied.

A further conclusion of considerable importance that may be drawn from this study relates to the role of risk analysis in accident prevention. Table I suggests that "Reliability" is an important facet of accident prevention. As discussed in the text, the major need relating to R was, in all appropriate cases, an understanding of failure modes and generic effects. Nowhere, in our considered opinion, would prevention of the accidents studied here have necessitated a quantitative risk analysis in which each potential consequence was understood in terms of its probability of occurrence. Thus, considering the limited scope of this study, we can conclude tentatively that risk analysis (when this term is used to denote quantification of risk vs consequences) offers relatively few benefits for accident prevention. This, to us, suggests that efforts to join in the increasingly popular activity of "risk analysis" should be undertaken with care and discrimination.

In closing, it is perhaps well to point out, for those familiar with other approaches to accident investigation, that there is less difference between the ultimate categories of concern studied here and those found in other approaches than might be apparent at first. Generic analysis of why procedures are not used, for example, leads one to consider familiar inadequacies in administrative support, policy, motivation, communication, training, and so forth. Thus, a program designed to achieve use of adequate procedures must have these familiar elements. Philosophically, however, the focus of an assurance approach based on system safety principles is very different. The emphasis is on a structured approach to independently assuring that the needed elements of an ES&H program are adequate and used. In this context, policy, training, and so forth can be derived (as just suggested) as necessary and sufficient elements, whose existence and adequacy is to be independently judged. In this way, many of the familiar elements of "accident-prone" theories (Reference 2) or management oversight and risk trees (Reference 3) become elements of logically derivable "checklists" to be used in assurance reviews and audits.

Since the findings presented here were first obtained earlier this year, considerable progress has been made toward defining and testing the generic elements needed in an assurance approach to ES&H program management. Descriptions of this work will be found in References 1, 4, 5, 6 and 7.

References

1. C.A. Trauth, Jr., *Planning for a DOE ES&H Assurance Program*, SAND78-1887, Sandia Laboratories, to be published.

2. A.D. Swain, "The Human in Systems Safety," Industrial and Commercial Techniques, Ltd., Camberley, England. Revised July 1976 (published in the U.S. by the author.)

3. "MORT" - Management Oversight and Risk Tree," a program analysis system developed by the Idaho Operations Office of the Department of Energy and Aerojet Nuclear Co.

4. A.C. Ellingson, C.A. Trauth, Jr., L.M. Jercinovic, and D.E. Farr, *An Approach to Incorporating Proven Quality Assurance, Reliability, and Human Factors Principles into Industrial Safety Programs*, SAND78-0581, Sandia Laboratories, June 1978

5. A.C. Ellingson, C.A. Trauth, Jr., *An Approach to Incorporating Proven Quality Assurance, Reliability, and Human Factors Principles in Fire Protection Programs*, SAND78-0582, Sandia Laboratories, September 1978.

6. A.C. Ellingson, W.D. Burnett, D.E. Farr, *An Approach to Incorporating Proven Quality Assurance, Reliability, and Human Factors Principles into Environmental Health Programs*, SAND78-0583, Sandia Laboratories, July 1978.

7. M.S. Tierney, *Requirements for an Environment, Safety and Health Assurance Program at the Working Levels of Organization*, SAND78-2003, Sandia Laboratories, to be published.