DEVELOPING OPERATIONAL SAFETY REQUIREMENTS FOR NON-NUCLEAR FACILITIES

Jeffrey A. Mahn, Sandia National Laboratories
Sandia National Laboratories
P.O. Box 5800, MS 0369
Albuquerque, NM 87185-0369
(505) 844-9995

Introduction

Little guidance has been provided by the DOE for developing appropriate Operational Safety Requirements (OSR) for non-nuclear facility safety documents. For a period of time, Chapter II of DOE/AL Supplemental Order 5481.1B (Ref. 1) provided format guidance for non-reactor nuclear facility OSRs when this supplemental order applied to both nuclear and non-nuclear facilities. However, after the nuclear facility portion of the supplemental order was superseded by DOE Order 5480.23 (Ref. 2), it was never rewritten. Thus, DOE Albuquerque Operations Office personnel still want to see non-nuclear facility OSRs in accordance with the supplemental order (i.e., in terms of Safety Limits, Limiting Conditions for Operation, and Administrative Controls). Furthermore, they want to see a clear correlation between the OSRs and the results of a facility safety analysis. Unfortunately, the supplemental order addresses neither the type of safety analysis to be performed for non-nuclear facilties nor how OSRs are to be derived from safety analysis results.

This paper demonstrates how OSRs can be rather simply derived from the results of a risk assessment performed using the "binning" methodology of SAND95-0320 (Ref. 3).

An "OSR-friendly" Risk Assessment Methodology

The methodology of SAND95-0320 is used to evaluate accident scenario likelihoods of occurrence by considering the failure probabilities of facility structures and systems and the probabilities of human errors involved in accident scenarios. The methodological approach is to first characterize individual accident scenarios in terms of the following four elements, as applicable:

Initiating Event
System Response
Operator Response
Structure Response

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy.

DISCLAIMER

These elements allow ready identification of relevant safety structures and systems as well as worker safety programs that are applicable to individual accident scenarios. The frequency of an accident initiating event and the probabilities of applicable system and structural failures and associated human errors are then determined using generic frequency/probability data provided in the methodology report. The overall likelihood of occurrence of an accident is found by considering these elements as the functional events of an event tree (Figure 1). The methodology report provides four levels of "binning" criteria for both consequence severity and likelihood of occurrence, which can be used as shown below for developing appropriate OSRs.

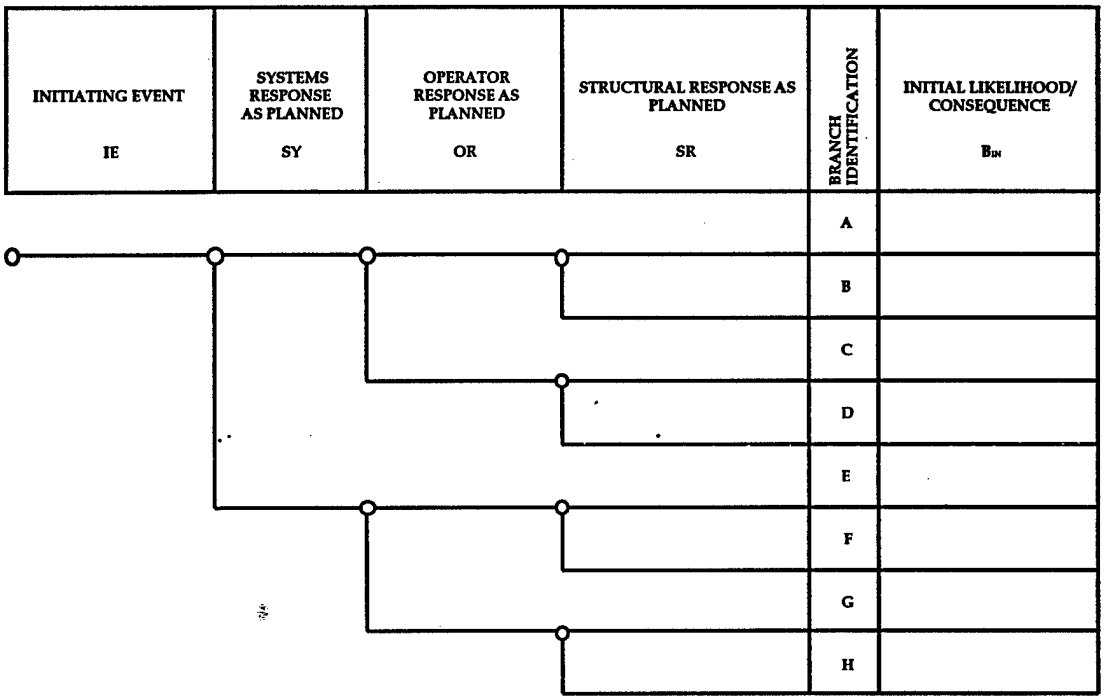

Figure 1. Generic Event Tree for Accident Likelihood of Occurrence Evaluation.

Derivation of OSRs - A Case Study

This process for developing OSRs can best be understood by illustrating how it was used to derive OSRs for Sandia National Laboratories' Kauai Test Facility (KTF). The potential accidents evaluated for the KTF included 10 operational accidents, 3 natural phenomena occurrences, and an aircraft crash scenario. The structure, system, and component (SSC) failures and human performance errors evaluated for the operational accident scenarios are shown in Table 1. The operational accident assessment results are summarized in Table 2.

These results indicate that only 6 of the 10 operational accidents are considered credible, while only 3 of the 6 credible accidents have potentially serious consequences. There are no credible

accidents having the potential for serious consequences to the offsite public. The three credible accidents with the potential for serious worker consequences are the Missile Assembly Building rocket motor fire, the launch pad missile ignition during "safing," and the dropped solid rocket motor explosion. The accident scenario SSC failures and human performance errors of Table 1 thus identify the relevant safety structures and systems and relevant worker safety programs relied upon for prevention and mitigation of these operational accidents, as shown in Table 3.

Table 1. KTF Accident Scenario Failures

Accident	SSC Failures	Human Errors
Launch Operations Bldg. (LOB) Fire	Fire detection system Fire suppression system	Inadequate response by PMRF Fire Department personnel
Missile Assembly Bldg. (MAB) Rocket Motor Fire	Ordnance grounding system	Worker failure to maintain electrical ground
Launch Pad Missile Ignition During Safing Procedure	Ordnance grounding system	Worker failure to preclude undesired electrical current
Uninterruptible Power Supply (UPS) Failure with Loss of Onsite AC Power	Onsite AC power system Uninterruptible power supply	None
Dropped Solid Rocket Motor Explosion	Crane/hoist	Inadequate maintenance of crane/hoist systems
Atmospheric Release of Unsymmetrical Dimethylhydrazine (UDMH) from Storage	Primary storage container	Inadequate surveillance monitoring
Atmospheric Release of UDMH During Fueling	UDMH fuel transfer system	Inadequate actions by emergency response personnel
Hazardous Material Leak to Soil	Primary storage container Secondary containment structure Leak detection system	Inadequate surveillance monitoring of fuel storage containers
Electromagnetic Field Radiation Exposure (Radar)	Radar tracking system	Radar operator error
Lightning Strike of Fueled STARS Missile	Ordnance grounding system Lightning protection system	Failure to ensure adequate electrical ground

There are no structures, systems, or components (SSC) associated with preventing or mitigating accident consequences to the offsite public, while only one safety system is identified as necessary to prevent significant, credible accident consequences to workers --- the ordnance grounding system. Operability of this system represents the lowest functional capability or performance level of equipment required for continued safe operation of the KTF, and thus constitutes a limiting condition for operation (LCO). Note that even though an explosion of a

dropped solid rocket motor is considered to be a credible accident, drop tests with Class 1.1 rocket motors have not been able to achieve a detonation event. Thus, KTF cranes and hoists have not been classified as safety systems.

Table 2. KTF Operational Accident Results Summary.

Accident	Public Consequence	Worker Consequence	Credible? ($>10^{-6}$ yr^{-1})
Launch Operations Building (LOB) Fire	NA	Negligible	Yes
Missile Assembly Bldg. (MAB) Rocket Motor Fire	NA	Catastrophic	Yes
Launch Pad Missile Ignition During Safing Proc.	NA	Catastrophic	Yes
Uninterruptible Power Supply (UPS) Failure with Loss of Onsite AC Power	NA	Negligible	No
Dropped Solid Rocket Motor Explosion	NA	Catastrophic	Yes
Atmospheric Release from Unsymmetrical Dimethylhydrazine (UDMH) Storage - Fast - Slow	Critical NA	NA Marginal	No Yes
Atmospheric Release of UDMH During Fueling	Critical	NA	No
Hazardous Material Leak to Soil	Negligible	NA	No
Electromagnetic Field Radiation Exposure (Radar)	Negligible	NA	Yes
Lightning Strike of Fueled STARS Missile	NA	Negligible	No

One other system has also been given LCO status because of its importance to the explosive safety program, even though its failure does not necessarily contribute to an accident. The Potential Gradient Measurement System is used to control explosive operations on site such that all outdoor explosive operations and indoor operations with unsafed ordnance are to be terminated whenever the atmospheric potential gradient reaches a level of ±2000 volts per meter.

Since the other safety structures and systems listed above are not necessary to prevent significant accident consequences to workers, their effective performance in preventing or mitigating lesser accident consequences can be assured via normal conduct of operations program controls (e.g., procedures). Enhanced effectiveness of worker performance in preventing or mitigating accident consequences can similarly be achieved via safety training programs. Thus, both procedures for assuring reliability of these structures and systems and associated safety training for facility workers are classified as administrative controls within the context of operational safety requirements.

Table 3. Facility Structures, Systems, and Worker Safety Programs Providing Accident Prevention/Mitigation Functions

Accident	Relevant Safety Structures & Systems	Relevant Worker Safety Programs
LOB Fire	LOB fire detection system LOB fire suppression system	Fire extinguisher awareness Emergency response awareness
MAB Rocket Motor Fire	Ordnance grounding system	Explosives safety
Launch Pad Missile Ignition During Safing Procedure	Ordnance grounding system	Explosives safety
UPS Failure with Loss of AC Power	Onsite diesel generators Uninterruptible power supply	None
Dropped Solid Rocket Motor Explosion	Cranes/hoists	Crane, hoist, and rigging safety
Atmospheric Release from UDMH Propellant Storage	UDMH storage tank with overpack	Hypergolic propellant awareness
Atmospheric Release of UDMH During Fueling	UDMH fuel transfer system	Hypergolic propellant awareness
UDMH Leak to Soil	UDMH storage tank with overpack Above-ground, concrete lined pit for UDMH tank	Hypergolic propellant awareness
Gasoline Leak to Soil	Double-walled, underground gasoline storage tank Gasoline tank leak detection system	None
Diesel Fuel Leak to Soil	Diesel fuel storage tank Above-ground, concrete basin for diesel fuel tank	None
Radar Exposure	Radar tracking system	None
Lightning Strike of STARS Missile	Ordnance grounding system Lightning protection system	Explosives safety

This evaluation of the KTF accident analysis results culminated in the following Operational Safety Requirements:

Limiting Conditions for Operation

CONDITION	NON-COMPLIANCE ACTION	RESPONSE
The ordnance grounding system shall be operable with a resistance to ground not exceeding 0.001 ohms.	Explosive operations shall not be permitted on site.	Explosive operations may be initiated after the ordnance grounding system is declared operable.
The potential gradient measurement system shall be operable with a maximum potential gradient of less than ±2000 V/m.	Outdoor explosive operations and indoor operations with un-safed ordnance shall be suspended.	Explosive operations may not be resumed until 15 minutes after the atmospheric potential gradient returns to the acceptable range.

Administrative Controls

Conduct of Operations

- Ordnance grounds shall be tested and certified within a year of anticipated use in accordance with KTF-OP-1013, *KTF Ordnance Ground Testing and Certification.*
- Lightning protection on explosive facilities shall be visually inspected annually and electrically tested at least every 47 months in accordance with KTF-OP-1022, *KTF Lightning Protection Inspection and Certification.*
- The Launch Operations Building fire detection and suppression systems shall be inspected annually.
- The uninterruptible power supply shall be tested periodically in accordance with the manufacturer's recommendations.
- The potential gradient measurement system shall be maintained and calibrated annually in accordance with KTF-OP-1019, *KTF Potential Gradient System Calibration and Use.*
- The wind radar system is operated in accordance with KTF-OP-1515, *KTF Wind Radar System Operation.*
- Use and operation of the special KTF low power radios in the vicinity of any ordnance is governed by KTF-OP-1551, *Control and Use of Low Power RF Radios at KTF.*
- All explosives related work and explosives storage is conducted in accordance with SOP SP472378, *Operations at Kauai Test Facility*, Appendix B (Explosives Safety).
- All operations involving overhead cranes are conducted in accordance with KTF-OP-1553, *Crane, Rigging, and Hoisting Operations at Kauai Test Facility.*
- Hazardous operations, such as rocket motor movements, launch pad operations, hypergolic propellant activities, and rocket launches are conducted in accordance with SOP SP472378, *Operations at Kauai Test Facility*, Appendix C (Launch and Hazardous Operations Control).
- Transportation and loading of hypergolic fuels requires the participation of emergency response personnel and equipment in accordance with SOP SP472378, *Operations at Kauai*

Test Facility, Appendices C (Launch and Hazardous Operations Control at Kauai Test Facility) and F (KTF Operating Procedures).

- The loading of hypergolic fuels is performed by NASA White Sands personnel in accordance with NASA Standard Operating Procedures.
- In the event of a booster misfire, all systems will be returned to a safe condition, and the launcher area restricted to all personnel for a minimum of 30 minutes.
- Personnel are to maintain a separation distance of 2 feet (0.61 m) from antennae associated with radiating airborne transmitter system with average power ratings greater than 7 watts, or with frequencies greater than 1 GHz.
- Motor vehicles operating without spark arrested exhaust systems are to remain a minimum of 100 feet (30.5 m) from rocket motors and missiles.
- Two of the four available power systems (Kauai Electric Company, 2 onsite diesel electric generators, and the site uninterruptible power supply) must be operable prior to initiating a launch sequence.
- The onsite hypergolic propellant storage tanks shall be inspected weekly for observable leakage in accordance with KTF-LP-006, *Hazardous Material Storage Monitoring.*

Training

- Personnel working in the areas where liquid hypergolic propellants are present have hypergolic propellant awareness training as well as additional training that is dependent upon the individual's involvement with the propellants.
- Personnel working with explosives at KTF are trained in accordance with the requirements of the Sandia Explosives Safety Manual. Training requirements are dependent upon the individual's job classification.
- Personnel working with cranes, hoists, and rigging equipment are trained in accordance with the requirements of KTF-OP-1553, *Crane, Rigging, and Hoisting Operations at Kauai Test Facility.*
- All KTF personnel are required to complete fire extinguisher awareness and SNL emergency response awareness training annually.

Non-compliance Action

If the KTF is found to be out of compliance with any of the above administrative controls, then the out of compliance condition must be corrected within 72 hours or a violation of the OSRs must be declared.

The reason for inclusion of a non-compliance action is because administrative controls do not have action statements as the LCOs do. Thus, if a non-compliance with an administrative control is discovered there is no opportunity to rectify the condition prior to the occurrence of an OSR violation. The inclusion of a generic action statement to cover all administrative control programs permits a non-compliance to be corrected within a reasonable time following discovery of the non-compliance without incurring an OSR violation.

References

1. DOE/AL Supplemental Order 5481.1B, *Safety Analysis and Review System*, January 1988.

2. DOE Order 5480.23, *Nuclear Safety Analysis Reports*, April 1992.

3. Mahn, J.A., G.W. Hannaman, and P.M. Kryska, *Qualitative Methods for Assessing Risk*, SAND95-0320, Sandia National Laboratories, May 1995.

Report Number (14) SAND--97-2726C
CONF-980616--

Publ. Date (11) 199711
Sponsor Code (18) ~~DOE/DP~~ DOE/MA, XF
UC Category (19) UC-907, DOE/ER

DOE