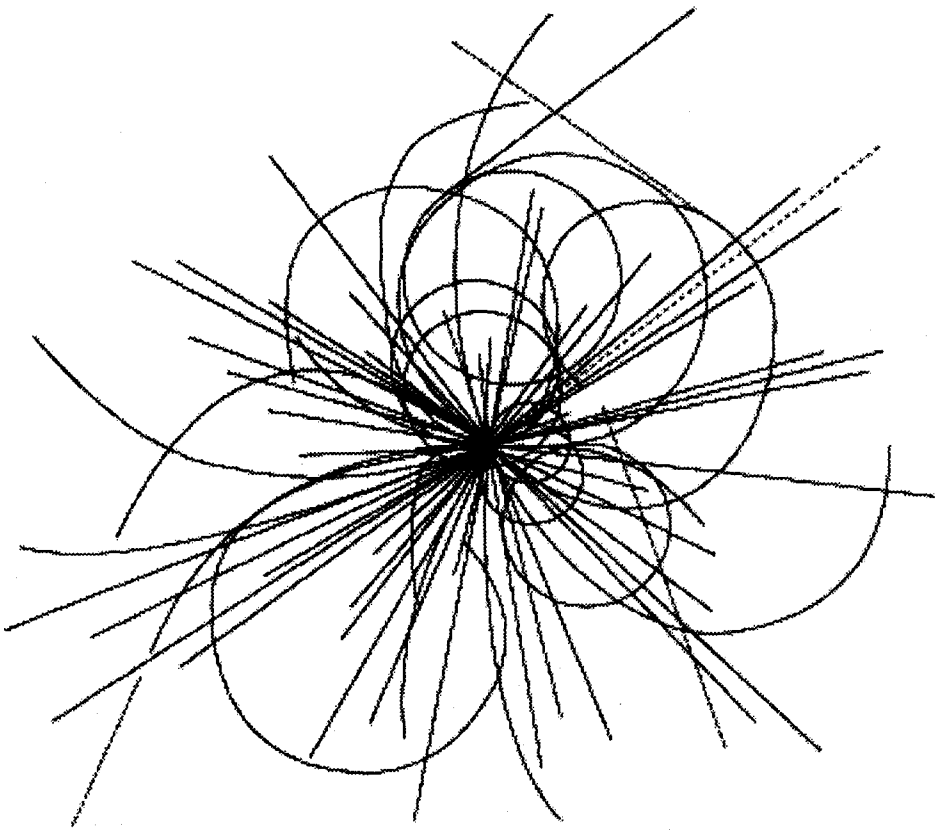
SSCL-Preprint-486

SSCL-Preprint-486
May 1993
Distribution Category: 400

R. Lavelle

A Systems Approach to Hazard and Risk Management for the SDC Detector



Superconducting Super Collider Laboratory

To be published in *Supercollider 5*

SSCL-Preprint-486

A Systems Approach to Hazard and Risk Management for the SDC Detector*

R. Lavelle

Superconducting Super Collider Laboratory†
2550 Beckleymeade Ave.
Dallas, TX 75237

May 1993

*Presented at the Fifth Annual International Symposium on the Super Collider, May 6–8, 1993 San Francisco, CA.
†Operated by the Universities Research Association, Inc., for the U.S. Department of Energy under Contract No. DE-AC35-89ER40486.

A SYSTEMS APPROACH TO HAZARD AND RISK MANAGEMENT FOR THE SDC DETECTOR

Robert F. Lavelle

Superconducting Super Collider Laboratory*
2550 Beckleymeade Avenue
Dallas, TX 75237-3997

INTRODUCTION

The realities of the day seem almost insurmountable: Environmental impact statements, public hearings, stringent enforcement of the existing government ES&H regulations together with new and seemingly costly requirements; the list goes on. It is self-evident that the recent years have seen a significant increase in environmental and system safety awareness. We are now beginning to see the effects of this awakening on the Department of Energy (DOE) and its High Energy Physics (HEP) programs.

The days of a laissez-faire and sometimes cavalier approach to safety and environmental issues are over. Environmental awareness and personnel safety are now paramount design criteria. In our environment, the importance of ES&H is now on par with physics performance itself, especially in the eyes of the customer. The predicament is further complicated by budget-driven extensions of development profiles, sometimes elongated out to ten or twelve years. All of these facts combine to render the traditional "post-hoc" safety analysis program obsolete.

The predominant question today centers on how HEP Project Managers can implement a cost and performance effective ES&H program. This program must at once address the needs of the customer, the needs of the research, the needs of the public, and must be dynamic enough to be viable over a ten or twelve year development schedule.

We must begin by coming to an understanding of our working environment, an understanding of the customer's requirements and a utilization of lessons learned from others who have existed in a similar environment. Surprisingly enough, there is real help in answering these questions. Let's characterize the current HEP environment in which such a program must operate.

THE NEW HEP ES&H ENVIRONMENT

Two facts of life conspire to present a complicated development environment. First, is just the nature of the beast; as we look deeper and deeper into the subatomic realm, we are required to use mechanisms of increasing size and complexity. Second, the more we learn

*Operated by the Universities Research Association, Inc., for the U.S. Department of Energy under Contract No. DE-AC35-89ER40486.

about the world around us, the more we realize that our performance as global custodians has been, to use a Washington term, dispositive. Thus, the new emphasis on ES&H in the first place.

So, now we find ourselves at the SSC, designing the world's largest and most complex P+P- particle detector, the SDC. It is a detector with significant ES&H challenges, a multi-million dollar ES&H budget, and a design environment that is the most restrictive and most carefully monitored in HEP history. We can anticipate a continuous string of assessment and audits in one form or another. Detailed design reviews, documentation reviews, and quantitative and qualitative ES&H analyses are all built into the development management approach.

The New Detectors

Today's high energy particle detectors are significantly larger and more complex than their predecessors. The SDC Technical Design Report (TDR) and the SDC Conceptual Safety Analysis Report (CSAR) describe in detail both the size and complexity of the SDC as well as the types of hazards and risks indigenous to a detector of this ilk. Of note for this article are the inherent hazards associated with the various detection mechanisms, including flammable gases and liquids, health physics concerns, and hazardous atmospheres. In addition, the detector is honeycombed with maintenance access confined spaces that will have to be managed.

The New Regulatory Environment

The DOE Energy Research Office has had at its disposal a comprehensive set of ES&H requirements and guidance that can be applied to the design and operation of particle detectors. In the past, these regulations, in the form of the nuclear-oriented DOE Orders, have been applied with some degree of uncandor. In today's environment, the DOE is calling for a much more sincere approach as well as attempting to better define the safety criteria for detectors in its new accelerator order, DOE 5480.25, Safety of Accelerator Facilities. A sincere attempt at compliance with this list is a formidable task indeed.

The Systematic Approach

The SDC ES&H program is an attempt to provide a viable approach to ES&H while living within tight budget constraints. To do this, three tasks are paramount. First and foremost, we must design and operate a safe, effective detector. Second, we must comply with the letter of the customer's (DOE's) ES&H requirements. And, third, we must capitalize on existing approaches and lessons learned from others in heavily scrutinized, requirements laden environments. Both the Department of Defense and the Nuclear Power Utility organizations operate in similar environments. Both are environments characterized by protracted development schedules and detailed design and analysis requirements. A number of important aspects dominate a successful program in their environments as well as in ours:

1. A well defined, detailed ES&H Program Plan and Schedule.
2. An austere but adequate funding profile that provides for continued engineering support for the life of the development.
3. Consistent and effective documentation trail.
4. Cost and Schedule Management.
5. Judicious use of quantitative and probabilistic analyses.
6. Gravitation towards design implementations that can be adequately analyzed using qualitative techniques.
7. Standardized analysis techniques.
8. Flowdown of responsibility from ES&H management to the actual design engineers.

The SDC ES&H approach coalesces all of the aforementioned points into an effective, albeit somewhat patchworked, systematic approach to requirements flowdown, design analysis, and analysis documentation that is both safety requirements and cost effective.

THE SDC SYSTEMATIC APPROACH

Figure 1 depicts both the four key elements of an effective program and the schedule flow. Foremost is a well defined program plan. This plan provides a framework for the ES&H organization to function. The majority of effort lies in the area of requirements flowdown into the design activities. The results of the design engineering efforts are subjected to an iterative series of qualitative and quantitative design reviews.

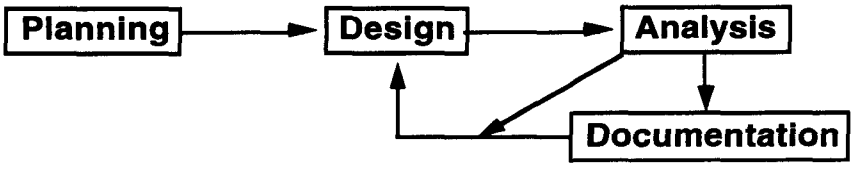


Figure 1. SDC ES&H Program Key Elements.

While ES&H is not the only area addressed at these both formal and informal reviews, it is a key player. The results of both the design work and the subsequent analyses are documented in a sequentially more detailed set of Safety Analysis Documents (SAD's). It is important to note that both the design reviews and the SADs act as a closed loop feedback system allowing both designers and management to assess design and program compliance.

The ES&H Program Plan

The ES&H Program Plan details the design, analysis and management tasks to be performed. It is a description of the methodology that you intend to employ to identify, evaluate and either resolve or manage all hazards and risks associated with the system in question. The SDC plan is modeled after the requirements MIL-STD-882 task 101 and its associated Data Item Description (DID) DI-SAFT-80100. The SDC plan provides the following types of information:

- ES&H Organization. Describes the organizational elements within the SDC collaboration with ES&H responsibility. It defines the responsibilities, authorities, and accountability of both management and engineering personnel.

- ES&H Program Schedule. Identifies integrated system activities and provides milestones for design requirements flowdown, design analyses, design reviews, and documentation deliveries. While the official version of this document does not include manloading for each task, the initial versions were used extensively for just that purpose.

- ES&H Requirements. This section describes three important aspects of the ES&H program: 1) the methods to be used to identify ES&H requirements, including health physics and human factors engineering. These requirements are provided to the engineering community via the SDC Engineering Guidelines. 2) ES&H assessment procedures for characterization of hazards identified in both the initial conceptual qualitative analyses and the more detailed quantitative type analyses, i.e., FMECA. 3) Management controls to be used to ensure compliance with requirements or justify deviations from those requirements

- Hazard Analysis Procedures. Detailed procedures for both qualitative and more detailed quantitative hazard analysis procedures.

This type of plan, with its associated level of detail provides a basis of understanding between the SDC collaboration and their customer, the SSC Laboratory and the DOE. This plan ensures that adequate consideration is given to ES&H issues during the development of the detector system.

Requirements Flowing into Design

The starting point in the implementation of this program is the identification and understanding of the requirements. Requirements can be thought of as consisting of two main categories, programmatic and criteria. Programmatic requirements refer the program precepts mandated by the customer; in this case, the DOE. Criteria refer to design stipulations. These are hard requirements that directly affect the hardware/software design of the system. The requirement for a Critical Design Review (CDR) is a programmatic requirement. Compliance with the National Electrical Code is a design criteria.

Both the programmatic and criteria requirements for the SDC detector are located in several different types of documents, including the DOE orders and their associated references (it's not uncommon to have requirements documents nested four and five deep on a government contract), SSC Laboratory Standards, Physics Research Documents, and even some self-imposed documents. In the interests of design acceptance and simplicity, these requirements are coalesced and flowed down to the engineering community in the form of SDC Engineering Guidelines. It's important to note that verification of compliance with these guidelines is a central task at both internal and external design reviews. These ES&H guidelines are part of a larger set of guidance documents that encompasses all the engineering best practices approach that SDC is taking.

Design Reviews

The SDC program is tied to the overall programmatic requirements in the SDC Program Management Plan. A formal design review process has been implemented consisting of five formal reviews as shown in Table 1.

Table 1. Design Phase, Design Reviews and associated documentation.

CONCEPTUAL DESIGN	DETAIL DESIGN	CONSTRUCTION	COMMISSIONING
PRELIMINARY DESIGN REQUIREMENTS REVIEW	PRELIMINARY DESIGN REVIEW CRITICAL DESIGN REVIEW	ACCEPTANCE TEST PLAN REVIEW	OPERATIONAL READINESS REVIEW
CSAR	dPSAR PSAR	SAR	FSAR

Documentation

Detailed information on the breadth of these reviews is available in the SDC Program Management Plan. The intent is simple: Provide a vehicle for assessing design compliance with criteria at each logical transition point in the engineering development and construction of the SDC detector system.

Each of the above referenced design reviews is associated with an ES&H SAD delivery from the system or subsystem under review. The reviews and the SADs track the various life cycle phases of the system as illustrated in Table 1.

PROGRAM STATUS AND INITIAL RESULTS

The SDC ES&H program was initially implemented in the fall of 1991, subsequent to the approval of the SDC Letter of Intent and receipt of the approval to proceed with a Technical Design Report (TDR). This initial phase of the program has been dubbed the "conceptual phase," and the SAD that resulted from the first round of qualitative analyses is the SDC Conceptual Safety Analysis Report (CSAR). The initial version of the CSAR was provided to the laboratory for review together with TDR on 1 April 1992. The CSAR REV "A" was released in October of that same year. The SDC design and CSAR have been subjected to expert review by three panels: a Laboratory Review Panel, the Program Advisory Review, and by the DOE. Program approach, conceptual designs, and the CSAR all received positive reviews. The first results from the ES&H program are presented in Figure 2. The initial analysis of the conceptual SDC design yielded 60 catastrophic accidents with a probability of occurrence that was unacceptable. Subsequent to this analysis, and after engineering iterations in light of the analysis, the probability of occurrence of these accidents has been reduced to either improbable or impossible.

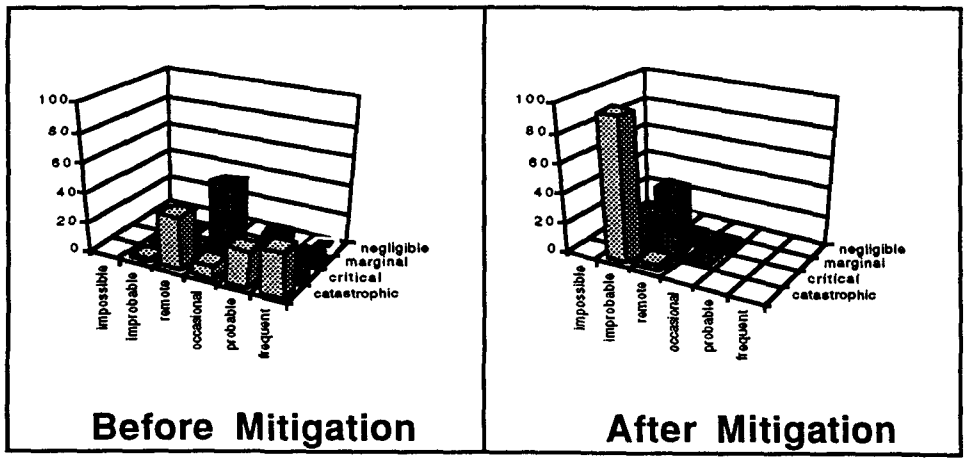


Figure 2. Initial ES&H Program Results.