LSST Hazard Analysis Plan

Large Synoptic Survey Telescope 950 N. Cherry Avenue Tucson, AZ 85719
www.lsst.org

REVISION SUMMARY:

1.

Contents

1 Introduction

The U.S. Department of defense has developed a formal system safety process, and has documented it in MIL-STD-882D w/CHANGE 1, *Standard Practice for System Safety* (Draft, 29 March 2010). The LSST project has adopted this process as detailed in this document.

Central to the process outlined in MIL-STD-882D w/CHANGE 1 is the concept of hazard analysis. Hazard analysis begins in the earliest phases of a project, starting as soon as elements of a conceptual design exist. Hazards must be identified, ranked and mitigated.

Hazard analysis is a critical element of system safety, and is the topic of this specification document for the Large Synoptic Survey Telescope (LSST).

This document also emphasizes the details of LSST project's implementation of the process and our plans for continuing the hazard analysis process through the construction phase of our project.

NOTE: In the interest of brevity in this document we refer to MIL-STD-882D w/CHANGE 1 as the "Standard".

2 Definition of Terms

MIL-STD-882D w/CHANGE 1 Draft establishes careful and precise definitions for 54 terms that it uses. It is sufficient to understand only about six of these to make sense of this summary. While the Standard lists its terms in alphabetical order, we choose to list them in a logical development where the first few, at least, don't require a precise understanding of other definitions to follow.

2.1 System

"The organization of hardware, software, material, facilities, personnel, data, and services needed to perform a designated function within a stated environment with specified results, such as the gathering of specified data, data processing, and delivery to users."

This is a somewhat broader definition of system than any other commonly used by telescope systems engineers, with its greater emphasis on people and process, but it is not far off. This additional emphasis is important for safety-related analyses.

2.2 Lifecycle

"All phases of the system's life, including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal."

In practice for LSST this is being accomplished by defining phases of our life cycle, which include:

- Design and Development (D&D);
- Fabrication (FAB);
- Construction (CONST);
- Integration, Test and Commissioning (IT&C);

- Maintenance (MAINT);
- Operations (OPS).

Since “disposal” of LSST (decommissioning and dismantling the facility) is many decades in the future, if ever, this final part of the life cycle has been intentionally left off in our hazard analysis.

2.3 Mishap

“An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. For the purposes of this document, the term “mishap” includes negative environmental impacts from planned and unplanned events and accidents.”

The important point here is that the analysis we are conducting must take into account three classes of mishaps:

- personnel death, injury or occupational illness;
- damage to or loss of equipment or property;
- damage to the environment.

The Standard does not explicitly consider an event that causes lack of availability of a system (i.e. “downtime”) to be a mishap. For example a high-humidity event that causes water to condense on the primary mirror surface requiring downtime to wash the mirror is not considered a mishap. As inconvenient as the event may be, no one was injured; no equipment was permanently damaged, nor was the environment negatively impacted. Nevertheless events causing process losses still can be included in the analysis without contravening any of the basic principles of the Standard (process safety).

An event that almost causes a mishap is called a “near-mishap” and is still object of reporting (OSHA).

2.4 Hazard

“A condition that if triggered by one or more causal factor(s) can contribute to or result in a mishap.”

The difference between a hazard and a mishap, therefore, is that a hazard represents a potential for a negative event while a mishap is the realization of that event.

There may be hazards associated with the early moments of a power failure if systems have not been designed to fail safely, but once the observatory is in a benign (though non-operational) state with flashlights issued to all, a condition that results in the temporary inability to do physics is not, by this definition, a hazard.

2.5 Risk

“A measure of the potential loss from a given hazard. Risk is a combined expression of the severity of the mishap and the probability of the causal factor(s).”

The Standard eventually establishes a means of assigning a numerical value to this “expression” allowing a formal ranking of risks.

2.6 System Safety

"The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system lifecycle."

With this definition in place it is possible to understand the meaning of the title of the Standard: *Standard Practice for System Safety. Environment, Safety, and Occupational Health Risk Management Methodology for Systems Engineering.*

3 Identification of Hazards

MIL-STD-882D requires us to: *"Identify hazards through a systematic hazard analysis process that includes system hardware and software, system interfaces, the environment, and the intended use or application. Consider and use mishap data; relevant environmental and occupational health data; user physical characteristics; user knowledge, skills, and abilities; and lessons learned from legacy and similar systems. The hazard identification process shall consider the entire system lifecycle and potential impacts to personnel, infrastructure, defense systems, the public, and the environment. As hazards are identified, they are entered into the hazard tracking system."*

One critical element of this formal process is careful documentation. The LSST project uses a single spreadsheet to contain the identification, the assessment of risk, and mitigation phases. The result appears in Appendix A. We have opted to maintain one of these forms for each of the main subsystems using dedicated worksheets.

3.1 Hazard Number

This is initially a consecutive integer number beginning with 1, but is made unique project wide by pre-pending the form and subsystem code (e.g. M1M3-43). During the course of the process the spreadsheet may be sorted by a different column, but on the initial pass the form will be presented in numerical order by hazard number.

3.2 Machine or Sub-Process

We used this space to precise the process or the location associated with the hazard.

3.3 User

This column is used to indicate the type of personnel that could be involved with this mishap.

3.4 Task Description

This column describes the task during which the mishap could happen.

3.5 Hazard Category

The hazard category is identified by a single word chosen from a general list.

3.6 Hazard

The hazard column is used to specify the class of hazard. Some common examples include:

- pinch hazard;
- collision hazard;
- fall hazard;
- spill hazard.

3.7 Cause or Failure Mode

This column lists the circumstances or conditions that would lead to the mishap.

3.8 Project Phase(s)

As noted above in the definition of lifecycle, we enter one or more of the following phases for each identified hazard:

- Design and Development (D&D)
- Fabrication (FAB)
- Construction (CONST)
- Integration, Test and Commissioning (IT&C)
- Maintenance (MAINT)
- Operations (OPS)

"All" is used when the hazard could happen during construction, integration, maintenance and operations.

3.9 Comments

The Comments column can be used during any part of the process to add additional explanations, to pose questions for additional study, or anything else pertinent to the hazard.

4 Risk Estimation

The quantitative estimation of the risk is made relatively easy by the very specific process and guidelines set out in the Standard. In summary, each risk is ranked based on two criteria: the severity of the problem, and the likelihood.

4.1 Severity

The severity of a mishap is ranked into one of four well defined categories:

1. Catastrophic – Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or loss exceeding $10M.
2. Critical – Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or loss exceeding $1M but less than $10M.
3. Marginal – Could result in one or more of the following: injury or occupational illness resulting in 10 or more lost work days, reversible moderate environmental impact, or loss exceeding $100K but less than $1M.

4. Negligible – Could result in one or more of the following: injury or illness resulting in less than 10 lost work days, minimal environmental impact, or loss less than $100K.

The explanation included with each category takes much of the potential subjectivity out of the analysis, which is one of the great strengths. Once the hazard is understood it takes little or no discussion to decide what rank it deserves. The amount of monetary losses permissible for each level of severity must be adjusted to the size of the system and actual financial impact, and constantly updated to reflect current replacement or indemnification costs, and changing economic environment.

4.2 Probability

Similar detailed criteria are provided for six measures of the probability of a mishap:

A. Frequent – Likely to occur often in the life of an item; with a probability of occurrence greater than 10^{-1} in that life.
B. Probable – Will occur several times in the life of an item; with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.
C. Occasional – Likely to occur sometime in the life of an item; with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.
D. Remote – Unlikely, but possible to occur in the life of an item; with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.
E. Improbable – So unlikely, it can be assumed occurrence may not be experienced in the life of an item; with a probability of occurrence of less than 10^{-6} in that life.
F. Eliminated – Incapable of occurrence in the life of an item. This category is used when potential hazards are identified and later eliminated.

NOTES:

I. Use either the quantitative or qualitative descriptions of probability, as appropriate, for a given analysis.
II. Use either the individual item or fleet inventory description, depending on which description produces the more frequent probability level for a given analysis.
III. Probability level F is reserved for cases where the causal factor is either no longer present or it is impossible to lead to the mishap. No amount of doctrine, training, warning, caution, personal protective equipment (PPE), or other change can move a mishap probability to level F.
IV. The probability of occurrence may have to be adapted to what's acceptable, tolerable or legally mandated for a given system.

Once again, if the hazard is well understood and rankings are established by a group having experience with the environment and materials with which we work, there will be quick consensus about what ranking a hazard should be given.

Once severity and probability rankings are established for a hazard, three more columns of the hazard analysis form can be completed. These are risk index, and risk level. These are discussed in the following sections.

4.3 Risk Level

The last step in preliminary risk estimation is to make one more classification: the risk level. There are five categories specified in the Standard. The Standard does not give guidance as to what hazard categories rise to a level that must be addressed, and which are low enough to be neglected. This bears on the question of a given project's tolerance for risk, which greatly varies between systems and industries.

The Standard includes a risk assessment matrix (table III) that formally combines severity and probability to yield a single risk level, which is reproduced below.

Risk Assessment Matrix		Severity			
		Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Probability	Frequent (A)	High	High	Serious	Medium
	Probable (B)	High	High	Serious	Medium
	Occasional (C)	High	Serious	Medium	Low
	Remote (D)	Serious	Medium	Medium	Low
	Improbable (E)	Medium	Medium	Medium	Low
	Eliminated (F)	Eliminated			

Figure 1: Risk Assessment Matrix

In past versions of the Standard a numerical value was assigned to each combination of severity and probability, yielding 20 possible "risk indexes" organized as 1 = highest risk, 20 = lowest risk. Consequently the new probability level "eliminated" would have a risk index of 21. This is still useful as intermediate step in preparing automated spreadsheets.

4.4 Software Contribution to System Risk

The draft version of the revised Standard also contains a separate table for software safety criticality matrix based on software contribution to system risk.

Although it is similar in appearance to the Risk Assessment Matrix (Figure 1), the Software Criticality Matrix is not an assessment of risk. The level of rigor (LOR) associated with each software criticality index (SwCI) is the minimum set of verification activities required to be performed on the identified software.

Software Safety Criticality Matrix		Severity Level			
		Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Software Control Category	1	SwCI1	SwCI1	SwCI3	SwCI4
	2	SwCI1	SwCI2	SwCI3	SwCI4
	3	SwCI2	SwCI3	SwCI4	SwCI4
	4	SwCI3	SwCI4	SwCI4	SwCI4
	5	SwCI5	SwCI5	SwCI5	SwCI5

Figure 2: Software Safety Criticality Matrix

5 Risk Mitigation

The last step in the hazard analysis is to consider mitigation and the recommended actions to address mitigation are entered into the column labeled “Risk Mitigation” on the Hazard Analysis form. The standard establishes four broad categories of mitigation:

- change the design or select design options that eliminate the hazard;
- incorporate safety devices (railings, guards, safety controllers, etc.);
- provide warning devices;
- develop procedures and training.

We use this column to give a detailed description of the mitigation action.

6 The Analysis Process

6.1 Hazard Analysis Meetings

The primary means for making progress with the hazard analysis is based on a regular meeting. Each meeting is dedicated to a specific area, subsystem or process. The meetings last for approximately one hour which was found to be as long as the group could maintain focus before becoming distracted by other concerns.

6.2 Personnel Roles

The number of attendees is four people in average. This core group consists of:

- the systems engineer;

- the lead engineer (or architect) for the item being analyzed;
- the electronics/controls engineer;
- the NOAO risk manager.

6.2.1 Systems Engineer

For the LSST project the systems engineer has taken the lead role in hazard analysis. His responsibilities have included the following:

- schedule hazard analysis meetings;
- determine attendees;
- preside and serve as facilitator during the meetings;
- fill in the columns of the of the hazard analysis form as work proceeds;
- terminate the meeting at the appropriate time;
- report progress to non-attendees via the project's weekly reports.

6.2.2 Lead Engineer

The lead engineer typically brings drawings (hard copies) of the assembly under analysis and takes the lead in walking through the subsystems. It is essential that some sort of systematic approach be taken to the problem so that important elements are not forgotten or neglected.

The lead engineer also has the best understanding of anticipated activities during all relevant phases of work on the assemblies. We found it useful, in architectural parlance, to "get small" and imagine working with and/or around the equipment in question.

6.2.3 Electronics/Controls Engineer

The electronics/controls engineer is present at all meetings because of his responsibility for designing the safety interlock system (SIS).

6.2.4 NOAO Risk Manager

The NOAO risk manager participates in these meetings because of his familiarity with hazard safety issues.

7 Bibliography

Department Of Defense. *Standard Practice for System Safety.* MIL-STD-882D, 10 February 2000.

Department Of Defense. *Standard Practice for System Safety. Environment, Safety, and Occupational Health Risk Management Methodology for Systems Engineering.* MIL-STD-882D w/CHANGE 1. Draft Dated 29 March 2010.

Ericson, Clifton A. II. *Hazard Analysis Techniques for System Safety.* Hoboken, New Jersey: John Wiley and Sons, 2005.

Appendix A – LSST Hazard Analysis Form

ITEM ID	MACHINE OR SUB-PROCESS	USER	TASK DESCRIPTION	HAZARD CATEGORY	HAZARD	CAUSE OR FAILURE MODE	PROJECT PHASE	Prior to Safeguard Selection				RISK MITIGATION
								SEVERITY	PROBABILITY	RISK INDEX	RISK LEVEL	
								Four Levels	Six Levels	1 to 21	Five Levels	
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												