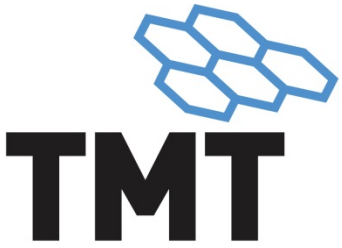

THIRTY METER TELESCOPE

ENVIRONMENTAL, SAFETY AND HEALTH PROCESS GUIDELINES

TMT.PMO.MGT.12.009.REL01

2012-03-20

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

1.1 INTRODUCTION

This document provides guidelines to the Thirty Meter Telescope (TMT) Environmental, Safety, and Health (ES&H) processes that are required for the entire TMT project. The processes described here are intended to:

- assure ES&H protection for personnel and equipment throughout all life cycle phases of TMT activities; including design, construction and fabrication, installation, commissioning and operations
- provide TMT Management with insight into all ES&H assessments and decisions for all facilities, interfaces, services, procedures and systems within the TMT Observatory
- enable the TMT Project manager to certify that all aspects of the TMT Observatory are safe for operations.

1.2 PURPOSE

The objective of this document is to define courses of action for reducing potential hazards to acceptable levels for all TMT services, procedures and systems. This process includes identification, assessment, mitigation, and reassessment of potential hazards. An important element of the process is to regularly communicate the results of the ES&H process so that the TMT Project Office understands potential hazards and the proposed methods for controlling them to acceptable levels. The ES&H Officer within the TMT Project Office is responsible to approve all hazard controls and to ensure that all services, procedures and systems integrate safely into the overall TMT Project.

1.3 SCOPE

This document applies to all elements within the TMT Work Breakdown Structure as described in RD05. It is intended to be used by TMT Project Office personnel, TMT partners, and suppliers of services and systems that influence the TMT Observatory Environmental Safety and Health.

Supplier organizations that have existing processes for managing ES&H protection may use their internal processes. If this option is chosen, the supplier must demonstrate that their internal ES&H process is equivalent to the process described in this document. The TMT project office must agree that the supplier internal process may be used in the place of this one.

Since ES&H protection for software requires additional guidance, it is provided in the document:

TMT Guidelines for Software Safety (RD01)

1.4 CHANGE RECORD

Revision	Date	Section	Modifications
DRF01	2012-03-09	All	Initial draft

1.5 REFERENCE DOCUMENTS

Reference documents contain information complementing, explaining, detailing, or otherwise supporting the information included in the current document.

RD01 TMT Guidelines for Software Safety, TMT.SFT.TEC.11.022

RD02 Standard Practice for System Safety, MIL-STD-882D

RD03 TMT Guidelines for Failure Mode, Effects and Criticality Analysis, TMT.XXX.XXX.XX.XX

RD04 Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL-STD-1929A

RD05 TMT Work Breakdown Structure Report, TMT.BUS.SPE.05.003.REL07

RD06 TMT Structural Design Safety Guidelines, TMT.XXX.XXX.XX.XXX

1.6 SAFETY STANDARDS

The standards documents below describe safety, design and workmanship standards for many types of systems. The ES&H Plan prepared by each TMT group, TMT partner or supplier shall incorporate the standards that are applicable to the work to be performed. All the standards are not applicable to each situation.

If desired, comparable alternate standards may be proposed by a supplier. If this option is selected, the supplier has the responsibility to demonstrate that the proposed standards are equal to or better than those listed below. TMT Project Office must approve the replacement of the standards listed below with alternate proposed standards.

USA Federal Law (required on Mauna Kea):

SD1 Occupational Safety and Health Administration Standards: OSHA 1910

SD2 Title 49, Code of Federal Regulations, Transportation: 49 CFR

Standards/Requirements:

SD3 U.S. Department of Energy Handbook on Electrical Safety, draft for R&D: DOE-HDBK-1092-2009

SD4 Functional Safety – Safety-Related Systems: IEC 61508

SD5 Metallic Materials and Elements for Aerospace Vehicle Structures: metallic material definitions, formulas, principles, failures, properties, metallurgical joints, and analysis procedures: MIL-HDBK-5J

SD6 Design Criteria for Controlling Stress Corrosion Cracking: MSFC-SPEC-522B

SD7 Handbook for Corrosion Prevention and Deterioration Control in Electronic Components and Assemblies: MIL-STD-1250A

SD8 Fasteners – General Requirements for bolts, screws, studs, and nuts: ISO 8992:1986

SD9 Standard Specification for Annular Ball Bearings for Instruments and Precision Rotation Components: ASTM F2332-06

SD10 Lift Sling Design: 540-PG-8719.1.1-A

SD11 Standard Practice for Performance Testing of Shipping Containers and Systems: ASTM D 4169

SD12 Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems: MIL-STD-1522A

SD13 NFPA-75 – Fire Protection for Essential Electronic Equipment

SD14 National Fire Protection Association (NFPA) – Fire Codes and Handbook of Fire Protection

SD15 ANSI Z136.1 – Safe Use of Lasers

SD16 International Building Code: National and Regionally applicable documents for facilities, i.e. Seismic, Environmental, etc.

SD17 Accident Prevention Manual for Industrial Operations

SD18 Toxic Substances Control Act (TSCA)

SD19 TMT Seismic Hazard Analysis (TMT.STR.TEC.10.001.REL01)

1.7 ACRONYMS

AIV Assembly, Integration and Verification
DOD Department of Defense
DOT Department of Transportation
EPA Environmental Protection Agency
ES&H Environmental, Safety and Health
HA Hazard Analysis
HL Hazard List
HRI Hazard Risk Index
OSHA Occupational Safety and Health Administration
OSS Observatory Safety System
PPE Personnel Protective Equipment
RAC Risk Approval Code
SC Safety-Critical
SDR System Design Review
SHA System Hazard Analysis
SHRI Software Hazard Risk Index
SRR System Requirements Review
SSHA Software Subsystem Hazard Analysis
TMT Thirty Meter Telescope or TMT Project

1.8 DEFINITIONS

The terms below are defined as follows within this document:

Condition: An existing or potential state such as exposure to harm, toxicity, energy source, activity, environmental impact, etc.

ES&H critical computer software components: Those computer software components whose errors can result in potential hazards, or loss of predictability or control of a system.

ES&H Program: A program that ensures environmental, safety and health protection by identifying hazards, assessing the severity and probability of the hazards, formulating the best approaches to eliminate or mitigate the hazards and implementing the selected approaches in the final system through commissioning and into operations.

ES&H Safety: The application of engineering and management principles and criteria, with processes and techniques to assess and optimize all aspects of environmental, safety and health protection, within the constraints of operational effectiveness, time and cost throughout all phases of the TMT system life cycle.

ES&H Plan: A description of the planned tasks and activities to be used to implement the required ES&H safety program. This description includes organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other engineering and management activities and related systems.

Fail safe: A design feature that ensures that a system remains safe or, in the event of a failure, will cause the system to revert to a state which will not cause a mishap or hazardous condition.

Fault: Any change in the state of an item which is considered anomalous and may warrant some type of corrective action. A fault may or may not lead to a failure.

Fault tolerance: The ability of a system to withstand an unwanted event and maintain a safe and operational condition. It is determined by the number of faults that can occur in a system without the occurrence of a failure. A system with a fault tolerance of 2 can withstand two faults before failure.

Failure: The inability of services, procedures and systems to perform required functions within specified performance requirements. All failures are the result of one or more faults.

Hazard: A condition that poses a threat of injury or damage to life, health, equipment, or the environment. Each hazard has at least one cause, which in turn can lead to a number of effects (e.g., damage, illness, failure).

Hazard cause: A defect in hardware or software, a human operator error, an interface error or an unexpected input or event which results in a hazard.

Hazard control: A method for preventing the hazard, reducing the likelihood of occurrence of the hazard, or the reducing of the impact of that hazard. Hazard controls use hardware (e.g. add a pressure relief valve), software (e.g. detect a stuck valve condition and automatically respond by opening a secondary valve), operator procedures, or a combination of methods to avert the hazard.

Hazard probability: The aggregate probability of occurrence of the individual conditions that create a specific hazard.

Hazard Risk: An expression of the possibility and impact of a mishap in terms of hazard severity and hazard probability

Hazard Risk Assessment: A comprehensive evaluation of a service, procedure or system to determine possible hazards, their probability of occurrence, and the possible severity of each hazard

Hazard severity: An assessment of the consequences of the worst credible mishap that could be caused by a specific hazard.

Hazardous Material: Anything that, due to its chemical, physical, or biological nature, can cause a hazardous condition so that it requires special efforts to manage, handle or eliminate it.

Mishap: An unplanned accident, event or series of events resulting in a hazardous condition that causes death, injury, occupational illness, damage to or loss of equipment or property, damage to the environment, or loss of proper function so that observatory operating time is lost.

Safety (ES&H): Freedom from those conditions that can cause hazards.

Safety-critical: A term applied to any condition, event, operation, software, process or item where proper recognition, control, performance or tolerance is essential to protect environment, safety and health.

Subsystem: An element of a system that, in itself, may consist of many components such that it constitutes a system. For the purposes of this document, subsystems will be called systems.

Supplier: An organization engaged either through contracts or partnership arrangements to provide services or products for TMT.

System: A composite, at any level of complexity, of materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose and to meet defined requirements.

2. REQUIRED ES&H PROCESSES

2.1 ESTABLISHING A PLAN FOR ES&H PROCESSES

TMT groups, TMT partners and suppliers who will perform work at the TMT summit facility, deliver systems to the summit facility, or perform work as part of the construction of the TMT base facility in Hawai'i must develop and submit their ES&H plan for review and approval . The ES&H plan should be consistent with existing practices and policies of the supplying organization as much as possible. The TMT ES&H Officer will confirm that the ES&H plan conforms to this document.

If further description is desired beyond what is provided here, Appendix A of RD02 provides a detailed description for establishing a safety plan similar to what is required by TMT.

The ES&H Plan shall:

- Follow the guidelines in this document
- Provide a schedule of the tasks for each phase of the ES&H activities
- Be submitted to the TMT ES&H Officer for approval
- Include training for personnel who are working on TMT so that TMT ES&H Plan requirements are understood and implemented
- Manage the ES&H effort and resources to align them with the magnitude of the perceived hazard risks so that hazard control cost and complexity is minimized
- Create an ES&H team that will perform ES&H evaluation
    - The team should consist of personnel from the supplier organization who are working on the item to be delivered. It is important that the team is familiar with the details. The team should include representatives from the disciplines that are involved in providing the service, procedure or system since each discipline will bring a unique perspective to the process that will be required to uncover hazards. The objective is for the team to identify potential hazards as fully and as early in the design process as possible.
- Establish and maintain an effective procedure for reporting and communicating ES&H activities to the TMT Project Office
- Implement procedures for ES&H Hazard Analysis, Hazard Risk Assessment, and Hazard Control during all phases of the project based on the guidelines within this document. New results will be uncovered as the project matures from concept to implementation.
- Maintain a TMT Hazard/Risk Assessment Worksheet and provide it for review as the development of the work proceeds through its lifecycle phases
- Require reporting of any mishaps that occur during the process of development, fabrication, assembly, test, packaging, and shipping
- Require an application for a TMT safe work permit prior to delivery of services, procedures or systems to a TMT facility

The ES&H plan shall include but not be limited to the following items:

- Assignment of who will oversee and manage the ES&H activities
- A schedule for the ES&H training
- A schedule of the ES&H meetings including the intended purpose of the meetings
- The list of the engineering team members who will be on the ES&H team

2.1.1 Training

Maintaining an effective ES&H Plan will require the involvement of the personnel who influence the development of services, procedures and systems for TMT. It is important that each person understands the TMT philosophy and requirements for ES&H protection.

The goal for safe TMT ES&H protection is to produce an inherently safe product that will have the minimum safety-imposed operational restrictions because of wise design choices. This is best achieved through involvement of all engineering personnel in assessing ES&H issues early in the development process and at every subsequent stage through commissioning at TMT Facilities. Unless all personnel are familiar with programs of this sort, early training of all personnel will be necessary to optimize the team's ability to meet the TMT goal.

The TMT Observatory site on Mauna Kea presents an environment that is challenging for ES&H protection on several levels. Due to the high altitude, oxygen deprivation is a factor for workers at the TMT summit facility. All personnel who will be working at the observatory need to be trained to recognize oxygen-deprivation symptoms within themselves and others and to seek aid immediately. In addition, oxygen-deprivation tends to cause confusion and forgetfulness and to inhibit clear reasoning. Because of this, planning long, complex activities at the summit should be avoided where possible. Hardware design choices should be made to enable short and straightforward procedures, with check-list-style instructions for installation, commissioning, and maintenance.

Several additional factors need to be remembered when planning activities at the TMT summit facility:

- The telescope temperature will be cold. The telescope temperature is maintained as close as possible at the expected night-time temperature. All activities on the telescope will be in cold temperatures and warm, protective gear will be required.

- In addition, the environment at the summit is sacred to Hawaiian people and must be protected. All expendables at the summit must be collected and carried down the mountain for disposal. All personnel working at the summit are expected to be sensitive of the privilege granted to TMT when permission was given for location on Mauna Kea, to be respectful of local customs and protect the environment.

During all phases of the development, engineers must understand the TMT safety requirements so that compliance can be designed in. The safety standards that are applicable to the services, procedures and systems must be understood by the developing team. Some of the topics include:

- Structural factors-of-safety (guidelines are provided in RD06)
- Safety features built into the design (i.e., fail-safe, pressure relief mechanisms, emergency disconnects, fall protection, captive hardware, etc.)
- Seismic design considerations including historical data (local area) and probability assessments as defined in SD19
- Laser safety as defined in SD15
- Safe design, handling and operation of pressurized vessels, vacuum systems, and cryogenics per SD12

- Safe use and disposal of hazardous materials per SD18
- Electrostatic discharge safety requirements per SD3
- Confined space/limited access/egress work areas per SD1
- Fall protection per SD1
- Safe work in high altitude (protection from UV, hyperventilation, hypothermia, fluid loss, increased heart rate, etc.)
- Design, installation and safe use of cranes and man-lifts per SD1 and SD10
- Design and installation requirements for scaffolding and construction temporary support structures per SD1
- Design of high voltage electrical equipment to prevent threat of shock per SD3
- Inclusion of interlocks and lock-outs in the design (mechanical, electrical and software as appropriate) to prevent hazardous conditions
- Use of approved "Warning" (personnel safety) and "Caution" (hardware safety) placards and safety instructions per SD1 and SD15
- General workmanship and design considerations such as elimination of sharp edges during manufacture, and chamfering or rounding sharp corners
- Design to preclude any pinch or crush hazards

This is not a complete list.

Finally, training must cover the process of ES&H evaluation, documentation and reporting that is covered in the sections below.

2.2 ES&H EVALUATION

This section describes the steps required for the ES&H evaluation. This process must be followed during each project phase of development or design, fabrication, testing, integration and operation as applicable and must be reported at each TMT review at the end of each phase.

2.2.1 Failure Mode, Effects and Criticality Analysis

The Failure Mode, Effects and Criticality Analysis (FMECA) described fully in RD06 will provide a comprehensive list of possible failures. This list will be used to evaluate and improve the safety, reliability, and maintainability of each service or system. Any possible failures that may impact ES&H are classified as hazards and will be evaluated following the ES&H Evaluation process.

2.2.2 Hazard Analysis

Hazard Analysis consists of two activities: 1) developing a list of possible hazards; and 2) classifying each hazard into safety-critical categories as described below.

2.2.2.1 List of possible hazards

The FMECA list will not uncover all the hazards since it evaluates the intended functions of a system and does not consider unintended situations. Hazards are created when personnel interface with hardware, both operationally and during maintenance. The ES&H list of possible hazards shall include those from the FMECA and additional hazards that involve unplanned activities, especially those that include interaction of personnel. Developing the full list of possible hazards requires

brainstorming sessions of the ES&H team. Hazards may be caused by personnel error; environmental conditions; design inadequacy; procedural deficiency; interface incompatibility; system or component failure or malfunction; any combination causes or any other possible cause. The team must consider all possible incidents, failures and combinations that might occur in the services, procedures and systems and their effect on ES&H protection and observatory operations. The list should include all hazards associated with current and future activities including; design, fabrication, assembly, testing, handling, transportation, integration at the observatory, observatory operations, and observatory maintenance; where applicable.

At this stage, the focus should be on collecting a list of all potential hazards – not on whether the hazards would actually occur. The probability of occurrence will be addressed in a later step and it is better to assume that incidents or failures could occur so that consequences can be examined. All hazards should be listed along with the phase during which the hazard might occur; the conditions (failures or incidences) that created the hazard; and the consequences of each hazard. This information will be required in the Hazard/Risk Analysis Worksheet.

Hazard Analysis should be performed during each phase of development starting with conceptual design phase and proceeding through final acceptance reviews. It is expected that hazards that are identified during early phases will be eliminated or mitigated by design. Later phase hazard analysis will include hazards that are uncovered as the design details are implemented and tested. The final hazard analyses will identify operational constraints that must be applied to ensure safe use of the services, procedures and systems.

Situations that threaten ES&H protection for personnel and equipment are classified safety-critical (SC). In particular, hardware and software having the Safety-Critical characteristics described in Table 1 will require special attention to ensure related hazards are identified.

Table 1. TMT Characteristics of Safety-Critical Hardware and Software

Hazard Classification	Characteristics
Safety-critical	• Causes or contributes to ES&H risks. • Provides control or mitigation of ES&H risks. • Controls safety-critical functions. • Processes or transports safety-critical commands or data. • Detects, reports, and/or takes corrective action, if the system reaches a specific hazardous state. • Mitigates damage if an ES&H risk occurs. • Software that resides on the same system (processor) as safety-critical software.

2.2.3 Hazard Risk Assessment

The Hazard Risk Assessment process takes place in three steps as described below.

2.2.3.1 Hazard Severity Classification

The first step of Hazard Risk Assessment is to determine the severity of each hazard that has been identified. Severity classifications provide a method of quantifying the worst potential consequence resulting from each Hazard. Table 2 provides the Hazard Severity Categories for SC Hazards.

If it is not clear which category applies to a Hazard, the Evaluation Team should select a category and document the uncertainty and final choice in the Hazard/Risk Analysis Worksheet.

Table 2. Safety-Critical Hazard Severity Categories

SC Hazard Severity	Category	Definition
Catastrophic	**1**	**Death or permanent total disability, system loss, major property damage or severe environmental damage.**
Critical	**2**	**Severe injury, severe occupational illness, major system or environmental damage.**
Marginal	**3**	**Minor injury, lost workday accident, minor occupational illness, or minor system or environmental damage.**
Minor or Negligible	**4**	**Less than minor injury, first aid or minor supportive medical treatment type of occupational illness, or less than minor system or environmental damage.**

2.2.3.2 Determine Hazard Probabilities

The probability of occurrence must be evaluated for each hazard. The time frame for the evaluation is the planned life expectancy of the services, procedures and systems. The probabilities can be determined by testing, research, analysis, and evaluation of historical data from similar systems. Reliability data can also provide guidance for determining probabilities. Substantiation of the Hazard probability of occurrence will be a focus during the ES&H portion of project reviews. For the ES&H Analysis, the probabilities are categorized to enable the next process step. The categories for SC Hazards are shown in Table 3.

Table 3. Safety-Critical Hazard Probability of Occurrence Categories

SC Probability	Category	Description
Frequent	A	Likely to occur frequently or continuously experienced.
Probable	B	Will occur several times in the life of an item.
Occasional	C	Likely to occur during the life of an item.
Remote	D	Unlikely, but possible to occur in the life of an item.
Improbable	E	Possible, but so unlikely to occur in the life of an item that it can be assumed to not be experienced.

2.2.3.3 Determining Hazard Risk Index

The categories for severity and probability for each hazard are used to determine a hazard risk index (HRI). The HRI is created by combining the severity category with the probability category in a matrix as shown in Table 4. The colors on matrix indicate the next step in the ES&H process.

Table 4. SC Hazard Risk Index Matrix

SC Hazard Risk Index		SC HAZARD SEVERITY CATEGORY			
		1 Catastrophic	2 Critical	3 Marginal	4 Negligible
SC HAZARD PROBABILITY OF OCCURRENCE CATEGORY	A Frequent	1A	2A	3A	4A
	B Probable	1B	2B	3B	4B
	C Occasional	1C	2C	3C	4C
	D Remote	1D	2D	3D	4D
	E Improbable	1E	2E	3E	4E

2.2.3.4 Assign a Hazard Risk Approval Code (HRAC)

Based upon the HRI, a Hazard Risk Approval Code (HRAC) is assigned that classifies the acceptability level for each hazard. The RAC also indicates the required level of involvement of TMT Project Management for acceptance. Table 5 shows the HRAC and TMT Project Management involvement requirements applied to HRIs for SC Hazards.

Table 5. TMT Hazard Risk Approval Level

Hazard Risk Index (HRI)	Hazard Risk Approval Code	Level of TMT Project Management Required
1A, 1B, 1C, 2A, 2B, 3A	Unacceptable – Hazard Risk must be mitigated further	Hazard Risk not accepted
1D, 2C, 2D, 3B, 3C	Undesirable – Further review, testing, and analysis are required to determine if Hazard Risk is acceptable	Review and Decision required
1E, 2E, 3D, 3E, 4A, 4B	Moderate – Hazard Risk must be reviewed prior to acceptance	Review required
4C, 4D, 4E	Low – Hazard Risk is acceptable without review	none

2.2.4 Hazard Control

The next step is for the ES&H team to perform hazard control engineering. All hazards without acceptable RAC codes must undergo evaluation to consider methods to eliminate or reduce the hazard. TMT hazard control practices will be governed by an order of precedence as follows:

1. Design for Minimum Hazard Risk: The primary means for mitigation of hazard/risk shall be to eliminate the hazard through design.

2. Incorporate ES&H devices: Fixed automatic or other protective devices shall be used in conjunction with the design features to attain an acceptable level of hazard/risk. The use of redundant protective devices may be required in some situations where an unacceptable hazard/risk could occur if a protective device were to fail. Provisions shall be made for periodic functional verification checks as applicable.

3. Provide Warning Devices: When neither design nor ES&H protective devices can effectively eliminate or reduce hazards, devices shall be used to detect the condition, and to produce an adequate warning to alert personnel of a hazard. Devices may include audible or visual alarms, permanent signs, or movable placards.

4. Procedures and Training: Where it is impractical to substantially eliminate or reduce the hazard or where the condition of the hazard indicates additional emphasis, special operating procedures and training shall be used.

TMT prefers hardware-based hazard controls for hardware hazards or hardware-based hazard controls in conjunction with software-based hazard controls. This follows from the precedence list above.

In some situations the software control and hardware control cooperate. The software control may be the first line of defense with a hardware-based control as a backup if the software control fails.

Sometimes neither of the solutions described above is feasible and only software-based hazard controls are possible. If a software control is the only control, then the software needs to be implemented and tested carefully. Software-only control of a hazard risk requires TMT approval.

In addition, multiple controls may be necessary to mitigate some hazards.

2.2.5 Mitigated Hazard Risk Assessment

Following the hazard control engineering, the modified hazards will be reanalyzed by undergoing the Hazard Risk Assessment processes listed in Section 2.2.3. This will result in mitigated severity and probability classifications, HRIs and RACs.

2.3 ES&H REQUIRED DOCUMENTATION – SAFETY DATA PACKAGE

At each review, the appropriate documents from the following list shall be gathered into a Safety Data Package that will be presented to the TMT Project Office.

2.3.1 Introduction

The Safety Data Package is required to have a signature page that includes the following signatories: Supplier ES&H Evaluation Team Leader or Leaders, Supplier Manager, TMT Work Package Manager, TMT Group Leader, TMT Project ES&H Safety Officer and TMT Project Manager. At each phase, approval of the Safety Data Package is required before proceeding to the next phase.

Following the signature page, the Safety Data Package shall include a summary page that briefly describes the activities and findings of the ES&H Assessment during the phase under review including the Hazard Risk Approval Codes and hazards that require TMT management review. Any hazards that involve interfaces with other systems should be summarized in this section to ensure the hazard will be communicated appropriately.

2.3.2 ES&H Plan

The ES&H plan, including description of the personnel involved, the schedule, and the implementation shall be provided at each project phase review. The initial presentation will describe the suppliers plan and subsequent presentations will focus on reporting status against the schedule and cost along with any changes that have occurred in the plan.

2.3.3 TMT Hazard/Risk Assessment Worksheet

The ES&H Evaluation process described in Sections 2.2.1, 2.2.2, 2.2.3 and 2.2.5 are to be documented in a TMT Hazard/Risk Assessment Worksheet. A sample of the spreadsheet is shown in Appendix A. This spreadsheet will be provided to the TMT Project Office and updated and presented at reviews.

The headings of the TMT Hazard/Risk Assessment Worksheet are as follows:

- ID – Unique identifier formatted as SYS-HAZ01 etc. where SYS represents the appropriate Work Breakdown Structure subsystem abbreviation from RD05
- Item – Description of the services, procedures, systems or component that is involved in creating the hazardous condition
- Project Phase – The phase when the hazard could occur: design; fabrication; assembly; integration and test; or operations (more than one phase may be applicable)
- Hazard Description – Brief description of the hazard including details of functions or activities being performed and any conditions that contribute to the hazard (e.g. failures, system state)
- Hazard Cause – Description of the cause of the hazard
- Effects – Description of whether personnel injury or what equipment may be damaged or what loss of operations may occur
- Severity Category – The Hazard Severity Category 1, 2, 3 or 4 (defined in Section 2.2.3.1) prior to any hazard control actions
- Probability Category – The Hazard Probability Category A, B, C, D or E (defined in Section 2.2.3.2) prior to any hazard control actions
- Hazard Risk Index – Consists of the Severity Category and the Probability Category
- Hazard Risk Approval Code (HRAC) – UN – unacceptable, UD – undesirable, MO – moderate, and LO – low as described in Section 2.2.3.4
- Hazard Control – Describe the action necessary to eliminate or improve the RAC of the hazard as described in Section 2.2.4: e.g. design change, addition of requirement, addition of interlock in OSS, operational procedure, audible/visual warning etc. If the hazard requires multiple controls, each control must be described, but all controls will contribute to the mitigated assessment levels.

- Mitigation Comments – Detailed description of how the hazard will be reduced or mitigated
- Mitigated Severity Category – Hazard Severity Category after Hazard Control actions
- Mitigated Probability – Hazard Probability Category after Hazard Control actions
- Mitigated Hazard Risk Index – Consists of the Mitigated Severity Category and the Mitigated Probability Category
- Mitigated HRAC – Hazard Risk Approval Code after Hazard Control actions
- Hazard /Risk Mitigation Verification – List the method of verifying that the mitigation has the expected results using the following verification codes: DE for design, An for analysis, Te for test, and In for inspection
- Safety Interlock – Flags whether the hazard risk mitigation requires that an interlock be implemented by the observatory safety system

2.3.4 Incident Reports

It is expected that there will be incidents of mishaps, failures or malfunctions during activities prior to delivery. These incidents are very informative because they are examples of occurrences of unplanned events that may create hazards and hazard-like conditions. These incidents must be reported so that the TMT Systems Group can understand and evaluate whether additional systems requirements are needed to avoid repetition. Maintaining a record of all incidents will also aid the TMT operations team by providing a list of lessons learned that will guide mishap avoidance during operations. TMT would like all incidents to be reported using a standard form that can be found in APPENDIX B.

The Incident Reports should be submitted to the TMT Project as quickly as practical following the incident and also should be collected and included in the Safety Data Package for each Project Phase Review.

The sections in this form are:

- Type of Incident: select appropriate choice
- Facility/site location: where the incident occurred
- Reporting employee: person filling out the report (who may answer follow-up questions)
- Date and time of incident
- List persons involved: personnel who were present when the incident occurred, if injury or illness occurred – who was injured or became ill
- Conditions present during the incident: all conditions that may affect the incident: the environment (temperature, humidity, etc.); the functioning state of equipment; the set of commands; etc.
- Describe fully how the incident occurred: what each person was doing, and activities leading to incident

- Describe factors that contributed to the incident: any additional factors that may or may not normally be part of the activity that lead to the incident

- Recommendations to prevent similar incidents from occurring: recommendations of the team involved in the incident

- Signature of reporting employee and date that the incident form was filled out

2.3.5 Safe Work Permit

A Safe Work Permit based on the form in APPENDIX C is required for activities that will occur in TMT facilities including facility construction; assembly, testing, integration and test of systems and components; and commissioning tasks. The Safe Work Permit documents all potential hazard risks associated with the planned work and proposes methods to be used to eliminate or reduce them.

The TMT ES&H Steering Committee must certify that the work may proceed safely prior to beginning the desired activity. In addition, periodic reviews of the TMT Safe Work Permits will be conducted to determine that each hazard/risk was identified and understood and that the appropriate level of effort was exercised to provide acceptable ES&H protection.

The Safe Work Permit should be completed and submitted to the TMT Project ES&H Office as early as possible prior to the expected period of performance of the work so that approval and certification can be obtained.

If the information in a section does not fit on the form, the form shall indicate that the section is attached, and the information shall be included on attached sheets that are labeled with the appropriate section.

The Safe Work Permit Package including the form and all required information listed below shall be submitted to the TMT ES&H Steering Committee in time for approval prior to commencing the activities per the planned schedule.

The sections in the Safe Work Permit Form are described below:

Section 1

- The first section will be filled in by the TMT Project ES&H Steering Committee upon approval and certification that the requested work can commence.

Section 2

- The second section contains the work location, the performing organization, the name and signature of the responsible manager of the performing organization, the expected period of performance of the work and a summary of the work description.

- A list of required attachments is provided at the end of the section. The attached documents will justify that the ES&H hazards are understood and controlled, precautions are determined and in place, and will include a copy of the up-to-date TMT Hazard /Risk Assessment Worksheet for the proposed work.

Section 3

This section lists required precautions that must be verified for activities that take place in TMT facilities. It is expected that the work performing organization will coordinate with the TMT facility to understand facilities that are available to support the work and what the performing organization will need to prepare for and to supply.

- Emergency procedures that inform the work force what to do in case of emergencies.

- Emergency contacts: names and phone numbers – more than one person is required.

- All required emergency equipment has been obtained and the location on the work site has been determined and communicated to work crew.

- Maps and driving instructions so all work crew personnel understand how to arrive at the work site.

- A complete list of all hazard precautions that must be understood in order for the work to proceed safely.

- All inherent hazards in the work area are identified and controlled.

- A buddy system plan is in place for all work activities.

- Safety monitor personnel are arranged appropriately for the size of the work task.

- Certifications have been obtained for activities that require them such as: make & break electrical connections, crane operation.

- Most of the activities at TMT facilities will require two-way communication equipment that must be arranged.

- Personnel Protective Equipment (PPE) that will be required during the planned work must be supplied as appropriate and must have current inspections. Examples of PPE that may be required are:

    - Particulate safety glasses
    - Hardhats
    - Safety shoes
    - Fire extinguishers
    - Supplementary illumination
    - Warning signs
    - Barricades
    - Safety harnesses
    - Lifelines
    - 2-way radios or phones
    - Protective clothing and gloves (Extreme environmental conditions)
    - Ladders / lifts / scaffolds
    - Laser safety glasses
    - Current and volt meters
    - Fire extinguishers

- The work crew must receive training in proper use of all PPE

- A list of observatory facilities and subsystems (such as electricity, fluid cooling, cranes, controls signals and safety systems, etc.) that will be required to perform the work safely must be provided to ensure the facility will be functioning and available.

- All work procedures must be reviewed and approved by the TMT ES&H Office.

- The work crew must receive training for ES&H protection.

Section 4

Many services, procedures and systems will require special precautions to prevent the occurrence of Hazards. These will be identified by the TMT Hazard/Risk Assessment Worksheet. All required precautions that are not already covered must be listed, with the control method described and an indication that the control method has been implemented.

Section 5

Any critical handling and critical lifts that are intended during the work should be listed. Critical handling and critical lifts are defined as any movement of delicate systems from one location to another when damage to the system will impact the TMT schedule or funding resources. The movement may involve manual carrying, the use of rolling carts, lifting with cranes, or movement involving any specialized TMT handling equipment.

3. APPENDICES

APPENDIX A. Sample TMT Hazard/Risk Assessment Worksheet

			HAZARD/RISK						HAZARD/RISK RESOLUTION					
						Hazard Risk Index				Hazard Risk Index				
Hazard ID	Item	Project Phase: Des/Fab/Ass/Int/Op	Description	Cause	Effect	Severity Category: 1/2/3/4	Probability Category: A/B/C/D/E	Hazard Risk Approval Code: UN/UD/MO/LO	Hazard/Risk Mitigation Description	Mitigated Severity Category: 1/2/3/4	Mitigated Probability Category: A/B/C/D/E	Mitigated HRAC: UN/UD/MO/LO	Hazard /Risk Mitigation Verification : De/An/Te/In	Safety Interlock Required (Y/N)

LEGEND	
Symbol	Description
Des	Design Phase
Fab	Fabrication Phase
Ass	Assembly Phase
Int	Integration and Test Phase
Op	Operations Phase
UN	Unacceptable Hazard Risk
UD	Undesirable Hazard Risk
MO	Moderate Hazard Risk
LO	Low Hazard Risk
De	Verification by design
An	Verification by analysis
Te	Verification by test
In	Verification by inspection

APPENDIX B. TMT PROJECT INCIDENT REPORT FORM

TMT Project Incident Report

The original of this report is to be sent to the TMT Work Package Manager and the Supplier ES&H Evaluation Manager

TYPE OF INCIDENT: ____Illness ____ Injury ___ Unsafe Condition ____Property Damage ____Loss of Operating Time ____Other

FACILITY/SITE LOCATION: _____

REPORTING EMPLOYEE: _____
(PRINT) (LAST) (FIRST)

DATE OF INCIDENT: _____ TIME OF INCIDENT: _____

LIST PERSONS INVOLVED: _____

_____

_____

EXPLAIN CONDITIONS PRESENT DURING THE INCIDENT: _____

_____

DESCRIBE FULLY HOW THE INCIDENT OCCURRED:
(STATE WHAT EACH PERSON WAS DOING AND THE CIRCUMSTANCES LEADING TO THE INCIDENT):_____

_____

_____

_____

_____

_____

_____

DESCRIBE FACTORS THAT CONTRIBUTED TO THE INCIDENT: _____

_____

_____

_____

_____

_____

RECOMMENDATIONS TO PREVENT SIMILAR INCIDENTS FROM OCCURRING: _____

_____

_____

_____

_____

SIGNATURE: _____ DATE OF REPORT:_____

APPENDIX C. TMT SAFE WORK PERMIT FORM

TMT PROJECT SAFE WORK PERMIT

SECTION 1: **TMT ES&H STEERING COMMITTEE SECTION: DO NOT FILL IN**

SAFE WORK PERMIT APPROVAL DATE: _____ (YYYY/MM/DD) APPROVED PERIOD OF PERFORMANCE: _____ (YYYY/MM/DD – YYYY/MM/DD)

APPROVING PERSON: _____ _____
PRINT: (LAST) (FIRST) SIGNATURE

SECTION 2: WORK LOCATION: _____ PERFORMING ORGANIZATION: _____

PERFORMING ORGANIZATION MANAGER: _____ _____
PRINT: (LAST) (FIRST) SIGNATURE

PERIOD OF PERFORMANCE: _____ (YYYY/MM/DD – YYYY/MM/DD) SUMMARY WORK DESCRIPTION: _____

_____

_____

_____

NOTE: ATTACH WORK PLANS, LIST OF WORK AREA INHERENT HAZARDS AND CONTROLS, WORK PROCEDURES, PRECAUTIONS AND TMT HAZARD/RISK ASSESSMENT WORKSHEET THAT COVERS THE PROPOSED WORK

SECTION 3. REQUIRED PRECAUTION COMPLIANCE:

NAMES PHONE NUMBERS

EMERGENCY PROCEDURES INCLUDED: (Y/N) ( ) EMERGENCY CONTACTS: _____

EMERGENCY EQUIPMENT DEFINED AND LOCATED: (Y/N) ( ) _____

MAPS & DRIVING INSTRUCTIONS INCLUDED: (Y/N) ( ) TWO-WAY COMMUNICATION ARRANGED (Y/N) ( )

HAZARD PRECAUTION LIST INCLUDED: (Y/N) ( ) PPE – CURRENT INSPECTION: (Y/N) ( )

WORK AREA INHERENT HAZARDS CONTROLLED: (Y/N) ( ) WORK CREW TRAINED TO USE PPE: (Y/N) ( )

BUDDY SYSTEM PLAN IN PLACE: (Y/N) ( ) REQUIRED OBSERVATORY FACILITIES LIST ATTACHED: Y/N ( )

SAFETY MONITOR(S) ARRANGED: (Y/N) ( ) PROCEDURES REVIEWED WITH TMT ES&H OFFICER: (Y/N) ( )

REQUIRED CERTIFICATIONS OBTAINED: (Y/N) ( ) WORK CREW TRAINING FOR ES&H PROTECTION: (Y/N) ( )

SECTION 4. SPECIAL PRECAUTIONS COMPLIANCE: (LIST ALL SPECIAL PRECAUTIONS, CONTROL METHODS AND COMPLIANCE)

SPECIAL PRECAUTIONS	CONTROL METHOD	COMPLIANCE (Y/N)

SECTION 5. LIST OF ALL INTENDED CRITICAL HANDLING OR CRITICAL LIFTS

_____

_____