ATST Hazard Analysis

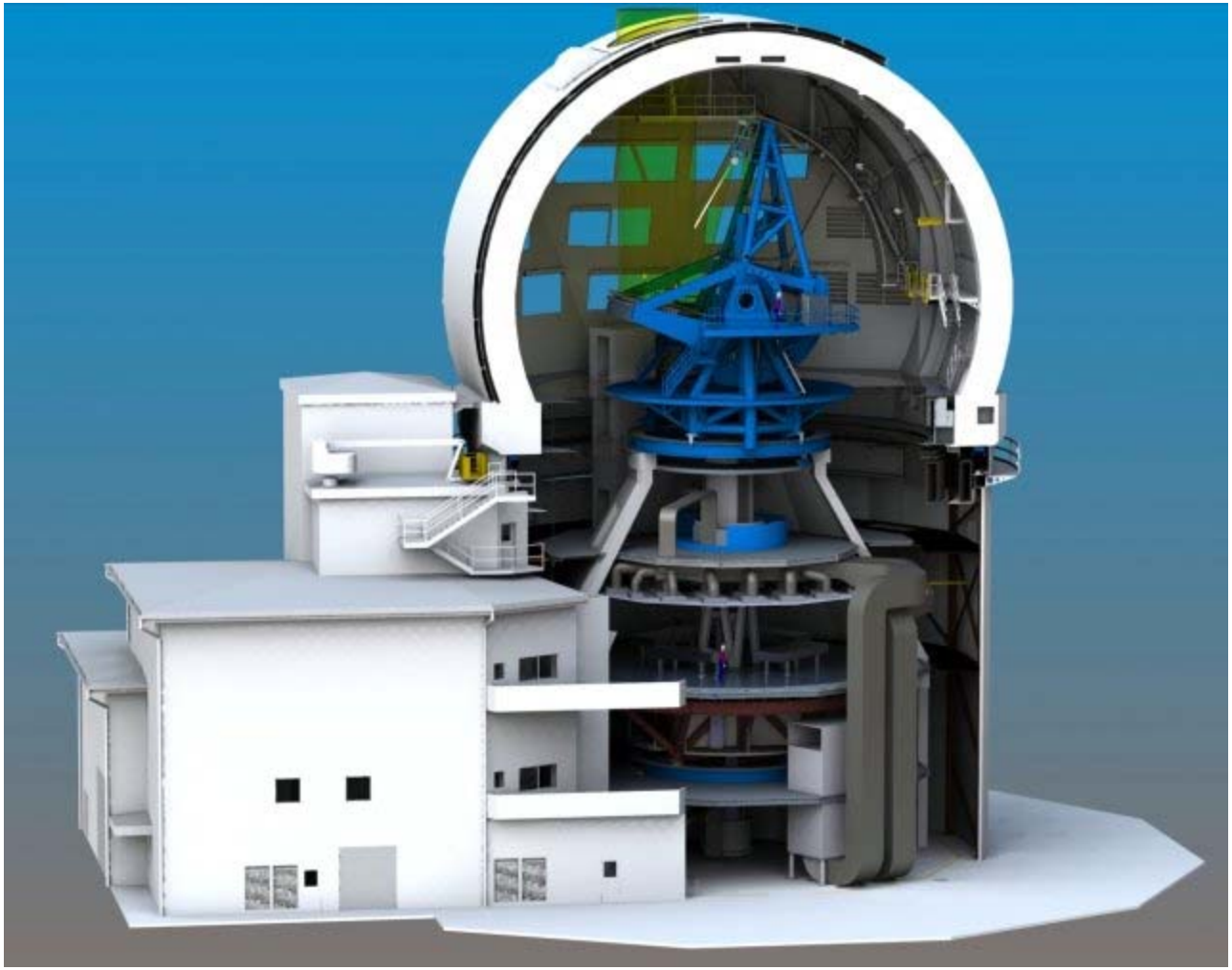
Making Sense of MIL-STD-882D

Rob Hubbard

ATST Systems Engineering

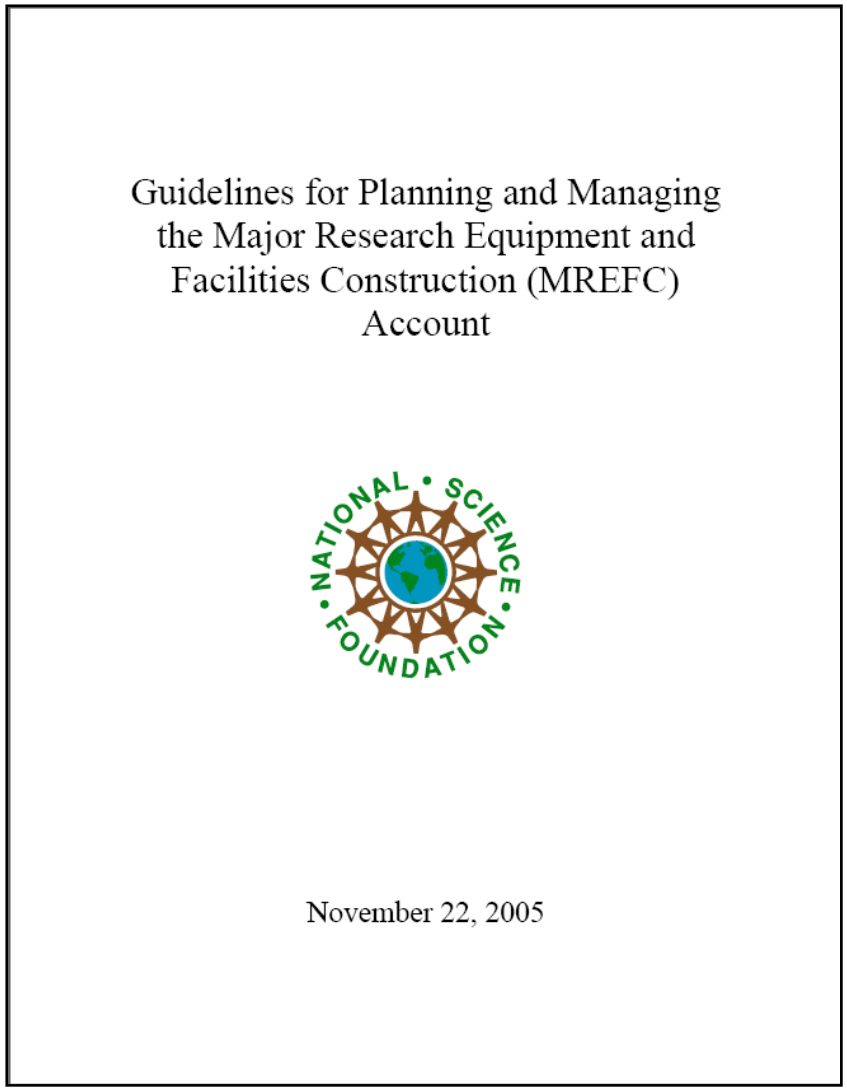
The Advanced Technology Solar Telescope

ATST Cut-away



- Solar telescope
- 4-meter aperture
- Off Axis
- All reflecting
- Diffraction limited images (with high-order adaptive optics)
- Large (16-meter diameter) rotating coudé room.
- Cooled mirrors.
- Cooled enclosure.

MREFC Guidelines

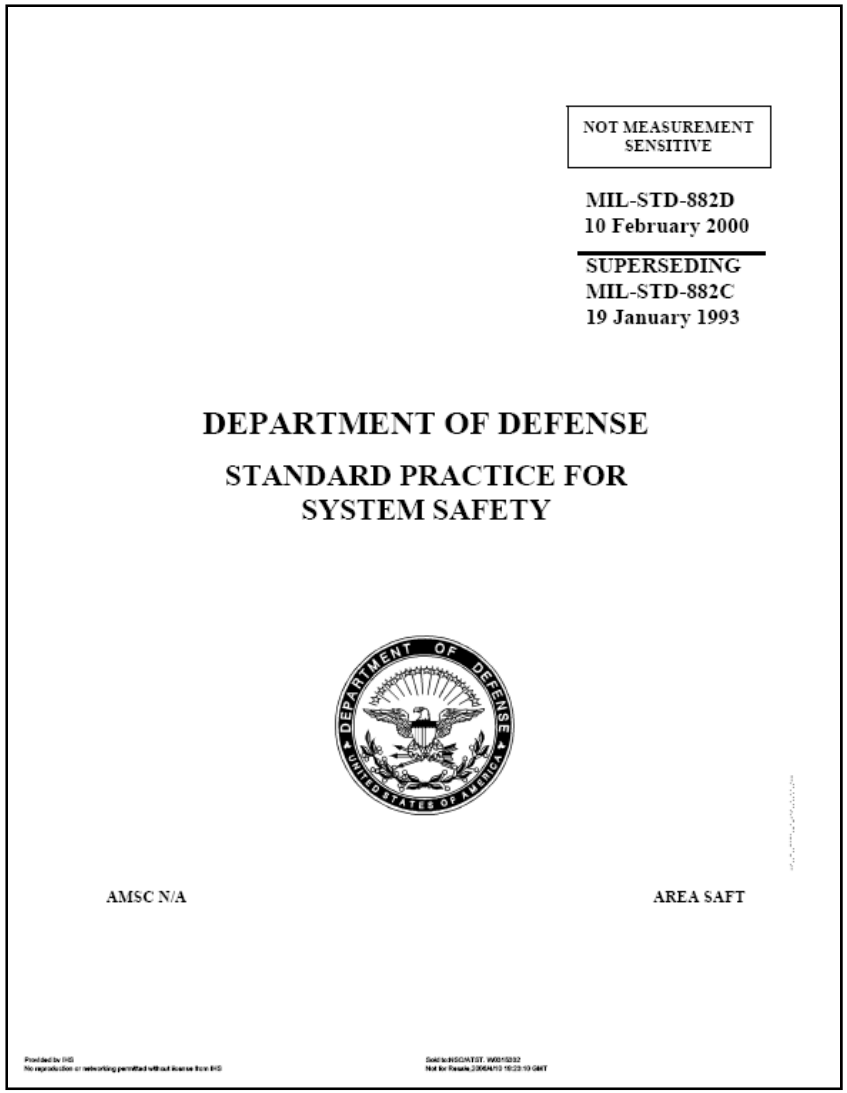

Guidelines for Planning and Managing the Major Research Equipment and Facilities Construction (MREFC) Account

NATIONAL SCIENCE FOUNDATION

November 22, 2005

- Upon exiting the conceptual design phase, the PEP should include an assessment of "Environmental, safety, and health issues that may arise through all project phases."
- By the time of the construction-ready PEP all safety and health issues need to be in a "well defined" state.
- A formal hazard analysis is one aspect of this.
- ATST has adopted MIL-STD-882

MIL-STD-882D



NOT MEASUREMENT SENSITIVE

MIL-STD-882D
10 February 2000

SUPERSEDING
MIL-STD-882C
19 January 1993

DEPARTMENT OF DEFENSE

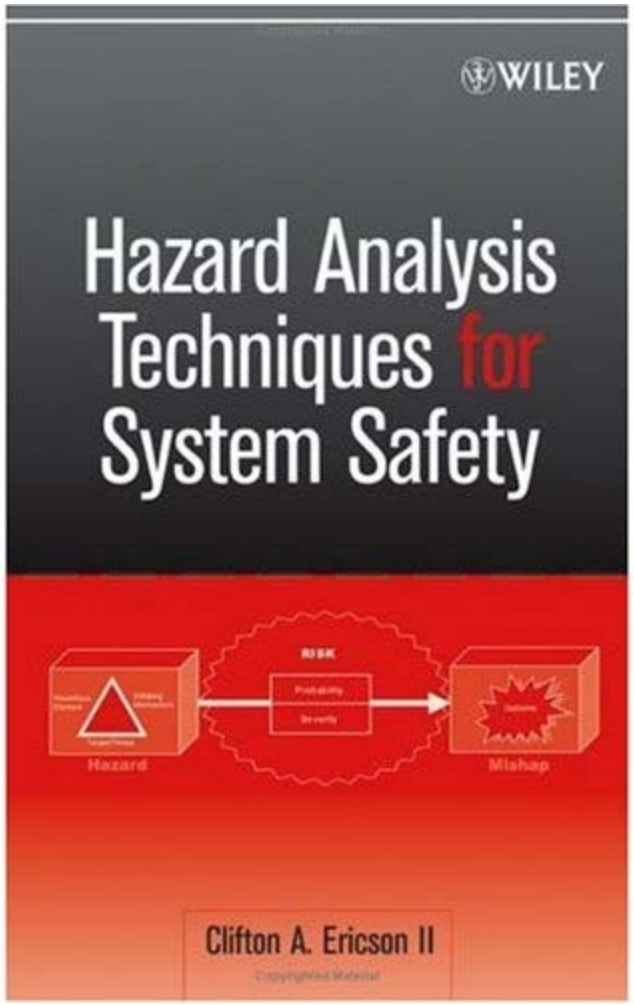
STANDARD PRACTICE FOR SYSTEM SAFETY

AMSC N/A

AREA SAFT

- "[MIL-STD-882D] provides a consistent means of evaluating identified risks."
- "Mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by the system user or customer)…"

Hazard Analysis
The Book



Ericson II, Clifton A., *Hazard Analysis Techniques for System Safety*, Hoboken, NJ: John Wiley & Sons, 2005.

- Ericson has 40 years of experience in system safety,
- 22 specific techniques described (out of hundreds)
- MIL-STD-882D is the underlying basis.

Some Definitions

System – An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.

Life Cycle– All phases of the system's life including design, research, development, test and evaluation, production, deployment, operations, and disposal.

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

More Definitions

Hazard – Any real or potential condition that *can* cause

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

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.

Mishap risk – An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence.

And finally…

System Safety – The application of engineering and management principles, criteria, and techniques to achieve *acceptable mishap risk*, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

Step 1: Identify Hazards

- MIL-STD-882D requires us to:

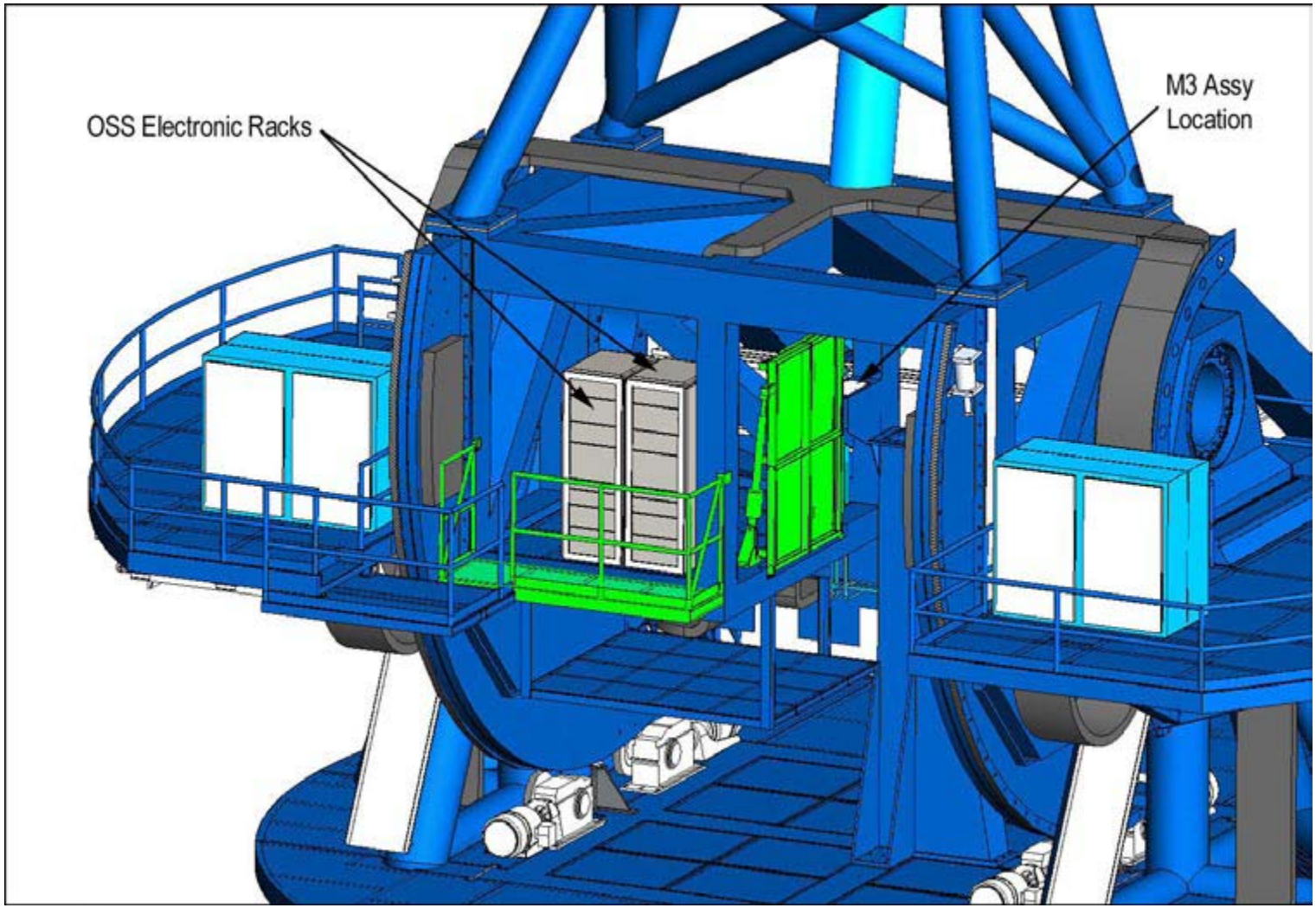
"Identify hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment (in which the system will exist), and the intended use or application."

…and document the process!

The ATST Hazard Analysis Form

Subsystem:				Preliminary Hazard Analysis						Last Update:			
Number	System Item	Hazard	Causes	Effects	Project Phase(s)	Risk			Recommended Action	Risk			Comments
						IMRI	Value	Cat.		FMRI	Value	Cat.	

Deployable Platform



Hazard Identification Example

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

Project phases	
1. D&D	Design and Development
2. FAB	Factory fabrication & preassembly
3. CONST	On-site construction or installation
3. IT&C	Integration Test and Commissioning
4. OPS	Operations
5. MAINT	Maintenance

Subsystem: TMA — **Preliminary Hazard Analysis** — Last Update: 7/4/08

Number	System Item	Hazard	Causes	Effects	Project Phase(s)	Risk IMRI	Risk Value	Risk Cat.	Recommended Action	Risk FMRI	Risk Value	Risk Cat.	Comments
TMA-3	-X access deployable Platform	Pinch Hazard from rotating machinery	The Deployable platform that allows access to the OSS racks will bring a worker within very close proximity to one of the altitude gears.	Personal injury. Clothing capture, fingers	FAB, CONST, IT&C, MAINT								Access denied during operations.

Performed as a group activity

Meeting Makeup

Quorum Participants

- Systems Engineer (presiding)
- Lead Engineer/Architect
- Controls Engineer

Additional Participants

- Project Manager
- Enclosure Engineer (former process engineer)
- Lead Software Engineer
- NOAO/NSO Risk Manager

Step 2: Assess Mishap Risk

A two dimensional assessment:

- Should the hazard become a mishap, are severe are the results?
  - Catastrophic
  - Critical
  - Marginal
  - Negligible
- How likely is this mishap?
  - Frequent
  - Probable
  - Occasional
  - Remote
  - Improbable

Mishap Severity Rankings

	Severity	Description
1	Catastrophic	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
2	Critical	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
3	Marginal	Could result in injury or occupational illness resulting in one or more lost work days, loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
4	Negligible	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

Probability of a Mishap

	Probability	Description
A	Frequent	Likely to occur often in the life of an item.
B	Probable	Will occur several times in the life of an item.
C	Occasional	Likely to occur some time in the life of an item.
D	Remote	Unlikely but possible to occur in the life of an item.
E	Improbable	So unlikely, it can be assumed occurrence may not be experienced.

The Mishap Risk Index

- Weighs both severity and probability.
- Results in Mishap Risk Index, Value, and Category.

	Catastrophic		Critical		Marginal		Negligible	
Frequent	1-A	1	2-A	3	3-A	7	4-A	13
Probable	1-B	2	2-B	5	3-B	9	4-B	16
Occasional	1-C	4	2-C	6	3-C	11	4-C	18
Remote	1-D	8	2-D	10	3-D	14	4-D	19
Improbable	1-E	12	2-E	15	3-E	17	4-E	20

Value	Category
1 – 5	High
6 – 9	Serious
10 – 17	Medium
18 – 20	Low

What must be mitigated?

The Deployable Platform Revisited

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

Project phases	
1. D&D	Design and Development
2. FAB	Factory fabrication & preassembly
3. CONST	On-site construction or installation
3. IT&C	Integration Test and Commissioning
4. OPS	Operations
5. MAINT	Maintenance

Subsystem: TMA — **Preliminary Hazard Analysis** — Last Update: 7/4/08

Number	System Item	Hazard	Causes	Effects	Project Phase(s)	Risk IMRI	Risk Value	Risk Cat.	Recommended Action	Risk FMRI	Risk Value	Risk Cat.	Comments
TMA-3	-X access deployable Platform	Pinch Hazard from rotating machinery	The Deployable platform that allows access to the OSS racks will bring a worker within very close proximity to one of the altitude gears.	Personal injury. Clothing capture, fingers	FAB, CONST, IT&C, MAINT	2-C	6	Ser					Access denied during operations.

Critical – Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization.

Occasional – Likely to occur some time in the life of an item.

Step 3: Mitigation

Four mitigation classifications per MIL-STD-882D:

- Design change or selection
- Incorporation of safety devices
- Incorporation of warning devices
- Development of procedures and use of training

Finished Preliminary Hazard Analysis Entry

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

Project phases	
1. D&D	Design and Development
2. FAB	Factory fabrication & preassembly
3. CONST	On-site construction or installation
3. IT&C	Integration Test and Commissioning
4. OPS	Operations
5. MAINT	Maintenance

Subsystem: TMA				Preliminary Hazard Analysis						Last Update: 7/4/08			
						Risk				Risk			
Number	System Item	Hazard	Causes	Effects	Project Phase(s)	IMRI	Value	Cat.	Recommended Action	FMRI	Value	Cat.	Comments
TMA-3	-X access deployable Platform	Pinch Hazard from rotating machinery	The Deployable platform that allows access to the OSS racks will bring a worker within very close proximity to one of the altitude gears.	Personal injury. Clothing capture, fingers	FAB, CONST, IT&C, MAINT	2-C	6	Ser	The platform should include a fence or shield, audible alarm before slew, procedures, training				Access denied during operations.

- Safety devices
- Procedures and training

Other Hazards

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

Project phases	
1. D&D	Design and Development
2. FAB	Factory fabrication & preassembly
3. CONST	On-site construction or installation
3. IT&C	Integration Test and Commissioning
4. OPS	Operations
5. MAINT	Maintenance

Subsystem: 5.0 Enclosure — **Preliminary Hazard Analysis** — Last Update: 8/11/2008

Number	System Item	Hazard	Causes	Effects	Project Phase(s)	Risk IMRI	Risk Value	Risk Cat.	Recommended Action	Risk FMRI	Risk Value	Risk Cat.	Comments
12	Telescope Level	Electric shorts, water damage.	Fluid leak in enclosure altitude wrap, plate coils or other.	Damage to equipment	CONST, IT&C, OPS, MAINT	1-D	8	Ser	Gutter between TMA floor and pier floor.				
13	Telescope Level	Trapped by fire	Only safe egress is to find a way from the telescope level to the exterior catwalk, which has an emergency stairway to the ground.	Personal injury	CONST, IT&C, OPS, MAINT	1-C	4	High	Alternate exits through the enclosure to the catwalk. They should be interlocked until motion stops.				In the current reference design there are three ways off of the telescope level: the LULA lift, the stairs next to it, or via the lift in the unlikely event that everything is aligned and the platform lift is up at the telescope level.
14	Enclosure TEOA Platform	Fall hazard	Fall while working on the TEOA	Personal injury	CONST, IT&C, MAINT	1-C	4	High	Tie-off procedure				
15	Enclosure TEOA Platform	Fall hazard	Fall before platform is deployed.	Personal injury	CONST, IT&C, MAINT	1-C	4	High	Design the rails with overlap so there can be no gap.				
16	Enclosure TEOA Platform	Dropping or falling objects	Tools dropped while working on the TEOA	Personal injury, damage to lift.	CONST, IT&C, MAINT	2-C	6	Ser	Hard hats below.				
17	Enclosure TEOA Platform	Fall hazard	Try to drive platform with gates in the wrong position.	Damage to equipment. Personal injury.	CONST, IT&C, MAINT	1-C	4	High	TEOA gates must interlock with deployment and retraction of platform.				
18	Enclosure TEOA Platform	Fall hazard	Overtravel of deployable gates.	Damage to equipment. Personal injury.	CONST, IT&C, MAINT	1-C	4	High	Design change.				
19	Rear Access Door	Pinch/crush	Someone is leaning over the railing when someone else closes the overhead door	Personal injury	CONST, IT&C, MAINT	2-D	10	Med	Move gate far enough back to prevent this.				This is a roll-up door

Some Comments on the Hazard Meetings

- Bring drawings or have access solid model
- Control the discussion: keep on task
  - Complete an entry before moving on,
  - But jot down notes to prompt return to new hazard.
- Limit meetings to one hour.
- Meet at a regular time for a protracted period.
  - PHA took months!
  - At the last peak of the activity we were meeting three times a week.
- Keep reading the severity and probability definitions

After the PHA?

- Implement some safety design changes in reference design
- Add requirements to the relevant specification and design-requirements documents
- Develop detailed procedures
- Calculate a final mishap risk index
- Discuss the project's risk tolerance
- Use our PHA of the reference design as an example for vendors
- Review vendor risk analyses

The TMA Statement of Work

Contractor shall perform a thorough hazard analysis of the TMA as prescribed in MIL-STD-882D, “System Safety Requirements”/”Standard Practice for System Safety” with respect to personnel and equipment safety conditions and possible unsafe scenarios. This analysis shall be included in the Safety Plan and shall be continuously reviewed and updated throughout the duration of the Work. At least once per each of the phases of the Work, Contractor shall formally present to AURA an update to the Safety Plan.

Some Shortcomings of Our Process

- We started late and did things in the wrong order initially.
- Still need to stand back and look at larger systems rather than one assembly at a time.
  - Fire
  - Hurricane
  - Power failure
- We are much better now than when we began, and would benefit from a second pass in some cases.

ATST
Hazard Analysis

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

Project phases	
1. D&D	Design and Development
2. FAB	Factory fabrication & preassembly
3. CONST	On-site construction or installation
3. IT&C	Integration Test and Commissioning
4. OPS	Operations
5. MAINT	Maintenance

Subsystem: 5.0 Enclosure — **Preliminary Hazard Analysis** — Last Update: 8/11/2008

Number	System Item	Hazard	Causes	Effects	Project Phase(s)	Risk			Recommended Action	Risk			Comments
						FMRI	Value	Cat.		FMRI	Value	Cat.	
12	Telescope Level	Electric shorts, water damage.	Fluid leak in enclosure altitude wrap, plate coils or other.	Damage to equipment.	CONST, IT&C, OPS, MAINT	1-D	8	Ser	Gutter between TMA floor and pier floor.				
13	Telescope Level	Trapped by fire	Only safe egress is to find a way from the telescope level to the exterior catwalk, which has an emergency stairway to the ground.	Personal injury	CONST, IT&C, OPS, MAINT	1-C	4	High	Alternate exits through the enclosure to the catwalk. They should be interlocked until motion stops.				In the current reference design there are three ways off of the telescope level: the LULA lift, the stairs next to it, or via the lift in the unlikely event that everything is aligned and the platform lift is up at the telescope level.
14	Enclosure TEOA Platform	Fall hazard	Fall while working on the TEOA	Personal injury	CONST, IT&C, MAINT	1-C	4	High	Tie-off procedure				
15	Enclosure TEOA Platform	Fall hazard	Fall before platform is deployed.	Personal injury	CONST, IT&C, MAINT	1-C	4	High	Design the rails with overlap so there can be no gap.				
16	Enclosure TEOA Platform	Dropping or falling objects	Tools dropped while working on the TEOA	Personal injury, damage to lift	CONST, IT&C, MAINT	2-C	6	Ser	Hard hats below.				
17	Enclosure TEOA Platform	Fall hazard	Try to drive platform with gates in the wrong position.	Damage to equipment. Personal injury	CONST, IT&C, MAINT	1-C	4	High	TEOA gates must interlock with deployment and retraction of platform				
18	Enclosure TEOA Platform	Fall hazard	Overtravel of deployable gates.	Damage to equipment. Personal injury	CONST, IT&C, MAINT	1-C	4	High	Design change.				
19	Rear Access Door	Pinch/crush	Someone is leaning over the railing when someone else closes the overhead door	Personal injury	CONST, IT&C, MAINT	2-D	10	Med	Move gate far enough back to prevent this.				This is a roll-up door

END