THE UNIVERSITY OF TOKYO

Visiting Professor Lecture

Telescope Project Development Seminar

Session 1b: Systems Engineering

Matt Johns
1/20/2017
U. Tokyo

Session 1 Outline

Session 1a Introduction

1. Introduction
2. Project Initiation
3. Student Assignment
4. Project Implementation

Session 1b Systems Engineering

1. Systems Engineering Function
2. SE Documents
3. Requirements Flow-down
4. Interfaces
5. Document management system
6. Configuration control
7. Risk management
8. Modeling and analysis
9. Prototyping
10. Hazard management
11. Quality Assurance
12. Reviews
13. Integration and Commissioning
14. Student Assignment

Systems Engineering

The objective of the Systems Engineering effort is to assure successful development of the project primarily by defining clear and accurate system requirements and verifying compliance of the system to those requirements.

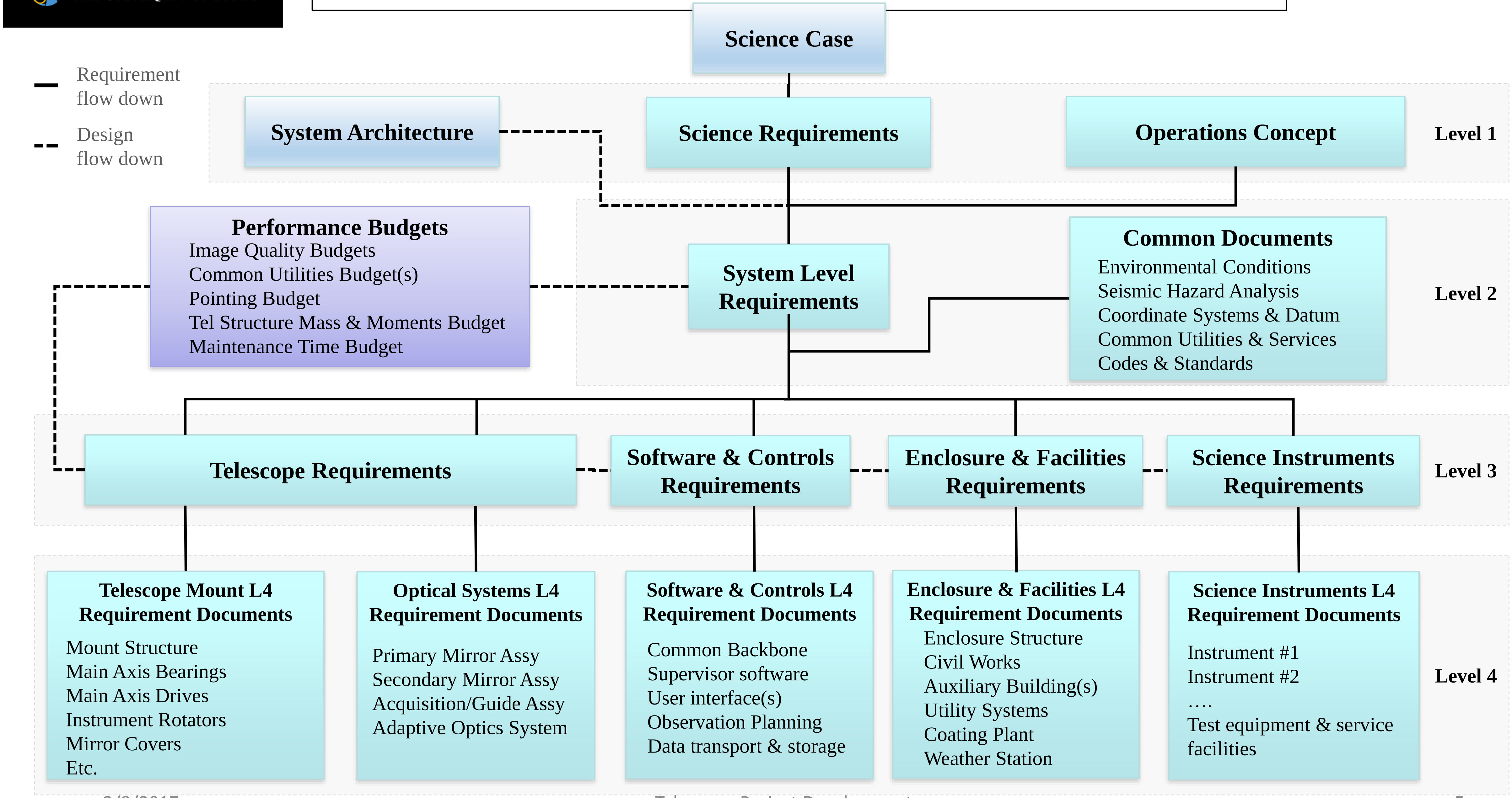
System Engineering responsibilities and procedures are captured in a Systems Engineering Management Plan (SEMP)

Systems Engineering Functions

- Foundation docs (system architecture, operational concept documents, project dictionary, standards, codes, coordinates, environments, …)
- Documentation management
- Configuration control
- Performance budgets and allocations
- Requirements Management
- Product Breakdown Structure (PBS)
- Interface Controls

- System-level modeling
- Technical Risk Management
- Quality assurance
    - Test and Verification procedures
- Project Reviews
- Assembly, Integration, Test and Commissioning (AITC) Plans
- *Safety Plan & hazard analysis*

Systems Engineering Document Tree



— Requirement flow down

-- Design flow down

Science Case

Level 1

System Architecture

Science Requirements

Operations Concept

Level 2

Performance Budgets
Image Quality Budgets
Common Utilities Budget(s)
Pointing Budget
Tel Structure Mass & Moments Budget
Maintenance Time Budget

System Level Requirements

Common Documents
Environmental Conditions
Seismic Hazard Analysis
Coordinate Systems & Datum
Common Utilities & Services
Codes & Standards

Level 3

Telescope Requirements

Software & Controls Requirements

Enclosure & Facilities Requirements

Science Instruments Requirements

Level 4

Telescope Mount L4 Requirement Documents
Mount Structure
Main Axis Bearings
Main Axis Drives
Instrument Rotators
Mirror Covers
Etc.

Optical Systems L4 Requirement Documents
Primary Mirror Assy
Secondary Mirror Assy
Acquisition/Guide Assy
Adaptive Optics System

Software & Controls L4 Requirement Documents
Common Backbone
Supervisor software
User interface(s)
Observation Planning
Data transport & storage

Enclosure & Facilities L4 Requirement Documents
Enclosure Structure
Civil Works
Auxiliary Building(s)
Utility Systems
Coating Plant
Weather Station

Science Instruments L4 Requirement Documents
Instrument #1
Instrument #2
….
Test equipment & service facilities

System Architecture (Level 1)

- Requirements in themselves do not determine the design of the telescope, instruments or associated facilities. An initial concept is required. The concept is developed in discussions with the project stakeholders and through trade studies conducted by the Project.
- A layout of the telescope facility and functional description of the various parts of the observatory are used to translate Science Requirements into System Level Requirements and flow them down to lower levels. This information is captured in a System Architecture Document.
- The observatory architecture is tied to the presumed site location and environmental conditions.
- The System Architecture is the basis of the Conceptual Design Review.
- The Architecture will evolve with time as the designs and operational concepts mature.

Operations Concept Document (Level1)

- The Operations Concept Document describes in high-level detail how the facility will operate.
  - Observation planning and procedures
  - Nighttime observing procedures including observing modes (“classical” on-site observer, remote observing, service observing, queue observing,…)
  - Telescope configuration changes (instrument ports, optical configuration)
  - Day time instrument set-up and calibration
  - Science Instrument changes
  - Off-telescope Science Instrument service and assembly
  - Data acquisition, storage and transport
  - Servicing and maintenance of the telescope subsystems and Science Instrumentation
  - Mirror re-coating
  - Mountain operations
  - Logistics and accommodations
- The Operations Concept is elaborated in additional documents at lower levels.

Common Documents

- Common Documents provide a shared framework for the design of the facility. Examples are:
  - Environmental Conditions – gives statistics for the ambient conditions (temperature, humidity, wind, sky brightness, atmospheric conditions such as sky brightness and water vapor) on site. These are specified as mean values and rates of change broken down by day-night and time of year and on days suitable for observing.
  - Site-specific Seismic Hazard Analysis – is a probabilistic analysis of the ground accelerations to be expected at the site over the lifetime of the facility in the event of a major earthquake. The analysis gives the maximum expected vertical and horizontal accelerations as a function of the specified return period. It also provides simulated acceleration time series for dynamically modeling the response and stressed in the telescope, instruments, and enclosure during major events.
  - Coordinate Systems and Datum – provides a common frame of reference and key fiducials for designing and locating all of the mechanical assemblies within the enclosure and on the telescope.
  - Common Utilities & Services – specifies the shared services (power, coolants, compressed gasses, communications, etc.) supplied by the facility and used by the various subsystems.
  - Codes and Standards – lists the codes and standards that apply across the project. It might include building codes, local regulations, electrical codes, hardware and software standards, robotic control standards, safety standards, etc.
- Creating these at the start of the project reduces the amount of back-tracking later on.

Allocation Budgets

- Budgets provide a way of allocating budgeted items to subsystems. The allocated amounts then end up as requirements at the subsystem level. Examples are:
  - **Image Quality Budgets** – list maximum subsystem contributions to the top level image size requirement. Separate budgets will be required for each optical configuration of the telescope including natural-seeing and adaptive optics operations.
  - **Optical Throughput Budgets** – allocates reflection, transmission, and vignetting losses for the separate optical configurations.
  - **Common Utilities Budgets** – lists the amount of facility utilities (power, water, gasses, etc.) available to the various subsystems and mountain facilities.
  - **Pointing Budget** – allocates maximum subsystem contributions to the pointing error budget. Separate budgets may be required for different telescope/instrument configurations but they need to be consistent. The Pointing Budget(s) contribute to the Image Quality Budgets.
  - **Telescope Structure Mass and Moments Budget** – lists masses and moments about the azimuth and elevation axes for the assemblies. It is used to check that the structure is balanced in elevation.
  - **Maintenance Time Budget** – allocates the total time allowed for various service operations.
- Other budgets – telescope slew and acquisition, instrument change-over, calibration sequences, data handling, etc. may exist at various levels in the requirements structure.

Image Quality Budgets

- Image Quality budgets are developed from a top-level requirement and decomposed into subsystem allocations.
- The metrics defining how image quality is defined and how allocations are combined are specified by Systems Engineering.
  - Common metrics are image size (e.g. FWHM, RMS diameter, ..) and encircled energy diameter (e.g. 80%ee).
- Allocations become requirements at the subsystem level.
- The Image Quality budgets are periodically re-balanced to reduce allocations that are overly generous and give relief to technically challenging or costly entries as long as the overall budget is not exceeded.
- IQ budgets are verified by bottom-up analysis & measurement.

THE UNIVERSITY OF TOKYO

Wide-field Image Quality Budget

Direct Gregorian Wide Field (DGWF)

Description:	Visible band, wide-field, natural seeing active optics error budget in terms of 80%ee. Segmented secondary mirror with fast tip-tilt.
Zenith angle	0 degrees
Field diameter	20 arc-min
Wavelength	0.37 - 1.0 microns
Metric	80% ee (arcsec)
Primary mirror	segmented, not phased
Secondary mirror	segmented, fast steering mode
Corrector/ADC	yes
Environmental:	
Windspeed	4.0 m/s to 6.5 m/s
Temperature Range	+7C to +18C
Temp rate of change	-0.44 K/hr to +0.2 2K/hr

	Allocations (80% ee)	**Level 3**	**Level 2**
Optical Design			**0.055**
Optical Surfaces:			**0.204**
	Primary mirror segment figure	0.166	
	Secondary mirror figure	0.081	
	Primary mirror supports	0.036	
	Secondary mirror supports	0.020	
	Corrector elements	0.076	
Active Alignment:			**0.178**
	Primary segments	0.088	
	Secondary segments	0.141	
	Corrector elements	0.059	
	Focal plane	0.010	
	Sensor error	0.025	
Wind disturbance			**0.133**
	Primary mirror figure	0.075	
	Optical alignment & pointing	0.109	
	Focus	0.017	
Thermal			**0.106**
	Primary mirror figure	0.089	
	Mirror seeing	0.057	
Tracking			**0.101**
	Drive errors	0.071	
	Differential flexure	0.071	
Dome seeing			**0.025**
	Total allocated error budget:		**0.341**
	Science Requirements		**0.380**
	Unallocated		**0.168**

Requirements Flow-down

- Requirements govern the functionality, operation and performance of the System.
- The top-level Science Requirements are developed from the goals described in the Science Case and possibly other Project objectives [eg. education, technology development, etc.] specified by the stakeholders.
- Requirements are logically grouped by subsystem below level 2.
- Upper-level requirements spawn “child” requirements on levels below as operational procedures are refined and engineering studies and designs develop, and so on down the pyramid.
- Requirements can and often do have more than one parent requirement and spawn more than one child.
- Requirements in one subsystem can have parents from another.

Requirements Guide

- Traceability
  - All requirements below the level 1 Science Requirements Document have one or more parent requirements from higher levels. They are child requirements for the higher level requirement. “No orphan requirements below level 1”.
  - System Architecture, design and engineering studies, technical budget allocations, operations concept documents, common documents, all feed into the requirements flowdown. Documenting the justification and source(s) within the requirements provides traceability.
- Verifiability
  - Avoid combining multiple requirements into one.
  - Provide measurable criteria for acceptance. Avoid using terms such as “maximize” or “minimize”.
  - Terminology:
    - “Shall” denotes requirements that are mandatory and subject to testing and verification.
    - “Will” specifies an action that will take place but is not treated as a requirement subject to verification.
  - Prescribe the method for acceptance (“Design”, “Inspection”, “Analysis”, “Test”, “Demonstration”) for each requirement. Test procedures may be specified as appropriate.
- Compliance Matrix
  - Produced for final acceptance of the system or subsystem.
  - Lists the requirement, measured value, acceptance criteria and “Pass” or “Fail” for each item.
- Software packages (Doors, Cognition Cockpit, home brew)

Level 1 GMT Science Level Requirements Examples

- **SCI-0951: GMT description**
- The GMT shall be a ground-based 25-meter class telescope with natural-seeing and adaptive-optics diffraction-limited observing modes optimized for fundamental scientific research at near-UV, optical and infrared wavelengths.

- **SCI-0952: Site location**
- The GMT facility shall be located at Las Campanas Observatory, Chile.

- **SCI-1006: Nighttime Operation**
- The GMT shall be designed for night time observing.
- *Note:* Night time is defined from astronomical twilight to twilight. GMT will be operable outside those hours for calibrations, etc. with certain restrictions.

- **SCI-0985: Lifetime**
- The GMT Observatory shall be designed for a 50 year lifetime assuming routine maintenance of the telescope and facilities and periodic upgrades of field replaceable components and subsystems.

Level 1 GMT Science Level Requirements

Representative science cases include: (a) planet and star formation, (b) stellar populations and chemical evolution, and (c) first light and reionization.

- **SCI-1016: Narrow-field natural seeing Capability**
- The GMT shall have a natural seeing mode of operation that delivers an unobstructed natural-seeing field of view to science instruments of not less than 10 arcminutes in diameter over the wavelength range of 320 nm to 25 microns.
- *Note:* This is a non-corrector/non-ADC mode.

- **SCI-1876: NF Natural Seeing Image Size**
- The GMT narrow-field natural-seeing observing mode shall contribute no more than 0.34 arcsecond [goal: 0.28"] 80% encircled energy diameter image blur combined in RSS to the overall image size at the center of the science field for the conditions specified in Table 8 over the full observing range on the sky after correction for zenith angle.

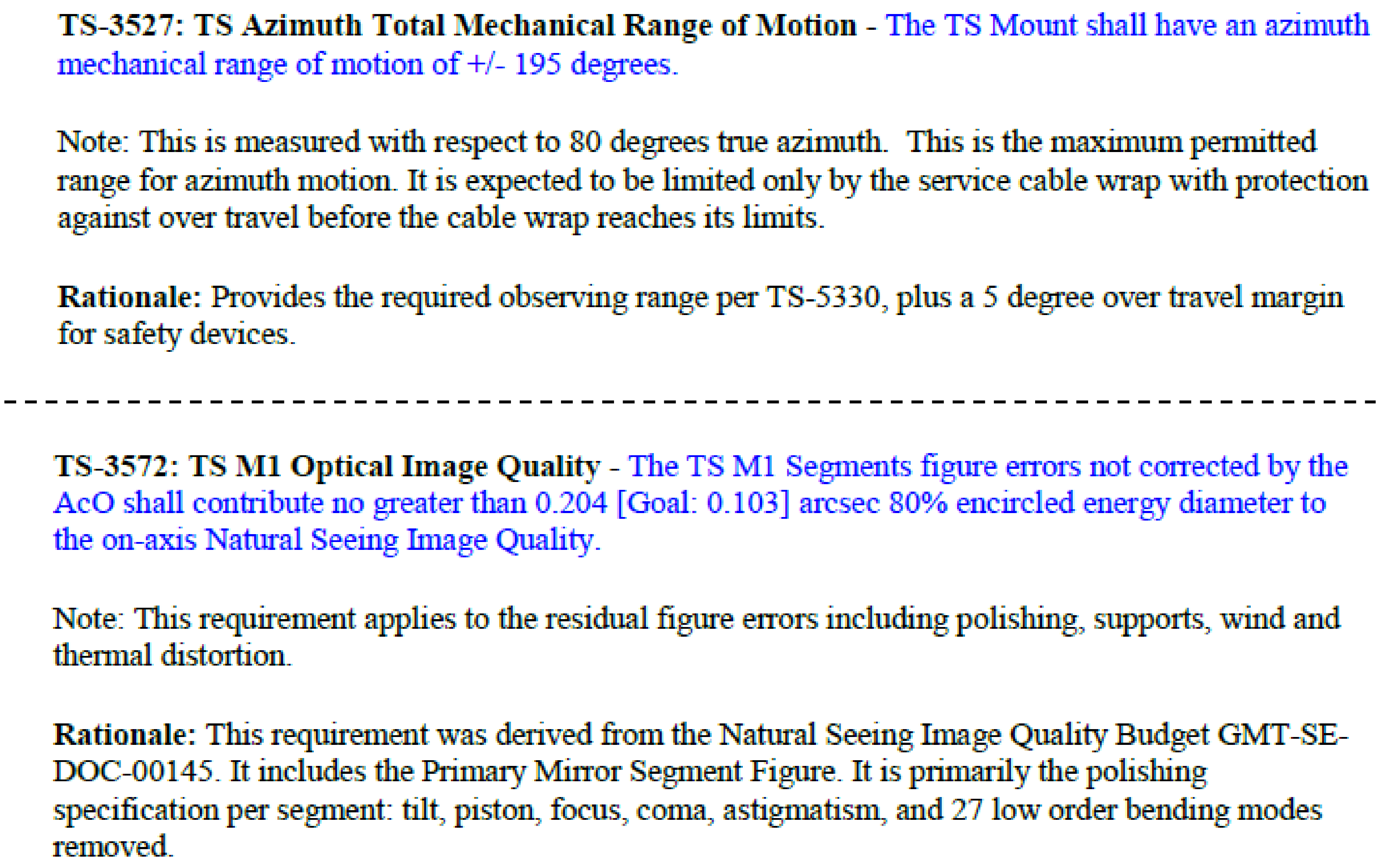
Level 2 GMT System Level Requirements

- **SLR-2557: Telescope Configuration -** The GMT shall have an altitude over azimuth structure.

- **SLR-2661: Gregorian Optical Design -** The GMT optical system shall be based on an aplanatic Gregorian prescription with segmented primary and secondary mirrors as specified in the Optical Design document GMT-SE-DOC-00010.

- **SLR-2701: Optical Prescriptions -** The GMT optical system shall be designed according to the prescriptions specified in the Optical Design document GMT-SE-DOC-00010.
- *Note:* There are three optical configurations specified:
  - Direct Gregorian - Narrow Field (DGNF)
  - Direct Gregorian - Wide Field (DGWF)
  - Folded Port (FP)

Level 3 GMT Telescope System Requirements



TS-3527: TS Azimuth Total Mechanical Range of Motion - The TS Mount shall have an azimuth mechanical range of motion of +/- 195 degrees.

Note: This is measured with respect to 80 degrees true azimuth. This is the maximum permitted range for azimuth motion. It is expected to be limited only by the service cable wrap with protection against over travel before the cable wrap reaches its limits.

Rationale: Provides the required observing range per TS-5330, plus a 5 degree over travel margin for safety devices.

TS-3572: TS M1 Optical Image Quality - The TS M1 Segments figure errors not corrected by the AcO shall contribute no greater than 0.204 [Goal: 0.103] arcsec 80% encircled energy diameter to the on-axis Natural Seeing Image Quality.

Note: This requirement applies to the residual figure errors including polishing, supports, wind and thermal distortion.

Rationale: This requirement was derived from the Natural Seeing Image Quality Budget GMT-SE-DOC-00145. It includes the Primary Mirror Segment Figure. It is primarily the polishing specification per segment: tilt, piston, focus, coma, astigmatism, and 27 low order bending modes removed.

- **TS** == Telescope System
- **AcO** == Active optics
- “**Shall**” denotes requirements that are mandatory and subject to testing and verification.
- **Rationale** provides additional justification for the requirement and traceability.
- **Note** provides information regarding application or implementation.

Excerpt from “Telescope System Requirements”, GMT-TEL-REQ-000158-A”

Interfaces

- Interface control is critical to the successful implementation of a project composed of multiple subsystems developed by different groups. The goal is to ensure that the various subsystems of the telescope can be assembled together and function as a whole to meet the top level performance requirements.
- The basic tool for interface control is the Interface Control Document (ICD).
- The ICD is an agreement, essentially a contract, between two or more Project teams working on their various subsystems. It may involve internal groups of the project, and/or external groups.
- Working from the Product Breakdown Structure (PBS), Systems Engineering identifies where interfaces exist between subsystems/subassemblies that require interface control and an ICD. The responsibility for these are then assigned to the team.
- ICDs specify the physical and mechanical properties of the interface, electrical and control hardware and protocols, and any other properties that affect the design and performance on either side of the interface.
- ICDs should be completed, accepted and under configuration control prior to completion of the subsystem preliminary designs.
- In the case of contracted systems, the ICD(s) become part of the Contractor’s workpackage.
- Compliance with ICDs are specific requirements for each subsystem.

Document Management

- Good document management is a necessary requirement for large projects.
- The document system needs the tools to
  - Assign document numbers
  - Accommodate different document types as required
  - Enter documents into the system
  - Locate documents (searchability)
  - Revise documents periodically and retain a history of past versions
  - Store metadata (type, title, author, revision date, WBS reference, document number(s), status, etc.)
  - Control access documents with proprietary/sensitive content
  - Distribute documents to authorized personnel
  - Enforce configuration control by requiring appropriate approvals
  - Archive and backup the database
- The document system should be established as early in the Project to avoid the necessity of going back and re-formatting/re-entering earlier versions.
- Simplicity is key to encouraging people to use the system
- A number of commercial web-based document management systems exist (Docushare, Content Central, …)

Configuration Control

- Documents that define the configuration of the facility, its design, performance and functional capabilities, and operation need to be placed under configuration control in order to ensure a stabile development process.
- Procedures are required for entering controlled documents into the system, responding to requests for changes, change-approval process, and communication of changes to affected groups.
- Change approval typically takes into account the performance, cost and schedule impact of the proposed change.
- Documents that are subject to configuration control include:
  - Requirements Documents
  - Interface Control Documents
  - Design documents (drawings, CAD models, specifications, etc.)
  - Operation and service manuals
  - Project procedures
- The design baseline is composed of the complete set of configuration controlled documents.
  - Change control also applies to technical reports and management procedures but these are not part of the Baseline.

Change Control

- Change control procedures should be well defined and specify:
  - Which documents are subject to control.
  - Who is responsible for managing the process.
  - How is a change request initiated.
  - Evaluation and approval procedures.
    - Evaluation criteria
    - Who has final approval authority (Systems/chief Engineer, Project Manager, Project Director, Board of Directors)
  - How changes are communicated within the project and to outside stakeholders.
  - Documenting the change process from start to finish.
- The change procedure may be different depends on the impact (major, limited, routine) of the request.

Technical Risk Management

- Systems Engineering identifies and tracks technical risks that impact system performance (technical), Project cost or schedule.
  - The risks are entered in a Risk Register.
  - Risks associated with personnel or equipment safety are handled separately with a Hazard Analysis.
- Identified risks are graded as to their potential impact and likelihood of occurrence.
  - The severity of the risk is the product of the impact and likelihood grades and is the higher of the technical, cost or schedule scores or the three could be tracked separately.
- Mitigation measures designed to lower the severity are developed for each risk.
- Mitigation measures are applied in an on-going process until the severity falls below some threshold and the risk is retired.
- Risks are periodically reviewed with Project Management, typically at monthly reviews.

Examples of major technical risks

- Inadequate modeling and analysis resulting in performance requirements not being met.
- Incomplete requirements and ICDs that result in delays, performance hits, additional remedial work, schedule slip, and costs.
- Process failures during optics fabrication that result in delays and/or damage to the part.
- Risks associated with first-time assembly and integration of major subsystems on site.
  - Incompatible subsystem interfaces due to incomplete or incorrect Interface Control Documents.
  - Incorrect AITC procedures
- Unavailability of critical components from suppliers.
- Faulty software (code specification, algorithmic, coding, etc.)

More Examples of major technical risks

- Faulty design of mechanical assemblies requiring rework or replacement.
- Poor planning during the on-site assembly, integration, and testing of subassemblies from different sources resulting in delays and possible cost penalties.
- Poor subsystem performance due to challenging environmental conditions at the site.
- Damage during handling or transport of optics, structure, and components.
- Schedule slips that delay overall project completion.

Risk Grading & Severity- Large Project

Likelihood of Occurring	
1	Chances of occurring are very low, less than 5%
2	Unlikely to occur 5% – 15%
3	Some chance of occurring 15 – 30%
4	Good chance of occurring 30% – 60%
5	Very likely to occur >60%

		Impact rating				
		1	2	3	4	5
Likelihood Rating	5	🟩	🟨	🟥	🟥	🟥
	4	🟩	🟨	🟨 (4)	🟥 (1)	🟥
	3	🟩	🟩 (3)	🟨 (6)	🟨 (1)	🟥 (2)
	2	🟩	🟩	🟩 (1)	🟨 (1)	🟨 (4)
	1	🟩	🟩	🟩	🟩	🟩

(#) = number of telescope risks

Risk Impact	Technical	Cost	Schedule
1	Results in not meeting non-critical design requirements documents	$100k – $250k	Delays delivery of sub-system by 1-3 months
2	Results in reduction in sub-system performance	$250k – $500k	Delays delivery of sub-system by 4-6 months
3	Results in reduction in system level performance	$0.5m – $2m	Delays critical path by up to 1 month
4	Results in minor change to Science Requirements	$2m – $10m	Delays critical path by 1-3 months
5	Results in significant change to Science Requirements	>$10m	Delays critical path by more than 3 months

Risk Severity = Likelihood x Impact

Source: GMT SPDR

Adjust costs as appropriate for each specific project.

Example: High Severity Risks

Risk	Description	Risk Type	Impact	Likelihood	Risk Exposure	Mitigations
0095: Corrector-ADC Optics Fabrication	Fabrication complexity and risk may limit vendors and result in costs that exceed the budgeted amount	Cost	4 - Significant	4 - Probable	16	0197: Descope to include only the corrector function. 0198: Investigate strategies to reduce glass specifications perhaps trading some performance. 0199: Cast a large test blank to demonstrate feasibility.
0085: Mirror segment catastrophic failure during manufacture	Catastrophic failure of M1 mirror blank during manufacture	Cost	5 - Significant	3 - Possible	15	0200: Require documented, reviewed and controlled process procedures.
0098: Mirror segment catastrophic failure during shipment	Catastrophic failure of a M1 segment during transport of a primary mirror segment to the site	Cost	5 - Significant	3 - Possible	15	0201: Provide engineered shipping container. 0202: Establish and review comprehensive shipping procedures and plan. 0203: Obtain insurance.
0126: Loss of M1 mirror during servicing operations	Damage or loss of a primary mirror segment due to equipment failure or improper handling procedures during on-site servicing operations	Cost	5 - Significant	3 - Possible	15	0257: Establish and enforce well-specified handling procedures. 0258: Inspect and/or load test equipment before handling operations.

Example: Medium Severity Risks

Risk	Description	Risk Type	Impact	Likelihood	Risk Exposure	Mitigations
0003: Telescope Wind Shake	If telescope response to vibration from wind loads and other sources is greater than estimated, then image motion may exceed allocated error budget value	Technical	3 - Moderate	4 - Probable	12	MIT0005: Use wind tunnel tests results and CFD modeling to verify wind-load assumptions. MIT0006: Use Tip/Tilt correction. MIT0007: Add damping to main truss.
0067: Telescope Fabrication Costs	If the bids for the fabrication of the telescope structure are significantly higher than the budgeted amount, then contingency funds will be required and/or a descope of the fabrication work may be necessary	Cost	4 - Significant	3 - Possible	12	MIT0146: Two industry-derived cost estimates have been used in the cost basis for this budget amount. MIT0147: Other large telescope fabrication costs are being tracked and compared. MIT0148: New estimates will be obtained following completion of the Structure preliminary design modeling.
0071: Telescope Design Schedule	If the telescope detailed design services contract is not underway at the end of the preliminary design phase, then the telescope structure fabrication and delivery dates will be adversely affected	Schedule	3 - Moderate	4 - Probable	12	MIT0152: Perform an exhaustive search for vendors capable and interested in performing the design work. MIT0153: Draft SOW and requirements documents well in advance of SLPDR. 0248: Change plan to shorten procurement time.

Modeling and Analysis

- Modeling and analysis is required to demonstrate a priori that the system as designed will meet its performance requirements.
- Examples:
  - Telescope structure modes
  - Wind shake
  - Active optics performance
  - AO performance
  - Telescope tracking
  - Telescope and enclosure seismic response
  - Thermal control
- Compliance with functional requirements are demonstrated with use cases
- Results of modeling are presented at major project reviews (e.g. Preliminary Design Reviews).

Prototyping

- Project risk can be reduced by prototyping and testing high risk exposure subassemblies. Prime examples:
    - Telescope main axis bearings and drives
    - Mirror supports and thermal controls for segmented mirror telescopes
    - Science instruments
        - Detectors.
        - Mechanisms (filter wheels, aperture masks, grating changers, etc.)
    - Control system hardware and software
    - Mirror coating system components
    - Utility wraps and cable chains
    - Mirror covers
    - Handling equipment including transport containers

Safety

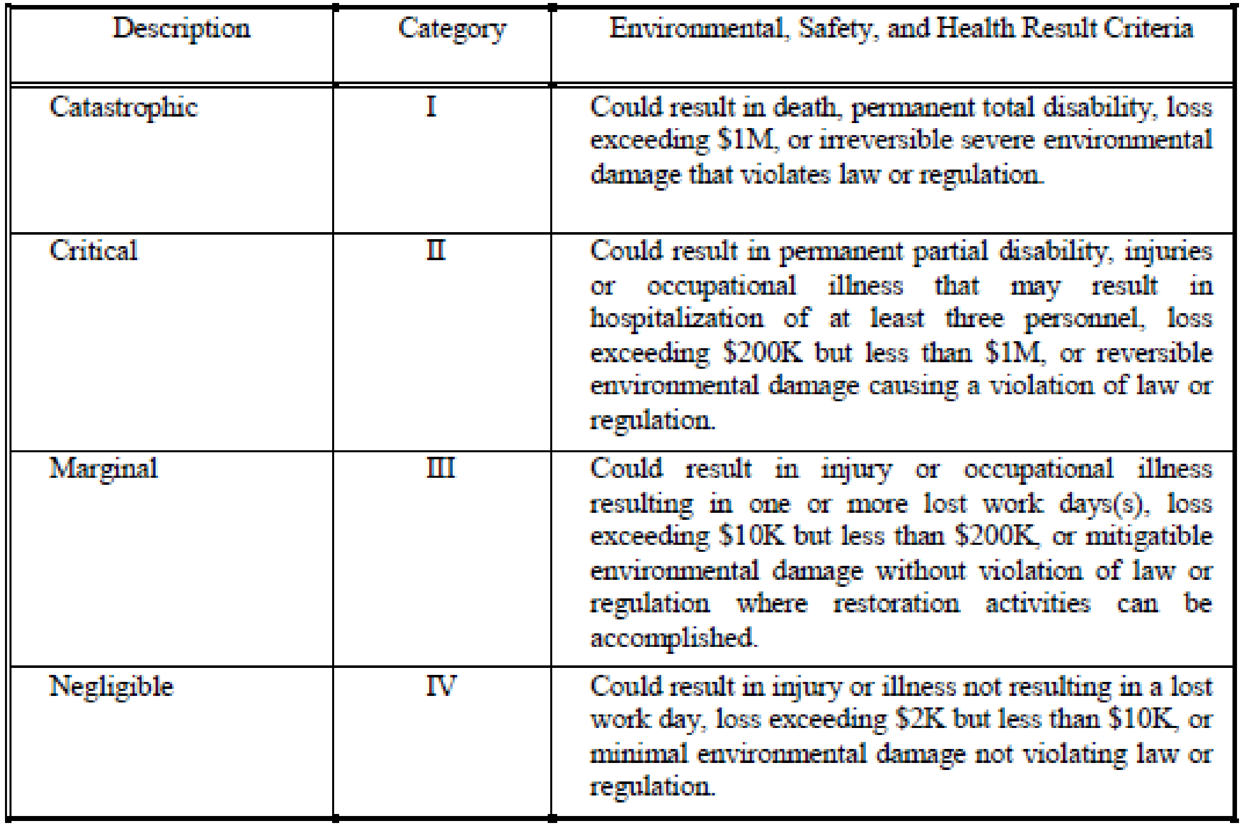
- “Safety” applies to both personnel and equipment safety
- Safety Policy
  - Specifies the Project procedures and practices for creating and maintaining a safe and healthy work environment.
  - Describes responsibilities for enforcing the safety policy.
  - Includes safety for work on site.
  - Adherence to all applicable safety codes a key element of the policy
- Design Safety Plan
  - The process for achieving operational and functional safety through design considerations throughout the lifecycle of the project.
  - Considers personal injury, damage to equipment, and damage to the environment.
- Hazard Analysis (e.g. US DOD Standard Practice for System Safety)
  - Subsystem by subsystem review to identify and grade hazards based on prescribed criteria.
  - Formulate recommended mitigation (risk control) measures and assign responsibility for their implementation.
  - Periodically update the HA as mitigation measures are applied.

Hazard analysis

- The hazard analysis covers both personnel and equipment safety
- Often managed by the safety officer as part of the safety program.
- Hazard evaluation and mitigation use a formalism similar to technical risk analysis.
- Provides requirements for the design of the observatory subsystems, operational procedures and, in particular the Interlock and Safety System (ISS).
- Coordinated and integrated with the overall Project safety program.
- Formalism is similar to risk assessment.

Hazard Severity & Probability

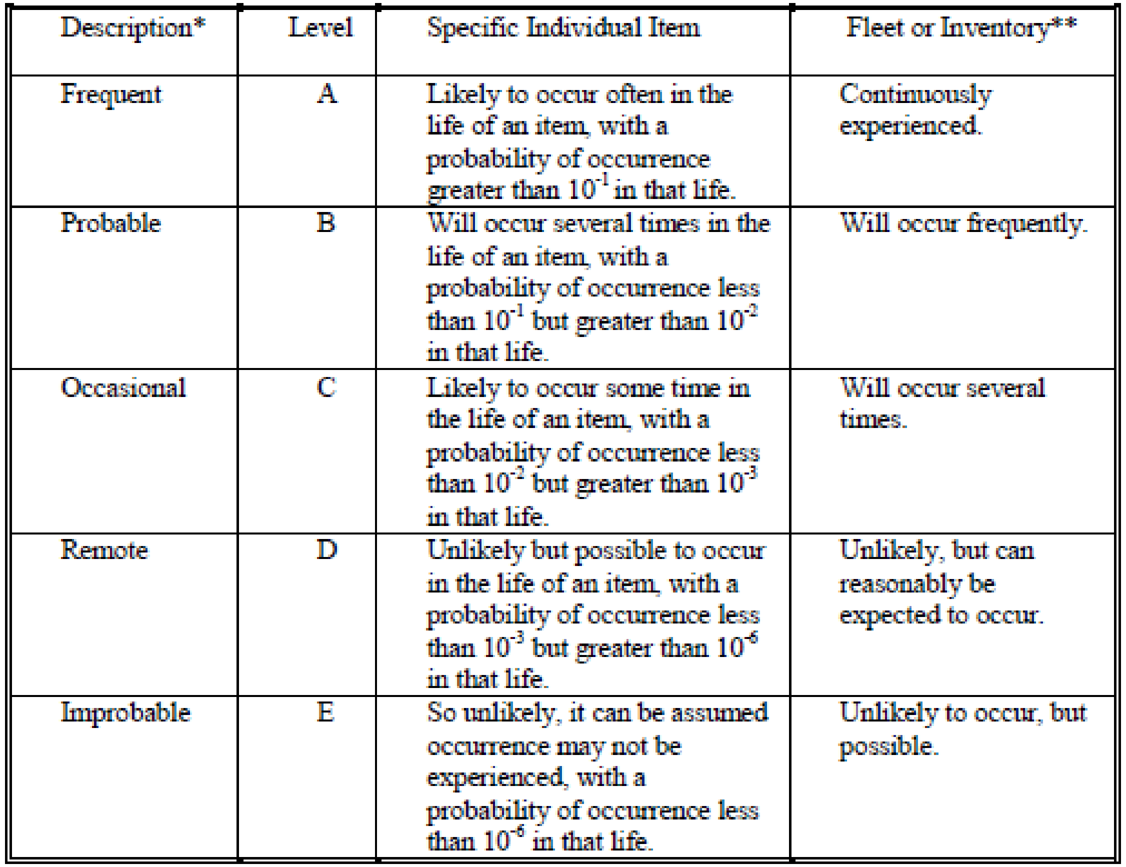
Severity



Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	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.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	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.

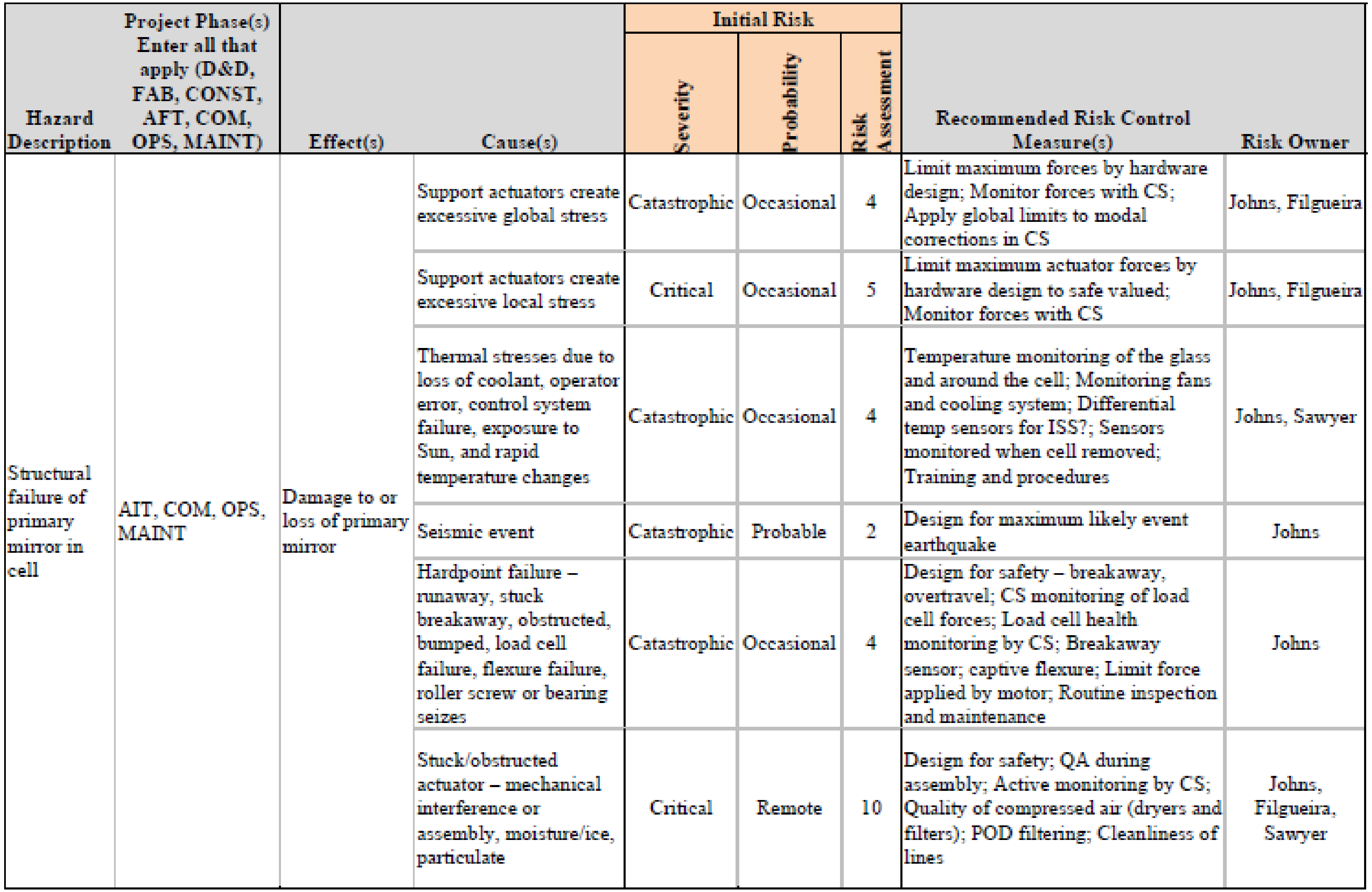
per MIL-STD-882D

Probability



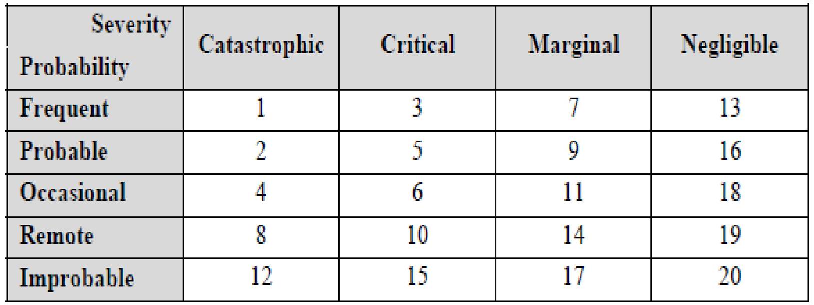
Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	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.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

Hazard Analysis Example



Hazard Description	Project Phase(s) Enter all that apply (D&D, FAB, CONST, AFT, COM, OPS, MAINT)	Effect(s)	Cause(s)	Initial Risk			Recommended Risk Control Measure(s)	Risk Owner
				Severity	Probability	Risk Assessment		
Structural failure of primary mirror in cell	AIT, COM, OPS, MAINT	Damage to or loss of primary mirror	Support actuators create excessive global stress	Catastrophic	Occasional	4	Limit maximum forces by hardware design; Monitor forces with CS; Apply global limits to modal corrections in CS	Johns, Filgueira
			Support actuators create excessive local stress	Critical	Occasional	5	Limit maximum actuator forces by hardware design to safe valued; Monitor forces with CS	Johns, Filgueira
			Thermal stresses due to loss of coolant, operator error, control system failure, exposure to Sun, and rapid temperature changes	Catastrophic	Occasional	4	Temperature monitoring of the glass and around the cell; Monitoring fans and cooling system; Differential temp sensors for ISS?; Sensors monitored when cell removed; Training and procedures	Johns, Sawyer
			Seismic event	Catastrophic	Probable	2	Design for maximum likely event earthquake	Johns
			Hardpoint failure – runaway, stuck breakaway, obstructed, bumped, load cell failure, flexure failure, roller screw or bearing seizes	Catastrophic	Occasional	4	Design for safety – breakaway, overtravel; CS monitoring of load cell forces; Load cell health monitoring by CS; Breakaway sensor; captive flexure; Limit force applied by motor; Routine inspection and maintenance	Johns
			Stuck/obstructed actuator – mechanical interference or assembly, moisture/ice, particulate	Critical	Remote	10	Design for safety; QA during assembly; Active monitoring by CS; Quality of compressed air (dryers and filters); POD filtering; Cleanliness of lines	Johns, Filgueira, Sawyer

Hazard Grading



Severity Probability	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

per MIL-STD-882D

Risk is re-evaluated after risk control measures are applied.

Quality Assurance

- The procedures used in the design and construction phases to ensure all the deliverables meet their specified requirements may be contained in a Quality Assurance Plan.
- Systems Engineering is responsible for managing and enforcing compliance with the QA plan.
- The subjects covered by the QA plan include:
  - Quality documentation
  - Quality in design and development
  - Software and controls quality
  - Reviews and audits
  - Inspection and testing
  - Non-conformance and corrective actions
  - Acceptance and delivery
- Reliability, Availability and Maintainability (RAM) process.
  - Addresses the ability of systems to perform their functions over their design life-times and be maintainable.

Technical Reviews

- Technical reviews function as gates to validate the work in progress and verify that technical and programmatic requirements are being met.
- Reviews with external members provide an opportunity to get outside input as to the practically of the proposed designs and their implementation.
- The number and protocol for reviews is usually chosen to be compatible with the funding agency's or other stakeholder's standard practice. In the USA that might be NASA, NSF or DOE or partner universities/research organizations.
- The review process is specified by Systems Engineering.
  - Protocol
  - Scope
  - Participants
  - Criteria for pass/fail
- Subsystem reviews roll up to System Level reviews conducted by Systems Engineering with Project Management oversight.
  - In some cases it may be convenient to combine subsystem and system reviews in the early stages (eg. Requirements).

Subsystem Technical Reviews

- Subsystem Level Reviews
  - Requirements Review
  - Preliminary Design Review (PDR)
    - Design and engineering studies are complete and demonstrate compliance with subsystem functional and performance requirements.
    - Verify level 3 flow-down of requirements.
    - Verify ICDs to other subsystems are complete.
  - Final Design Review (FDR) (also called Critical Design Review)
    - Subsystem design is complete and meets all functional and performance requirements including interface requirements.
    - Certify the subsystem is ready for construction.
  - Test and Verification Review (TVR)
    - Review all testing to be performed at the subsystem level and all other methods of verification for the subsystem requirements.
  - Pre-ship Review (PSR)/ Acceptance Review
    - Review all deliverable hardware and show requirements compliance as well as the meeting of all other contractual deliverables (drawings, documentation, meeting of ICDs, etc).

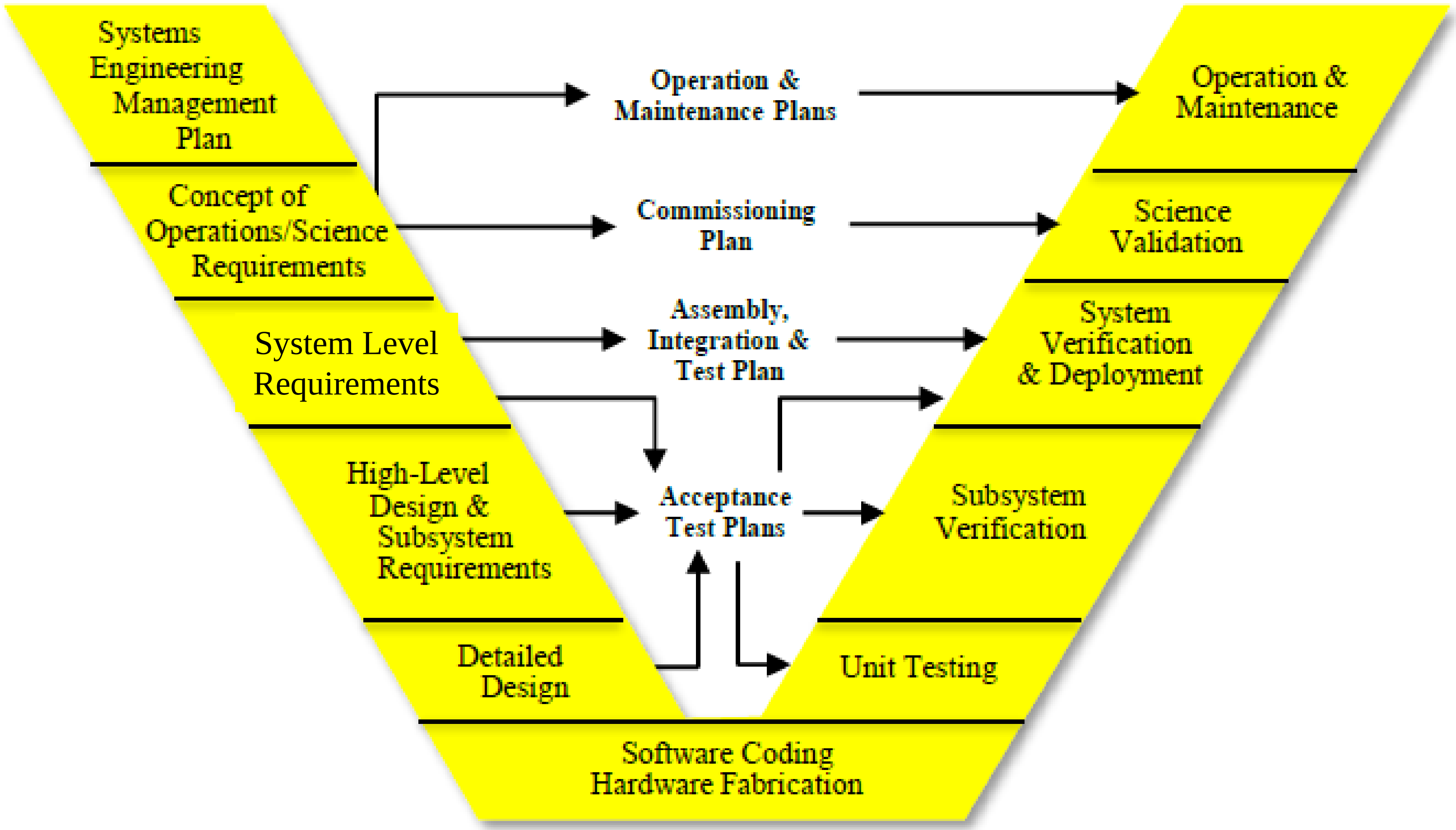
System Level Technical Reviews

- Conceptual Design Review (CoDR)
  - Trade studies and design have been conducted to arrive at a conceptual design for the telescope facility.
- System Requirements Review (SRR)
  - Validate the flow-down of requirements from the Science Requirements, Operations Concept, and Architecture to the System Level Requirements
- System Preliminary Design Review (SPDR)
  - Verify subsystem PDRs have been conducted with level 3 requirements flow-down
  - Interface control documents between subsystems are complete.
  - Delta-PDR may be required to address deficient items.
- System Integration and Test Review (SITR)
  - Verify that the on-site assembly, integration, test and commissioning of the telescope facility is complete and the system meets all requirements.
  - All deliverables are complete.
  - Identify remedial work needed to address non-compliances as a condition for final acceptance.
- Final Acceptance Review (FAR)
  - Certify that all remedial work has been completed and all deliverables to the stakeholders have been transmitted.

Integration and Commissioning Plan

- Telescope commissioning starts once the telescope is assembled and ready to acquire stellar images.
- The integration and commissioning of subsystems such as adaptive optics and science instruments starts after telescope commissioning has progressed to a certain stage of readiness where basic operation is possible.
- The work is described by a System Integration and Commissioning Plan (SICP) developed by Systems Engineering in collaboration with the Project teams.
- The SICP is compiled from subsystem ICPs that cover:
  - Required equipment and tools
  - Safety precautions for personnel and equipment
  - Step-by-step procedures to define the proper sequence of tasks
  - Test procedures to verify that the subassembly is functioning properly
  - Conditions that must be met by the GMT facility in order for integration to occur
  - Manpower requirements for both GMT and non-GMT personnel
  - Time estimates of tasks required
- The outcome of commissioning is a fully functional facility ready for final acceptance.

Development Process


Systems Engineering Management Plan
Concept of Operations/Science Requirements
System Level Requirements
High-Level Design & Subsystem Requirements
Detailed Design
Software Coding Hardware Fabrication
Unit Testing
Subsystem Verification
System Verification & Deployment
Science Validation
Operation & Maintenance
Operation & Maintenance Plans
Commissioning Plan
Assembly, Integration & Test Plan
Acceptance Test Plans

The standard Vee-diagram shows the various levels of requirements and the associated verification plans.

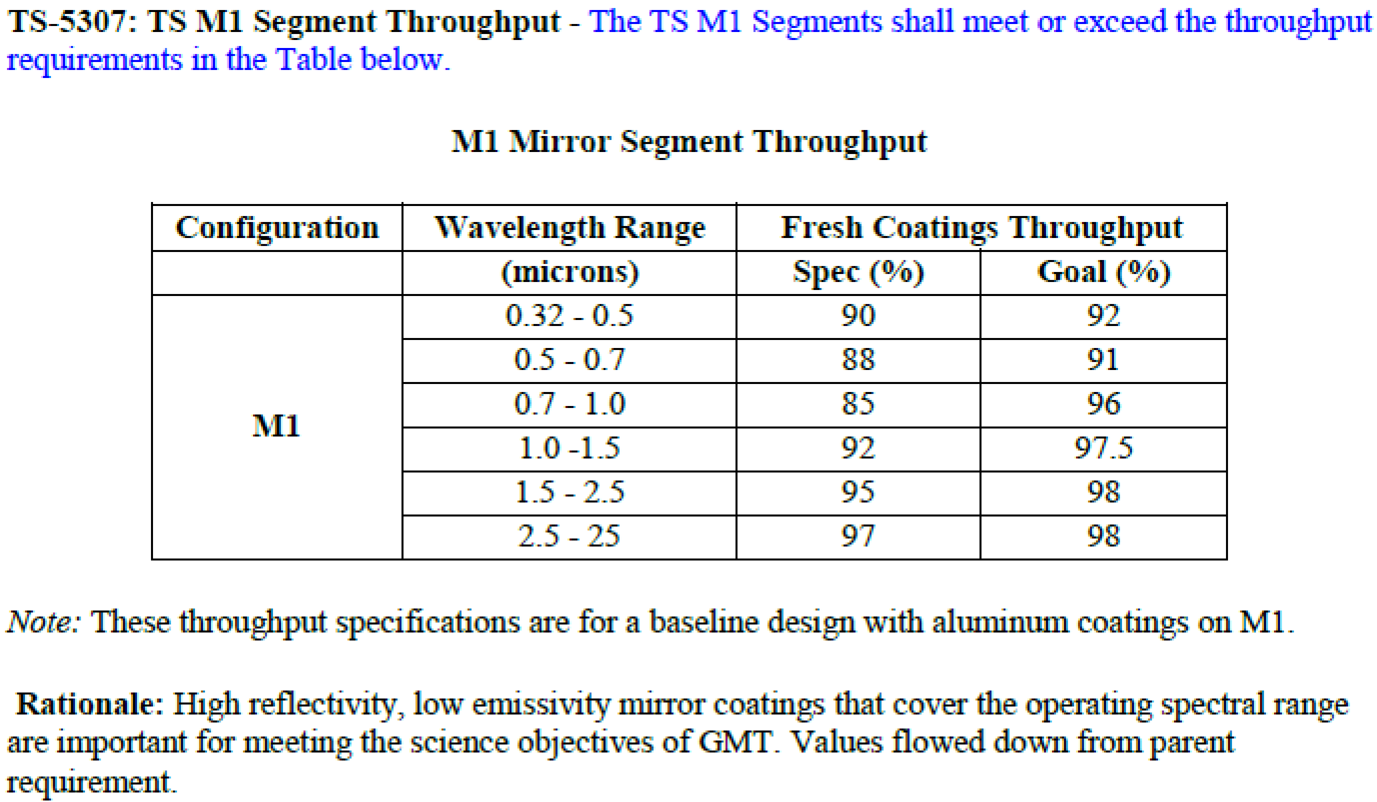
Student Assignment

- Be prepared to discuss the following topics:
  - What strategy would you use to create requirements for your project? Think about:
    - When is a specific requirement is needed?
    - What are the possible draw backs of specifying a requirement at too high a level?
    - What happens when a requirement is modified?
    - What happens when the architecture or operations concept upon which a requirement is based is modified, etc.?
    - What happens if a subassembly can’t satisfy its requirement or if there are conflicting requirements?
  - How would you decide what systems engineering procedures and level of SE detail is necessary and sufficient for your project?
  - Systems Engineering is said to be primarily about requirements but there are a lot more topics discussed in this section. How do they all tie together?

END OF SESSION 2

BACKUP SLIDES

Level 3 Telescope System Requirement Examples



TS-5307: TS M1 Segment Throughput - The TS M1 Segments shall meet or exceed the throughput requirements in the Table below.

M1 Mirror Segment Throughput

Configuration	**Wavelength Range**	**Fresh Coatings Throughput**	
	(microns)	**Spec (%)**	**Goal (%)**
M1	0.32 - 0.5	90	92
	0.5 - 0.7	88	91
	0.7 - 1.0	85	96
	1.0 -1.5	92	97.5
	1.5 - 2.5	95	98
	2.5 - 25	97	98

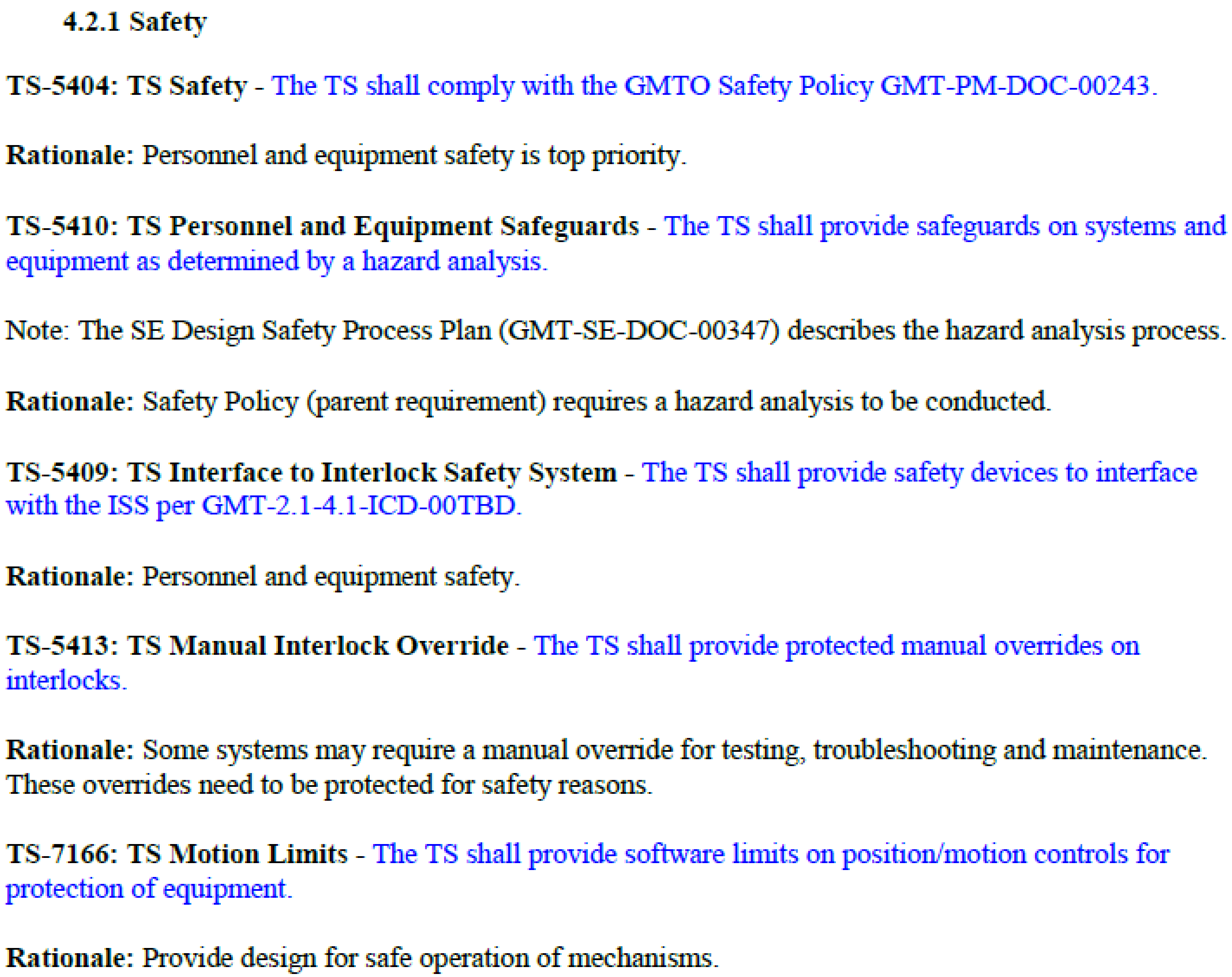
Note: These throughput specifications are for a baseline design with aluminum coatings on M1.

Rationale: High reflectivity, low emissivity mirror coatings that cover the operating spectral range are important for meeting the science objectives of GMT. Values flowed down from parent requirement.

- A **Goal** is a guide for the designer but is not a requirement for acceptance.

Excerpt from "Telescope System Requirements", GMT-TEL-REQ-000158-A"

Level 3 Telescope System Requirement Examples



4.2.1 Safety

TS-5404: TS Safety - The TS shall comply with the GMTO Safety Policy GMT-PM-DOC-00243.

Rationale: Personnel and equipment safety is top priority.

TS-5410: TS Personnel and Equipment Safeguards - The TS shall provide safeguards on systems and equipment as determined by a hazard analysis.

Note: The SE Design Safety Process Plan (GMT-SE-DOC-00347) describes the hazard analysis process.

Rationale: Safety Policy (parent requirement) requires a hazard analysis to be conducted.

TS-5409: TS Interface to Interlock Safety System - The TS shall provide safety devices to interface with the ISS per GMT-2.1-4.1-ICD-00TBD.

Rationale: Personnel and equipment safety.

TS-5413: TS Manual Interlock Override - The TS shall provide protected manual overrides on interlocks.

Rationale: Some systems may require a manual override for testing, troubleshooting and maintenance. These overrides need to be protected for safety reasons.

TS-7166: TS Motion Limits - The TS shall provide software limits on position/motion controls for protection of equipment.

Rationale: Provide design for safe operation of mechanisms.

Excerpt from "Telescope System Requirements", GMT-TEL-REQ-000158-A"