Shuttle Thermal Tile Processing Example Intent Specification

(Incomplete Draft (July 25, 2002): New versions will be placed at
http://sunnyday.mit.edu/ttps.pdf as more of the specification and analysis
is completed)

Nancy G. Leveson
Massachusetts Institute of Technology

Preface

This report contains an example *intent specification.*[1] Intent specifications are based on research in human problem solving and on basic principles of system theory. An intent specification differs from a standard specification primarily in its structure: The specification is structured as a set of models designed to describe the system from different viewpoints, with complete traceability between the models. The structure is designed (1) to facilitate the tracing of system-level requirements and design constraints down into detailed design and implementation, (2) to assist in the assurance of various system properties (such as safety) in the initial design and implementation, and (3) to reduce the costs of implementing changes and reanalysis when the system is changed, as it inevitably will be. Because of its basis in research on how to enhance human problem solving[2], intent specifications should enhance human processing and use of specifications and our ability to perform system design and evolution activities. Note that no extra specification is involved (assuming that projects produce the usual specifications), but simply a different structuring and linking of the information so that specifications provide more assistance in the development and evolution process.

There are seven levels in an intent specification (see Figure 1). Levels do not represent refinement, as in other more common hierarchical structures, but instead each level of an intent specification represents a completely different model of the same system and supports a different type of reasoning about it: Each model or level presents a complete view of the system, but from a different perspective. The model at each level is described in terms of a different set of attributes or language. Refinement and decomposition occurs *within* each level of the specification.

The top level (Level 0) provides a project management view and insight into the relationship between the plans and project development.

Level 1 of an intent specification is the customer view and assists system engineers and customers in agreeing on what should be built and whether that has been accomplished. It includes system goals, high-level requirements, design constraints, environmental assumptions, and system limitations.

The second level, System Principles, is the system engineering level and allows engineers to reason about the system in terms of the physical principles and laws upon which the system design is based.

---

[1] See Leveson, N.G. Intent Specifications: An Approach to Building Human-Centered Specifications, *IEEE Transactions on Software Engineering*, Vol. SE-26, No. 1, January 2000.

[2] See K.J. Vicente and J. Rasmussen. Ecological Interface Design: Theoretical foundations, *IEEE Trans. on Systems, Man, and Cybernetics*, vol 22, No. 4, July/August 1992.

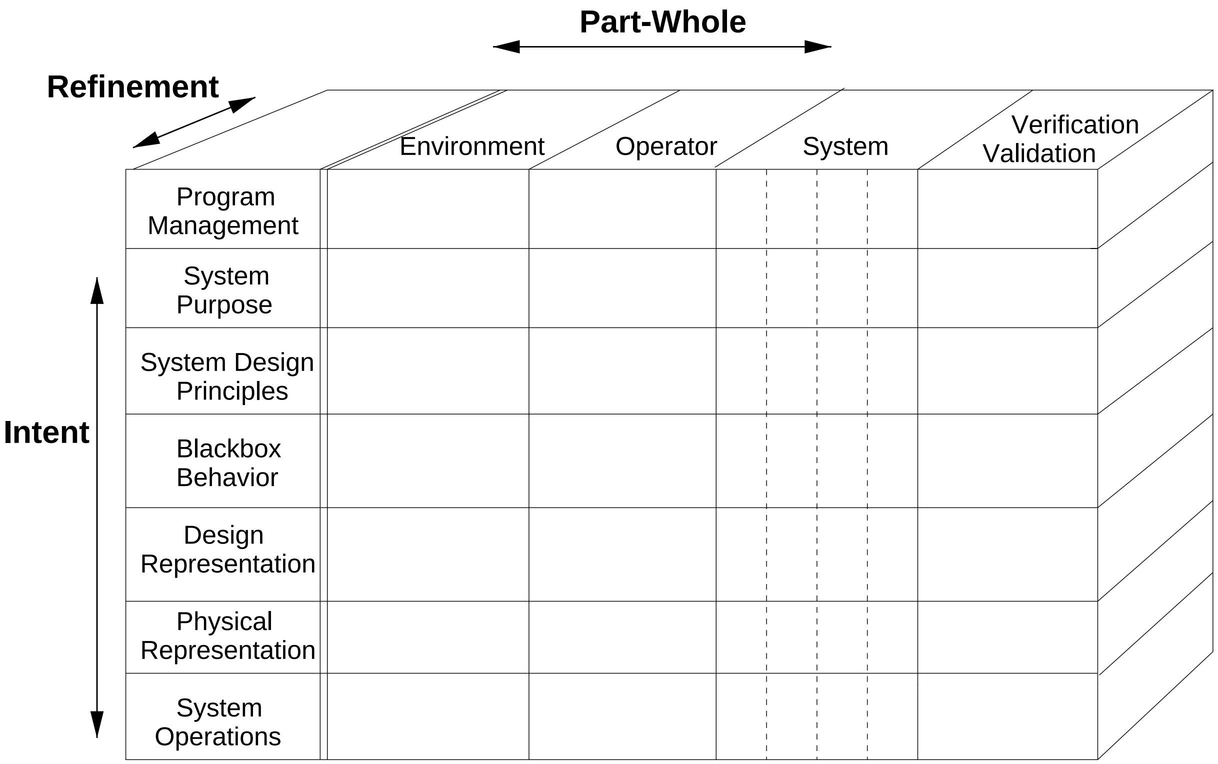


Figure 1: The Structure of an Intent Specification.

The third, or Blackbox Behavior level, enhances reasoning about the logical design of the system as a whole and the interactions between the components as well as the functional state without being distracted by implementation issues. This level acts as an unambiguous interface between systems engineering and component engineering to assist in communication and review of component blackbox behavioral requirements and to reason about the combined behavior of individual components using informal review, formal analysis, and simulation. The language used on this level, SpecTRM-RL, has a formal foundation so it can be executed and subjected to formal analysis while still being readable with minimal training and expertise in discrete math.

The next two levels provide the information necessary to reason about individual component design and implementation issues. Finally, the sixth level provides a view of the operational system.

Each level is mapped to the levels above and below it. These mappings provide the relational information that allows reasoning across the hierarchical levels and tracing from high-level requirements down to implementation and vice versa.

Intent information represents the design rationale upon which the specification is based. This design rationale is integrated directly into the specification. Each level also contains information about underlying assumptions upon which the design and validation is based. Assumptions are especially important in operational safety analyses. When conditions change such that the assumptions are no longer true, then a new safety analysis should be triggered. These assumptions may be included in a safety analysis document (or at least should be), but are not usually traced to the parts of the implementation they affect. Thus even if the system safety engineer knows that a safety analysis assumption has changed (e.g., the pacemakers are now being used on children rather than the adults for which the device was originally designed and validated), it is a very difficult and resource-intensive process to figure out which parts of the design used that assumption.

The safety information system or database is often separated from the development database and specifications. In the worst case, system and software safety engineers carefully perform analyses that have no effect on the system design because the information is not contained within the decision-making environment of the design engineers and they do not have access to it during system design. By the time they get the information (usually in the form of a critique of the design late in the development process), it is often ignored or argued away because changing the design at that time is too costly. Intent specifications integrate the safety database and information into the development specifications and database so that the information needed by engineers to make appropriate tradeoffs and design decisions is readily available.

Interface specifications and specification of important aspects of environmental components are also integrated into the intent specification as are human factors and human interface design. The separation of human interface design from the main system and component design can lead to serious deficiencies in each. Finally, each level of the intent specification includes a specification of the requirements and results of verification and validation activities of the information at that specification level.

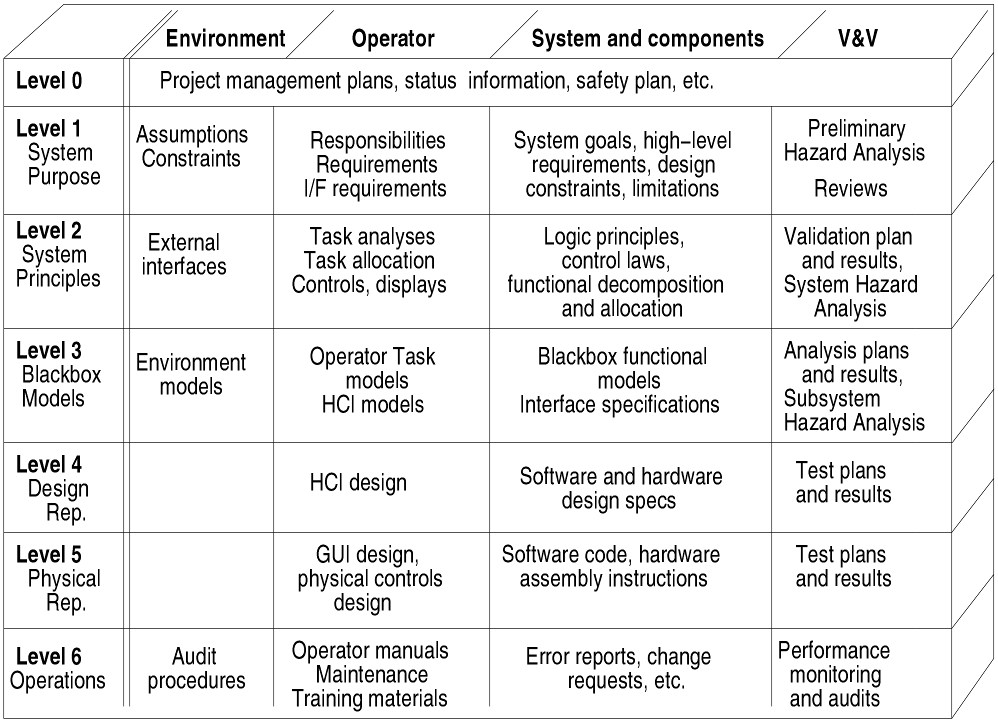
Although the contents of each level of an intent specification is not fixed and can vary according to the type of project and the views that are appropriate for it, Figure 2 show an example of what information might be found at each level of an intent specification for a typical complex system project.

In summary, intent specifications allow a seamless transition from system to component (including software) specifications and the integration of formal and informal aspects of system and software development. The specification structure facilitates the tracing of system level requirements and constraints into the design and the assurance of various system properties (such as safety) in the initial design and implementation as well as reducing the costs of implementing changes and reanalysis. While intent specifications should be helpful in ongoing project development and reducing development time (by assisting in early validation of design decisions and thus reducing rework), their most important advantages will be reaped during system evolution and sustainment. Their use should augment maintenance, troubleshooting, upgrades, operations, training, and the safety analyses needed to change the system without affecting risk.

Curtis *et al.*[3] did a field study of the requirements and design process for 17 large systems. They found that substantial design effort in projects was spent coordinating a common understanding among the staff of both the application domain and of how the system should perform within it. One of the characteristics they found that appeared to set exceptional designers apart from their colleagues was their knowledge of the application domain, and their ability to identify unstated requirements, constraints, or exception conditions and to to map between the behavior required of the application system and the computational

---

[3] B. Curtis, H. Krasner and N. Iscoe, A field study of the software design process for large systems, *Communications of the ACM*, 31(2): 1268–1287, 1988



	Environment	Operator	System and components	V&V
Level 0	Project management plans, status information, safety plan, etc.			
Level 1 System Purpose	Assumptions Constraints	Responsibilities Requirements I/F requirements	System goals, high-level requirements, design constraints, limitations	Preliminary Hazard Analysis Reviews
Level 2 System Principles	External interfaces	Task analyses Task allocation Controls, displays	Logic principles, control laws, functional decomposition and allocation	Validation plan and results, System Hazard Analysis
Level 3 Blackbox Models	Environment models	Operator Task models HCI models	Blackbox functional models Interface specifications	Analysis plans and results, Subsystem Hazard Analysis
Level 4 Design Rep.		HCI design	Software and hardware design specs	Test plans and results
Level 5 Physical Rep.		GUI design, physical controls design	Software code, hardware assembly instructions	Test plans and results
Level 6 Operations	Audit procedures	Operator manuals Maintenance Training materials	Error reports, change requests, etc.	Performance monitoring and audits

Figure 2: Sample Contents of an Intent ... cification.

structures that implement this behavior. This is exactly the information that is included in intent specifications.

Previously, I reorgani ed the government do cumentation on TCAS II (an airborne collision avoidance system) into an example intent specification. The specification following this preface is a second example, this time for a NASA robot. A difference this time is that development of the system occurred while building the intent specification (it was not reverse engineered).[4]

In this document, industry standard terminology is used where "shall" denotes a requirement, "may" denotes an option, ... "should" denotes ... constraint, and "will" ... assumption about the environment. ... cated by pointers, with subscripts denoting the page number on which the item can be found. An electronic version of this type of specification could use sophisticated hypertext links and multiple windows to denote these relationships.

The first number or letters of a link tells you what it is and where it is located:

$x.y$: Paragraph or entry y on Level x (where x is 0 to 6)

---

[4] The ... and positioning system, ... lo ok ing at the documentation for the software, I found it too complicated in some cases and too incomplete or inconsistent in others to understand. So I started the design of the software over from scratch and also changed some of the hardware and interfaces. Inconsistency is, of course, very hard to eliminate from any large system specification developed over a period of time. ... helpful ... to detect and eliminate ... stances of ... of the state-based model (Level 3) and the completeness and consistency chec ... also very helpful in this respect.

G: Goal (Level 1)
FR: Functional Requirement (includes performance)
EA: Environmental Assumption (Level 1)
OP: Operator behavioral requirement, assumption, or constraint (Level 1)
L: Limitation (Level 1)
C: Non-safety-related design constraint (Level 1)
SC: Safety-related design constraint (Level 1)
H: Hazard
HA-x: Line x of the Hazard Analysis.

Acknowledgements

Many people have reviewed this document or attempted something similar. Special thanks go to Israel Navarro, Iwao Hatanaka, David McLain, Jon Demerly, Steve Pickett, Mario Rodriguez, Jakob Kristina Hintersteiner, and I Lundqvist. [to be augmented]

Caveats

This specification is only an example. Although the idea for the example came from a CMU robot called Tesselator, the specification and design that appears here was redone from scratch and does not correspond to the current implementation or any past implementation of the real Tessellator robot.

In order to limit the amount of work required to produce the example (and the author's limited expertise in mechanical engineering), only MAPS (the robot mobility and positioning system) is emphasized in the specification. A complete specification for the entire Tessellator robot would simply contain more information (particularly at levels 2 and lower) about the other thermal tile processing functions.

Contents

Program Management Information

. [illegible] This section contains pointe

Program Management Plans

This section [illegible] contain pointe[illegible] [illegible] p[illegible] [illegible]ain

[illegible] [illegible] o [illegible] IEEE St[illegible] 1058 (d[illegible]

[illegible] p

1. Introduction
    1.1 Project Overview
    1.2 Project Deliverables
    1.3 Evolution of the Software Project Management Plan
    1.4 Reference Materials
    1.5 Definitions and Acronyms
2. Project Organization
    2.1 Process Model
    2.2 Organizational Structure
    2.3 Organizational Boundaries and Interfaces
    2.4 Project Responsibilities
3. Managerial Process
    3.1 Management Objectives and Priorities
    3.2 Assumptions, Dependencies, and Constraints
    3.3 Risk Management (1.5(35), 1.6(41))
    3.4 Monitoring and Controlling Mechanisms
    3.5 Staffing Plan
4. Technical Process
    4.1 Methods, Tools, and Techniques
    4.2 Software Documentation
    4.3 Project Support Functions
5. Work Packages, Schedule, and Budget
    5.1 Work Packages
    5.2 Dependencies
    5.3 Resources Requirements
    5.4 Budget and Resource Allocation
    5.5 Schedule

System Safety Plan

[illegible]

[illegible] (SSPP) [illegible]

[illegible]

I. General Considerations
  A. Introduction
  B. Scope and Purpose
  C. Objectives
  D. Applicable Standards
  E. Progress Reporting
  F. Documentation and Reports
II. System Safety Organization
  A. Personnel Qualifications and Duties
  B. Functional Organization
  C. Staffing and Manpower
  D. Communication Channels
  E. Responsibility, Authority, and Accountability
  F. Subcontractor Responsibilities
  G. Coordination
  H. System Safety Groups System Safety Working Groups
  I. Safety Program Interfaces with Other Disciplines
    Reliability

    Maintainability
    Design and System Engineering
    Software Development
    Configuration Management
    Quality Assurance
    Human Factors
    Test
    Industrial Safety

III. System Safety Program Schedule
  A. Critical Checkpoints and Milestones
  B. Start and Completion Dates of Tasks, Reports, Reviews
  C. Review Procedures and Participants

IV. System Safety Criteria
  A. Definitions (15, 35)
  B. Identification and Dissemination
  C. Classification/Ranking of Hazards (15, 35)
    Hazard Severity Categories
    Hazard Probability Levels
    Risk Assessment
  D. System Safety Precedence
  E. Safety Design Criteria
    Hardware
    Software
  F. Special Contractual Requirements

V. Safety Data
  A. Data Requirements
    Deliverable
    Non-deliverable
  B. Hazard Tracking and Reporting System
  C. Safety Requirements and Data
    Hazard Data Collection
    Lessons Learned
    Safety Documentation and Files (Data Library)
    Records Retention

VI. Hazard Analyses (Types, Documentation, and Expected Uses)
  A. Preliminary Hazard Analysis (16, 41)
  B. System Hazard Analyses (8, 11, 97)
  C. Subsystem Hazard Analyses (including Software Hazard Analyses) (35)
  D. Operating System Hazard Analyses (15)
  E. Integration of Subcontractor Analyses with Overall System Hazard Analyses
  F. Tracing System Hazards into Subsystems (15, 35)

VII. Verification
  A. Safety-Related Testing (26, 35)
  B. Special Demonstrations

- C. Review and Feedback Procedures

VIII. Audit Program (16, 26.3)

IX. Operations

- A. Emergency and Contingency Procedures (19 2(79))
- B. Configuration Control Activities
- C. Training (15 2)

X. Hazard and Incident Reporting and Investigation During Operations (16)

XI. Special Safety Activities

- A. Range Safety
- B. Facility Safety
- C. Explosives Safety
- D. Nuclear Safety
- E. Chemical and Biological Safety

Level 1

System-Level Goals, Requirements, Constraints

The [illegible] intent speci [illegible] fication contains t [illegible] , [illegible] [illegible] nst [illegible] lin [illegible] ns o [illegible] t [illegible] es, [illegible] n an [illegible] ities [illegible] s p [illegible] na [illegible] na

Le [illegible] is t [illegible] to [illegible] nt [illegible] [illegible] tiona [illegible] . [illegible] [illegible] tiona [illegible] onst [illegible] s at [illegible] intent

N [illegible] t [illegible] fication [illegible] ot [illegible] A [illegible] g [illegible] s [illegible] [illegible] p [illegible] a [illegible] n [illegible] o [illegible] op to [illegible] as [illegible] isions a [illegible] Th [illegible] intent spe [illegible] ions [illegible] v [illegible] tion o [illegible] s [illegible] in [illegible] ne [illegible] in [illegible] s.

Note [illegible] tent [illegible] pe [illegible] c [illegible] stea [illegible] nt enti [illegible] t [illegible] o [illegible] . [illegible] cent u [illegible] pt [illegible] Le [illegible] ation is on [illegible] to [illegible] ee [illegible] pt [illegible] s

1.1 Introduction

(The following description is adapted from *[illegible]*, R. Bennett, ckwell, T. Graham, S. Gatrall, R. O'Toole, and H. Schempf. The original Tessellator robot was designed as a research project in the Robotics Dept. at CMU with NASA funding. This specification was derived from one that students pursuing a master's degree created for a project at the SEI. Changes have been made from the original specification in order to satisfy our different goals.)

The Thermal Tile Processing System (TTPS) is designed to service tiles (the thermal protection system) on the Space Shuttle, thus saving humans from a laborious task that begins within minutes after the Shuttle lands and ends just prior to the launch—typically three four months. Upon landing at either the Dryden facility in California or Kennedy Space Center in Florida, the orbiter is brought to either the Mate-Demate Device (MDD) or the Orbiter Processing Facility (OPF). These large structures provide access to all areas of the orbiters.

The Shuttle is covered with several types of heat resistant tiles that protect the orbiter's aluminum skin during the heat of reentry. While the majority of the upper surfaces are covered with flexible insulation blankets, the lower surfaces are covered with silica tiles. These tiles have a glazed coating over soft and highly porous silica fibers. The tiles are 95% air by volume which makes them extremely light but also makes them capable of absorbing a tremendous amount of water. Water in the tiles causes a substantial weight problem that can adversely affect launch and orbit capabilities for the shuttles. Because the orbiters may be exposed to rain during transport and on the launch pad, the tiles must be waterproofed. This task is accomplished through the use of a specialized hydrophobic chemical, DMES, which is injected into each and every tile. There are approximately 17,000 lower surface tiles covering an area that is roughly 25m x 40m.

In the current process, DMES is injected into a small hole in each tile by a handheld tool that pumps a small quantity of chemical into the nozzle. The nozzle is held against the tile and the chemical is forced through the tile by a pressurized nitrogen purge for several seconds. The nozzle diameter is about 1 cm but the hole in the tile surface is about 0.1 cm. The heights range from 290 cm to 400 cm from the floor of the OPF. It takes about 240 person hours to rewaterproof the tiles on an orbiter. Because the chemical is toxic, human workers have to wear heavy suits and respirators while injecting the chemical and, at the same time, maneuvering in a crowded work area. One goal for using a robot to perform this task is to eliminate a very tedious, uncomfortable, and potentially ha activity.

The tiles must also be inspected. By inspecting the tiles more accurately than the human eye, it is hoped that the Thermal Tile Servicing System will reduce the need for multiple inspections. During launch, reentry, and transport, a number of defects can occur on the tiles. These defects are evidenced as scratches, cracks, gouges, discoloring, and erosion of surfaces. The tiles are examined for such defects to determine if they warrant replacement, repair, or no action. The typical procedure involves visual inspection of each tile to see if there is any damage and then assessment and categorization of the defects according to detailed checklists. Then, work orders are issued for repair of individual tiles.

The TTPS has three main parts: a mobile robot, a separate (off-board) computer (called the Workcell Controller) that controls the overall thermal tile processing tasks, and a human operator to monitor and control the other two components.

The mobile robot is designed to inspect each tile and inject the waterproofing chemical. Because there are so many tiles, the robot divides its work area into uniform work spaces, inspecting tiles in each area with as little overlap between work spaces as possible.

Before each inspection shift, the operator enters instructions into the Workcell Controller about shuttle position and inspection sequence. The Workcell Controller workstation creates jobs for the mobile robot and updates other NASA databases after the robot uploads data gathered during the course of the shift. This data includes tile images, records of tiles injected and inspected, and other pertinent job data. In addition, robot status data is used to monitor robot operation.

At the beginning of the shift, the mobile robot is downloaded a job. The job consists of a series of files describing the locations, sequences, target IDs, orbiter parking measurements, etc. The robot then uses a rotating laser to position itself under the shuttle, and the robot's camera locates the exact tile to be inspected. Because the shuttle's belly is not flat, the robot customizes its upward movement to each tile: Two vertical beams on either side of the robot raise the manipulator arm, which holds the injection tools and camera. A smaller lifting device raises the arm the rest of the way.

By comparing the current state of each tile with the state of the tile at previous inspections, the mobile robot characterizes anomalies in tiles as cracks, scratches, gouges, discoloring, or erosion. The robot also indicates when it is unsure what is wrong with a tile, so the supervisor can reexamine the tile on the screen of the Workcell Controller. At the end of a shift, the robot's updated tile information is entered into existing NASA databases.

On board, computers control the mobile robot's high-level processing tasks while low-level controllers and amplifiers direct arm and wheel motions. Two more computers control the robot's vision and injection systems. If anything goes wrong—rising compartment temperatures, low battery level, or other changes—safety circuits will shut the robot down.

MAPS (the mobility and positioning system) issues movement commands to the motor controller, which directs the wheel motors on the mobile base. MAPS in turn is controlled either by the operator or an on-board computer called the Tile Servicing Subsystem (TSS). The operator controls robot movement and positioning using a hand-held joystick. The TSS controls robot movement and positioning by providing MAPS with a specification of the destination and route.

The mobile base is unstable when the manipulator arm is extended, so stabilizer legs are used to provide stability. These legs must be retracted when the robot is in motion.

1.2 Historical Information

We know of no previous robots used to service the orbiter thermal protection system nor of any attempts to build such a robot. Although the CMU Tessellator robot was delivered to NASA in 1994, as far as we know it has not been used in Shuttle operations. We have changed the design from the original in order to enhance safety and to make it a better example for our purposes.

1.3 Work Area (Environment) Assumptions

EA1 The work areas of the Orbiter Processing Facility can be very crowded. The facilities provide access to all areas of the orbiters through the use of intricate platforms that are laced with plumbing, wiring, corridors, lifting devices, etc. After entering the facility, the orbiters are jacked up and leveled. Substantial structure then swings around and surrounds the orbiter at all sides and at all levels. With the exception of the jackstands that support the orbiters, the floor space directly beneath the orbiter is initially clear but the surrounding structure can be very crowded.

EA2 The mobile robot must enter the facility through personnel access doors 1.1 m (42") wide. 5') The platforms allow a length of 2. There are some structural beams whose heights are as low as 1. ce under the orbiter the tile heights range from about meters to 4 meters 2. Thus the compact roll-in form of the mobile system must maneuver these spaces and also raise its inspection and injection equipment up to heights of ch individual tiles while still meeting the 1 mm accuracy requirements (→ MB-FR3$_{(20)}$, MB-C1$_{(20)}$, MB-SC1$_{(20)}$).

EA3 Additional constraints involve moving around the crowded workspace. The robot must negotiate jackstands, columns, workstands, cables, and hoses. In addition, there are hanging cords, clamps, and hoses. Because the robot might cause damage to the ground obstacles, cable covers will be used for protection and the robot system must traverse these covers (→ MB-FR2$_{(19)}$).

1.4 Thermal Tile Processing System: Goals, Requirements, and Constraints

[illegible] not speci[illegible] [illegible] The[illegible] speci[illegible]fy [illegible] [illegible]sion to [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] itations on potentia[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]

Goals of the Thermal Tile Processing System (TTPS)

1. Inspect the thermal tiles for damage caused during launch, reentry, and transport.
2. Apply waterproofing chemicals to the thermal tiles.

Functional Requirements

TTPS-FR1 The TTPS shall inspect each tile to identify tiles with defects.

TTPS-FR2 The TTPS shall assess and categorize each defect identified.

TTPS-FR3 The TTPS shall inject DMES into each tile.

Design Constraints

TTPS-EC1 Use of the TTPS must not negatively impact the flight schedules of the orbiters more than that of the manual system being replaced.

TTPS-EC2 Maintenance costs of the TTPS must not exceed TBD dollars per year.

TTPS-SC1 Use of the TTPS must not cause or contribute to an unacceptable loss (accident) as defined by Shuttle management (35).

TTPS Components

The Thermal Tile Processing System has components located in the control room and on a mobile robot (see Figure 1.3). These components operate together to achieve the system functional requirements and to satisfy the design constraints.

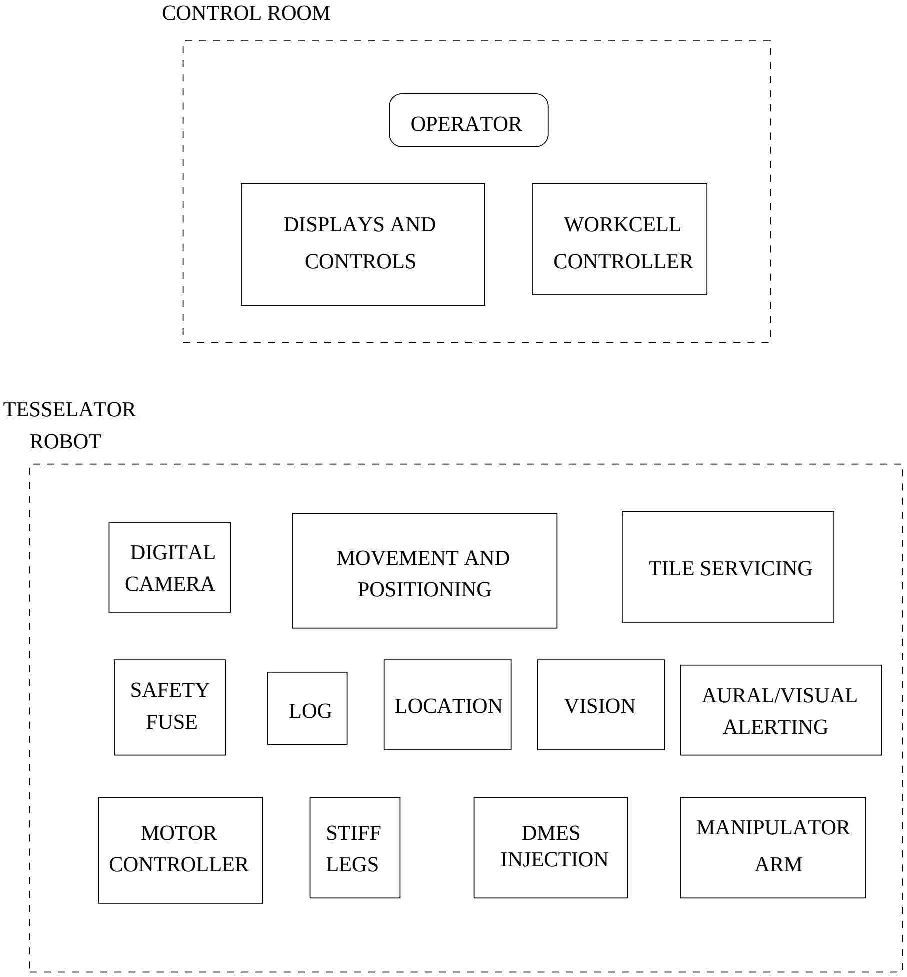


Figure 1.3: Components of the TTPS

1.4.1 Workcell Controller (WCC) Requirements and Constraints

Goals

Control the overall thermal tile processing performed by the mobile robot.

Requirements

WCC-FR1 The WCC shall download tile data from the NASA database for the mobile robot to use during a shift.

WCC-FR2 The WCC shall create jobs (instructions) for the mobile robot.

WCC-FR3 The WCC shall monitor robot operation to ensure tasks are completed.

WCC-FR4 At the end of a shift, the WCC shall update the NASA database with tile images, records of tiles injected and inspected, and other pertinent job data TBD

Safety-Related Design Constraints

WCC-SC1 The job (instructions) provided to the mobile robot must not result in any tiles being missed in the inspection or waterproofing process (→H8$_{(40)}$).

1.4.2 Mobile Robot

The mobile robot consists of a mobile base carrying a tile servicing subsystem, a mobility and positioning subsystem, a location subsystem, a motor controller, a digital camera, a manipulator arm, a DMES injection subsystem, a vision subsystem, a system log, and several safety subsystems included simply to provide safety functions including a safety fuse, a proximity-sensor, and an alerting subsystem.

1.4.2.1 Mobile Base (MB)

Goals

Support, contain, and transport the tile servicing equipment.

Requirements

MB-FR1 The mobile base shall be able to carry all the mobile robot subsystem components (↓2.6.3$_{(73)}$).

MB-FR2 The mobile base shall be able to move smoothly in any direction and to cross cable covers on the floor (←EA3$_{(15)}$) (→H3$_{(38)}$), (↓2.6.2$_{(73)}$).

MB-FR3 The mobile base shall be able to raise its inspection and injection equipment to the level required for servicing the tiles, from 2.9 meters to 4 meters ($\leftarrow$EA2$_{(15)}$) ($\downarrow$2.6.3$_{(73)}$, 2.10.1$_{(81)}$, 2.10.4$_{(81)}$).

Design Constraints

MB-C1 The mobile base must be no more than 2.5 meters long and 1 meter wise. While moving, it must fit under structural beams as low as 1.75 meters ($\leftarrow$EA2$_{(15)}$), ($\downarrow$4.6).

Safety-Related Design Constraints

MB-SC1 The mobile base must be able to ensure accuracy of 10 cm for positioning and 1 mm for tile servicing (inspection and injection) tasks. ($\leftarrow$EA2$_{(15)}$, $\rightarrow$H4$_{(38)}$, $\downarrow$2.6.1$_{(73)}$, 2.6.4$_{(73)}$)

MB-SC2 The mobile base design must protect against fire and explosion. ($\rightarrow$H6$_{(39)}$, $\downarrow$2.6.5$_{(73)}$, 2.6.6$_{(73)}$)

MB-SC3 It must be possible to move the mobile base out of the way in case of an emergency ($\downarrow$2.9.2$_{(79)}$).

1.4.2.2 Tile Servicing Subsystem

Goals

Direct and coordinate all tile servicing operations, including the positioning of the manipulation arm, the operation of the vision subsystem, and the operation of the DMES injection system.

Direct movement of the mobile base to the correct position for tile servicing.

Requirements

TSS-FR1 The TSS shall plan the course of action required to complete a given task.

- **TSS-FR1.1** The TSS shall raise the manipulator arm to the location of the tile to be serviced ($\downarrow$2.10.3$_{(81)}$).
- **TSS-FR1.2** The TSS shall inspect each tile and identify damaged tiles using the vision subsystem ($\downarrow$2.12.1$_{(85)}$)
  - **TSS-FR1.2.1** The TSS shall compare the current state of each tile with the state of the tile at previous inspections.
  - **TSS-FR1.2.2** The TSS shall characterize anomalies in tiles as cracks, scratches, gouges, discoloring, or erosion.
  - **TSS-FR1.2.3** The TSS shall indicate if unsure what is wrong with a tile so the operator can reanalyze the tile on the screen of the workcell controller.

TSS-FR1. The TSS shall command the operation of the DMES injection subsystem (↓2.11.1$_{(83)}$).

TSS-FR2 The TSS shall determine the next work location and the most optimal route of travel to it while avoiding obstacles

TSS-FR2.1 The TSS shall inform the operator about the next desired work zone location (↓2.1.1$_{(49)}$, 2.2.3$_{(58)}$).

TSS-FR2.2 When the mobility and positioning system is being commanded by the on-board TSS, it shall provide the route of travel and a destination. Locations shall be provided in world coordinates (↓2.1.1$_{(49)}$, 2.4.2.6$_{(62)}$, 2.4.5.3$_{(64)}$).

Rationale: For safety reasons, the operator is responsible for mobile base movement. However, to allow for potential autonomy and thus more efficient operation, the TSS can directly issue movement commands to the mobility and positioning subsystem. Any TSS movement commands must be monitored by the operator.

TSS-FR2. The TSS shall determine whether an adequate location has been achieved before beginning any tile servicing operations (↓2.4.5.1$_{(63)}$, 2.1.1$_{(49)}$).

Safety-Related Design Constraints

TSS-SC1 The TSS must not move the manipulator arm unless the vision system is operational (→H4$_{(38)}$).

TSS-SC2 The TSS must not command the manipulator arm into contact with any object unless required for servicing (→H4$_{(38)}$).

TSS-SC3 Chemicals must not be injected without providing a warning to humans in the area (→H7$_{(40)}$).

TSS-SC4 The injection system must not be operated unless the mobile base is stopped in the work zone and the manipulator arm has moved the injection tool to the proper tile (→H7$_{(40)}$).

1.3.4 Mobility and Positioning (MAPS)

Goals

Control the movement of the robot around the work area and position it in the appropriate locations in the hangar so the tiles can be serviced (→MAPS-FR1$_{(22)}$).

Navigate according to commands from an operator-controlled, hand-held joystick or according to routes and destinations provided by the on-board tile servicing subsystem (→MAPS-FR2$_{(22)}$, MAPS-FR3$_{(23)}$, MAPS-FR4$_{(23)}$, TSS-FR2.2$_{(21)}$, OP5$_{(32)}$).

Assumption All robot base movement will be commanded from outside MAPS, either by the computer TSS or the operator.

Control robot base stabilization and provide movement warnings (→MAPS-FR5$_{(23)}$, MAPS-FR6$_{(23)}$).

Store information about the operation of MAPS and the mobile robot as a whole (→MAPS-FR7$_{(23)}$).

> **Rationale:** The recording of a variety of performance data will enable NASA system engineers to fine tune the operation of the robot and its software and also assist in maintenance and operational audits.

Requirements

MAPS-FR1 MAPS shall generate motor control commands to maneuver the robot to the zones required for the current job session (←MAPS-G1$_{(21)}$) (↓2.4.5.4$_{(65)}$, 2.4.6.3$_{(67)}$).

MAPS-FR2 MAPS shall provide a computer-controlled mode of operation (Computer Mode) where routes and destination are provided by the on-board TSS (←MAPS-G2$_{(21)}$) (↓2.4.5$_{(63)}$).

> **Assumption:** Computer mode of operation will be used only under operator oversight. More efficient movement, particularly in tight spaces, can be commanded by the computer (compared to a joystick).
>
> **Rationale:** Human control of MAPS throughout the long and tedious tile servicing process (which takes several weeks) is impractical. In addition, more efficient movement, particularly in tight spaces, can be commanded by the computer (compared to a joystick). Sufficient confidence, however, cannot be obtained in the automated implementation of some safety-related robot operations (like detecting a passerby or an unexpected obstacle in the path of the robot), and therefore human movement control will be used during some limited but particularly hazardous operations.

MAPS-FR2.1 MAPS shall accept a set of target positions and final destination from the TSS and shall generate appropriate commands to the motor controller to direct the robot base to the final destination position via the intermediate target positions (↓2.4.5.4$_{(65)}$).

MAPS-FR2.2 MAPS shall notify the TSS and the user interface when a satisfactory zone has been achieved or when it has failed to complete a commanded move and the reason for any failure (↓2.4.5.3$_{(64)}$, 2.4.5.4.2.2.2$_{(66)}$, 2.4.5.5$_{(66)}$).

MAPS-FR2.3 Maps shall move into the Computer mode of operation in response to an appropriate message from the operator (→H1$_{(36)}$) (↓2.1.3$_{(51)}$, 2.4.7.3$_{(68)}$).

MAPS-FR2.4 While in Computer Mode, all joystick deflections shall be ignored. The operator shall be informed when this occurs (→H1$_{(36)}$, MAPS-SC1$_{(24)}$) (↓2.4.5.5$_{(66)}$, 2.4.7.3$_{(68)}$).

Rationale This requirement is included to prevent inadvertent joystick deflection from affecting robot movement. For example, if the operator is holding down the deadman switch on the joystick and his or her arm is jostled by an external force.

MAPS-FR2.2 Upon receipt of a command to change from Computer to Operator mode, MAPS shall stop all motion and begin operation in Operator mode (↓2.4.7.2$_{(68)}$).

MAPS-FR3 MAPS shall provide an operator-controlled mode of operation (Operator Mode) where movement is commanded via a joystick (←MAPS-G2$_{(21)}$) (↓2.4.6$_{(66)}$).

Rationale Operator control is safer when environmental conditions are uncertain or in a particularly hazardous state (e.g., there are people in the area where MAPS is moving). Manual control will also be used during routine maintenance operations.

MAPS-FR3.1 MAPS shall default to Operator Mode at powerup or after any type of temporary shutdown or movement inhibition (such as from the safety fuse) (↓2.4.2.2$_{(61)}$, 2.4.7.2$_{(68)}$, 2.4.5.4.1$_{(65)}$).

MAPS-FR3.2 In Operator Mode, MAPS shall be commanded corresponding to the position of the joystick (↓2.2.2$_{(57)}$, 2.4.6.3$_{(67)}$).

MAPS-FR3.3 MAPS shall be able to respond to either single joystick motion commands or to any combination of commands (↓2.4.2.4$_{(62)}$).

MAPS-FR3.4 While in Operator Mode, all movement messages from the TSS shall be ignored (↓2.4.7.2$_{(68)}$, 2.4.5.5$_{(66)}$).

MAPS-FR4 MAPS shall determine robot position using the Location System (←MAPS-G3$_{(22)}$) (↓2.4.3$_{(62)}$).

MAPS-FR5 MAPS shall control the deployment and retraction of the stabilizer legs (←MAPS-G3$_{(22)}$) (↓2.4.4$_{(63)}$).

MAPS-FR6 MAPS shall control the activation and deactivation of the aural and visual alert system (←MAPS-G3$_{(22)}$, AS-FR2$_{(31)}$) (→H1$_{(36)}$) (↓2.4.2.1$_{(61)}$, 2.17$_{(95)}$).

MAPS-FR7 MAPS shall send messages to the system log about all events and errors related to MAPS operation (←MAPS-G4$_{(22)}$) (↓2.4.8$_{(69)}$).

Design Constraints

MAPS- C1 Tolerances for movements must be modifiable after delivery (↓2.4.5.4.2$_{(65)}$).

MAPS- C2 Acceleration or deceleration when starting or stopping motion under normal circumstances must be low to allow a smooth start and a smooth stop at the destination (↓2.4.2.3$_{(62)}$, 2.4.5.2$_{(63)}$, 2.9.7$_{(80)}$). (But see safety constraint MAPS-SC2.2$_{(25)}$ below.)

Rationale: The goal of this constraint is to minimize wear on the physical parts of the robot and thus to reduce maintenance time and cost. However, it conflicts with safety constraint MAPS-SC2.2 below and the tradeoffs must be considered in the system engineering process.

MAPS-C3 Mobile base acceleration, deceleration, and velocity must be modifiable after delivery (↓2.1.4$_{(51)}$, 2.4.2.3$_{(62)}$, 2.4.6.3.1$_{(67)}$).

Rationale: The appropriate units of acceleration and deceleration must be determined through trial and error. In addition, hardware changes in the robot or temporary or permanent operational changes in the OFP and the OFP environment could require changes to these values in the future.

Safety-Related Design Constraints

MAPS-SC1 The mobile base must move only when commanded by the operator or when commanded by the TSS and approved by the operator (→H1$_{(36)}$) (←MAPS-FR2.5$_{(23)}$).

MAPS-SC1.1 MAPS must not enter Operator Mode unless the joystick is physically connected to the robot and the joystick is in the neutral position (↓2.4.6.1$_{(66)}$).

MAPS-SC1.2 The robot must not move unless the deadman switch is depressed (↓2.4.2.1$_{(61)}$, 2.4.5.4.1$_{(65)}$, 2.4.6.3.3$_{(67)}$).

MAPS-SC1.2 If the operator releases the deadman switch and then later depresses it again, all previous commands must be ignored and a new command must be issued before any robot movement occurs (↓2.4.2.5$_{(62)}$, 2.4.7.3$_{(68)}$, 2.4.5.4.1$_{(65)}$).

Rationale: A long enough time may exist between releasing the deadman switch and depressing it again that the environment may have changed and previous commands may no longer be safe.

MAPS-SC1.4 When the safety fuse is in the HALT state, the mobile base must not be capable of performing any kind of movement (→H1$_{(36)}$, H5$_{(39)}$).

MAPS-SC1.4.1. MAPS must not begin movement if the safety fuse is in the Halt state or if the state of the safety fuse is unknown (↓2.4.2.1$_{(61)}$).

MAPS-SC1.4.2. MAPS must stop all movement and notify the operator if the safety fuse goes into the Halt state during a move or if the state of the safety fuse is not determinable (↓2.4.2.2$_{(61)}$, 2.4.5.4.3$_{(66)}$).

MAPS-SC1.6. MAPS must reinitialize itself and all the subsystems it controls when the safety fuse changes from HALT to SAFE state. Any previous uncompleted movement commands must be discarded (↓2.4.7.1$_{(68)}$, 2.4.7.4$_{(69)}$).

Rationale: The system may be nonoperational for a long time while the problem that triggered the safety fuse is being identified and fixed. When the system is restarted, the environment around the robot may have changed and the previous movement commands may be inappropriate.

MAPS-C2 The mobile base must stop when commanded (→H1$_{(36)}$).

> **MAPS-C2.1** Release of the deadman's switch must cause the robot to cease motion. Motion must remain disabled until the switch is depressed again (↓2.4.2.2$_{(61)}$, 2.4.5.4.3$_{(66)}$, 2.2.1.3$_{(57)}$).
>
> **MAPS-C2.2** When the operator releases the deadman switch, the robot must decelerate quickly to avoid rolling into the obstacle the operator is trying to avoid (↓2.2.1.3$_{(57)}$, 2.4.5.2$_{(63)}$, 2.4.2.3$_{(62)}$, 2.9.7$_{(80)}$).
>
> > **Rationale:** The operator is tasked to release the deadman switch during a move when the robot is about to impact an obstacle. Rapid deceleration is required to avoid rolling into the obstacle the operator is trying to avoid. However, such rapid deceleration is hard on the robot mechanisms (see MAPS-C2 above) and should be used only when necessary to avoid a hazardous condition.
> >
> > **Assumption:** The maximum allowed velocity of the robot shall be such that the robot will come to a stop 0.5 seconds after releasing the deadman button (←MC-SC1$_{(27)}$, MC-SC2$_{(27)}$, Con5$_{(33)}$, Con6$_{(33)}$).
>
> **MAPS-C2.3** If the robot is in Operator Mode and the joystick is returned to the neutral position, all robot motion must cease (↓2.4.6.3.3$_{(67)}$).

MAPS-C3 The mobile base must not be commanded to an occupied position (→H1$_{(36)}$).

> **MAPS-C3.1** The operator must be kept informed of the location of the robot and of obstacles in the work area (↓2.4.2.2$_{(61)}$, 2.4.3.2$_{(63)}$, 2.4.5.1$_{(63)}$, 2.4.6.1$_{(66)}$).
>
> **MAPS-C3.2** Human override capability must be maintained at all times in either operating mode (↓2.4.2.2$_{(61)}$, 2.4.5.4.3$_{(66)}$, 2.4.6.3.3$_{(67)}$).
>
> **MAPS-C3.3** When operating in Computer Mode, MAPS must notify the user interface of the direction and route of a move and must require operator permission before commencing motion (↓2.4.5.4.1$_{(65)}$).

MAPS-C4 The manipulator arm must move only when the stabilizers are fully extended (→H3$_{(38)}$).

> **MAPS-C4.1** MAPS must ensure that the stabilizers are fully extended prior to enabling manipulator arm movement. (↓2.4.4.2$_{(63)}$).

MAPS-C5 The mobile base must not move when the stabilizers are extended (→H2$_{(37)}$).

> **MAPS-C5.1** The stabilizers must be retracted prior to commencing motion (↓2.4.2.1$_{(61)}$, 2.4.4.1$_{(63)}$).
>
> **MAPS-C5.2** If stabilizer retraction or deployment fails, MAPS must notify the Operator and the TSS of the failure (↓2.4.4.3$_{(63)}$).

MAPS-S C3.5 Wheel motors must be turned off while the stabilizer legs are extended and powered back up when the legs are retracted (↓2.4.4.1$_{(63)}$, 2.4.4.2$_{(63)}$).

MAPS-S C6 The manipulator arm must be stowed during all mobile base movement (→H4$_{(38)}$) (↓2.4.2.1$_{(61)}$, 2.4.4.1$_{(63)}$).

MAPS-S C7 The stabilizer legs must be deployed whenever the manipulator arm is not stowed (→H3$_{(38)}$).

MAPS-S C7.1 The manipulator arm must not be extended when the stabilizers are retracted (↓2.4.4.1$_{(63)}$, 2.4.4.2$_{(63)}$).

MAPS-S C7.2 The stabilizers must not be retracted until the manipulator arm is fully stowed (↓2.4.4.1$_{(63)}$).

MAPS-S C8 The mobile base must not move if any safety-related subsystems are nonoperational (→H1$_{(36)}$).

MAPS-S C8.1 MAPS must check that all safety-related systems are operational before beginning any move (↓2.4.1$_{(61)}$, 2.4.2.1$_{(61)}$, 2.4.2.2$_{(61)}$).

MAPS-S C9 Movement warnings must be provided (→H1$_{(36)}$).

MAPS-S C9.2 Visual movement alerts must start 10 seconds before mobile base movement begins and aural alerts must start 5 seconds before movement begins (↓2.4.2.1$_{(61)}$).

MAPS-S C9.2 Both visual and aural alerts must be activated continuously until movement is completed (↓2.4.2.1$_{(61)}$).

Rationale: The aural and visual alert system is provided to prevent injury to any humans in the area. Becuase of the relatively low acceleration and velocity of the robot, five seconds should be adequate to allow humans to move out of the way. Alerts that begin too long before robot movement may lead to human delay is moving out of the way. The longer period for the visual alert is provided to allow humans to complete any critical actions before moving. These times may need to be changed on the basis of operational experience (↓6.1).

MAPS-S C10.1 The mobile base must not move while the DMES system is in operation [not implemented yet].

1.4.2.4 Location System (LS)

Goals

Provide information about the location of the mobile base in the processing facility to be used in moving to a new work area (→LS-FR1$_{(27)}$).

Requirements

LS-FR1 Upon request the location system shall provide the location of the mobile base in world coordinates with an accuracy of ± 10 centimeters. (↓2.1.8$_{(53)}$, 2.4.1$_{(61)}$, 2.4.3.1$_{(62)}$, 2.4.5.4.2$_{(65)}$, 2.4.6.1$_{(66)}$, 2.4.2.6$_{(62)}$, 2.8.1$_{(77)}$).

1.4.2.5 Motor Controller (MC)

Goals

Control the wheels and wheel motors on the mobile base.

Requirements

MC-FR1 The motor controller shall provide power to the motor that drives the robot wheels (↓2.9.5$_{(79)}$).

MC-FR2 The motor controller shall provide modes of operation appropriate both for control by an automated system and for control by a human (↓2.1.6$_{(52)}$, 2.4.5.2$_{(63)}$, 2.4.6.2$_{(66)}$, 2.9.5$_{(79)}$).

Design Constraints

MC-C1 The acceleration and deceleration values and velocity must be changeable by the operator during operations (←MAPS-C3$_{(24)}$) (↓T2.2$_{(59)}$, 2.9.7$_{(80)}$).

Safety-Related Design Constraints

MC-SC1 The Motor Controller must be able to stop the motion of the mobile base within 0.2 seconds of receiving a STOP command (→MAPS-SC2.2$_{(25)}$, H1$_{(36)}$) (↓2.9.7$_{(80)}$).

MC-SC2 The maximum velocity of the robot must be no more than 30 cm/sec. (→MAPS-SC2.2$_{(25)}$, H1$_{(36)}$) (↓2.1.6$_{(52)}$, 2.4.6.2$_{(66)}$, 2.4.6.3.1$_{(67)}$, 2.9.5$_{(79)}$)

1.4.2.6 Digital Camera (DC)

Goals

Provide information to the operator about obstacles in the path of the mobile base during movement (→H1$_{(36)}$).

Requirements

DC-FR1 The digital camera system shall provide ... (↓2.13.1$_{(87)}$, 2.13.2$_{(87)}$).

1.4.2.7 Manipulator Arm (MA)

Goals

Raise the inspection (vision) system and injection system components to the level of the tiles.

Requirements

MA-FR1 The manipulator arm system shall provide the mobility necessary for the inspection and DMES injection tools to reach the tiles on the orbiter (↓2.10.1$_{(81)}$, 2.10.3$_{(81)}$, 2.10.4$_{(81)}$).

MA-FR2 The manipulator arm controller shall provide the status (position) of the arm upon request directly to the TSS, the operator, or MAPS (depending on the source of the request). (→MAPS-SC4$_{(25)}$, MAPS-SC6$_{(26)}$, H3$_{(38)}$, H4$_{(38)}$) (↓2.1.10$_{(54)}$, 2.4.2.1$_{(61)}$, 2.4.4.1$_{(63)}$, T4.2.2$_{(59)}$, T5.4$_{(60)}$).

> **Rationale:** In the original CMU design, the TSS received information about the manipulator arm and was responsible for determining whether movement was allowed. However, because of the importance of the information for safety and the difficulty of verifying AI software, the system design was changed so that the information can be obtained directly by MAPS.

Design Constraints

MA-C1 The manipulator must be designed to be manually operated should the need arise (↓2.10.3$_{(81)}$).

Safety-Related Constraints

MA-SC1 The manipulator arm design must keep the inspection and injection tools steady enough to allow accurate operation (→H4$_{(38)}$) (↓2.10.5$_{(81)}$).

MA-SC2 Movement of the manipulator arm must be capable of being disabled by the operator or by MAPS (→H4$_{(38)}$) (↓T7$_{(60)}$, 2.1.10$_{(54)}$).

1.4.2.8 DMES Injection Subsystem (IS)

Goals

The DMES Injection Subsystem shall apply the DMES to the tiles (↓2.11$_{(83)}$).

Requirements

IS-FR1 The injection system shall be controlled entirely by the TSS.

IS-FR2 The injection tool shall release DMES into a tile (↓2.11$_{(83)}$).

Safety-Related Design Constraints

IS-SC1 DMES injection subsystem operation must be inhibited when the manipulator arm is stowed or in motion (↓??).

1.4.2.9 Vision Subsystem (VS)

Goals

Perform the tile registration and inspection tasks.

Requirements

VS-FR1 The vision system shall be able to identify individual tiles ... (↓2.12$_{(85)}$).

1.4.2.10 System Log (SL)

Goals

To provide an automated data recording and information transfer function.

> **Rationale:** This automated function is expected to increase the data integrity, completeness, and accuracy of reports and thus to provide great value in tracking and planning work. Robot status information should be helpful in monitoring robot operation.

Requirements

SL-FR1 The system log shall be capable of holding the information collected during a work shift (↓2.14$_{(89)}$).

SL-FR2 The system log shall contain the information determined during system design to be useful for operations, maintenance, and safety or operations audits, including at least tile images, records of tiles injected or inspected, and robot status information (↓2.4.8$_{(69)}$).

SL-FR3 FR: Upon request, the system log shall transfer the information collected during a work shift to the Workcell Controller (↓2.14$_{(89)}$).

1.4.2.11 Safety Systems (Fuse, Proximity-Sensing, Alerting)

Three subsystems of the mobile base are included solely to maintain safe operating conditions: a smart fuse, proximity-sensing, and alerting.

1.4.2.11.1 Safety Fuse (SF)

Goals

Provide an emergency stop function.

Requirements

SF-FR The emergency stopping of the mobile base or the manipulator arm motion shall be performed at a low hardware level via safety circuits (→H5$_{(39)}$, MAPS-SC1.4$_{(24)}$) (↓2.15.1$_{(91)}$).

SF-FR If the fuse detects an unsafe state, all robot motion shall be electrically inhibited within 0.1 seconds by stopping the operation of any hardware actuator on the mobile base, including those controlling the wheels, the manipulator arm, and the injection system (→H1$_{(36)}$, H5$_{(39)}$, MAPS-SC1.4$_{(24)}$) (↓2.15.2$_{(91)}$).

SF-FR Upon a status request, the safety shall indicate whether the robot is in a state where it can be moved safely or not (↓2.15.3$_{(91)}$).

SF-FR Only the operator shall be able to reset the safety fuse (→OP4$_{(32)}$) (↓2.15.4$_{(91)}$).

> **Rationale:** We have changed this feature from the original CMU Tessellator robot design. Providing the software, particularly the TSS software, which is written using AI techniques, with this function will involve a safety analysis that would be at best expensive and at worst impossible. The triggering of the safety fuse indicates a serious condition that could lead to robot or orbiter damage and requires a high level of assurance that the condition has been removed before enabling movement again.
>
> **Assumptions** The safety fuse will be triggered rarely, on average no more than once a month. Frequent shutdown of the robot by the safety fuse could lead to inefficient operational performance and attempts to bypass the fuse. During system testing and operations, the frequency of safety fuse operation should be monitored (↓6.1).

SF-FR The operator shall be able to query the safety fuse for the cause of the shutdown (↓2.15.3$_{(91)}$).

1.4.2.11.2 Proximity-Sensing System (PSS)

Goals

1. Protect flight hardware by providing proximity sensing.

Requirements

PSS-FR1 The contact strips in the Proximity-Sensing System shall send a signal to the safety fuse in the event of contact with any external object (→H1$_{(36)}$, H4$_{(38)}$) (↓2.16.2$_{(93)}$).

> **Rationale:** The safety fuse can stop the base faster than a human operator can detect a signal and react. However, this system design decision has important ramifications with respect to operator complacency and alertness. Training and operational audits should be used to ensure that operators are not overly depending on the Proximity-Sensing System to avoid accidents (↓6.1).

1.4.2.11.3 Aural and Visual Alert System (AS)

Goals

Provide warning about mobile base movement to any humans in the area of the robot.

Requirements

AS-FR1 Whenever the robot is in motion, aural and visual indications shall be provided to alert humans in the vicinity (→H1$_{(36)}$, ↓2.17$_{(95)}$).

> **:Rationale** Both aural and visual alerts are needed to account for any individual human visual or aural deficiencies. In addition, visual warnings may be provided earlier than the aural ones in order to provide longer advance warning before more disruptive aural signals.

AS-FR2 The mobile base movement alert system shall be controlled by MAPS (←MAPS-FR6$_{(23)}$).

> **:Rationale** As MAPS provides all commands to the motor controller, it knows whenever the base is about to start movement and when it has stopped.

AS-FR3 Additional alerts, such as alerts about manipulator arm movement or DMES application, shall be provided as deemed necessary in the safety and human factors analyses.

1.4.3 Operator Task Requirements

This section contains assumptions, requirements, and constraints involving operator tasks and behavior. The information is used in the operator task analyses, the design of the operator interface, the MAPS logic, operator procedures, operator (user) manuals, and training plans and programs.

OP-FR1 The operator shall supervise all robot base movement (→H1$_{(36)}$, H2$_{(37)}$, H3$_{(38)}$, H4$_{(38)}$, Con1$_{(32)}$) (↓T4$_{(59)}$, T5$_{(60)}$) and tile servicing (↓T1$_{(59)}$, T7$_{(60)}$).

> **Assumption** Jobs will be defined so that movement will occur approximately every half hour.

> **:Rationale** If the operators are required to interact every few minutes with the system in order to monitor base moves, then the attractiveness of the system to users is far less than one that needs only infrequent attention. Therefore, the size of the work areas will be adjusted to satisfy the goal of approximately one base move per half hour. Once per half hour translates roughly into 80 moves during the course of rewaterproofing the orbiter, which results in a workspace of 300 tiles. In addition, with approximately 15,000 tile servicing steps and only a few hundred base moves at most, total task time is affected primarily by time to service a tile and very little (in comparison) by the time to move the mobile base.

OPF R2 The operator shall authorize all robot base movements before they are performed, including movements commanded by the TSS (→H1$_{(36)}$, H2$_{(37)}$, H3$_{(38)}$, H4$_{(38)}$, Con5$_{(33)}$) (↓T4.2$_{(59)}$, T5.5$_{(60)}$).

> **Rationale:** The TSS can drive the robot more smoothly and directly than the operator, but the operator is required to oversee the robot movement both to monitor the TSS movement for errors and for safety assurance. With the override control, the operator can stop the motion at any time and observe progress of the robot in the course of a move. This design feature was included in the original Tessellator robot because it allowed a simple to implement upgrade path for the software for robot autonomy. The operator-override option allows full-autonomy mode but also allows the robot to be shut down at any time by the operator.

OPF R3 The operator shall stop the robot immediately if any obstacle appears in the robot path (→H1$_{(36)}$, Con5$_{(33)}$, Con6$_{(33)}$) (↓T4.3.2$_{(59)}$).

> **Assumption:** The operators will have adequate visibility (direct or via the digital camera) of the work area to prevent collisions. Movement time and speed will be such that operator alertness is not a factor.

OPF R4 The operator shall be responsible for handling safety fuse alerts and for resetting the safety fuse when the system is ready for restart (←SF-FR4$_{(30)}$, SF-FR5$_{(30)}$) (↓T8.1$_{(60)}$, 2.15.3$_{(91)}$, 2.15.4$_{(91)}$).

OP5 The operator shall be able to drive the robot independently of the TSS by use of a joystick (→Con2$_{(33)}$, Con3$_{(33)}$, Con4$_{(33)}$, ↓T5$_{(60)}$).

> **Rationale:** While the computer can move the robot more precisely, human robot movement control may be safer in situations where the environment is uncertain (e.g., locations and times in the OPF when humans are working in the area where robot movement is necessary). In addition, this design feature will be useful if during operations it is determined that simply monitoring robot movement leads to inadequate alertness on the part of the operator and more direct control is necessary to assure safety.

1.4.4 Controls

Goals

Allow effective achievement of all assigned operator tasks and responsibilities as determined by the task analysis and system safety analysis.

Requirements and Constraints

Con1 Controls shall include at minimum a joystick and a deadman switch. Additional controls, such as dials, switches, buttons, or keyboard shall be provided as deemed necessary to perform the tasks identified in the operator task analysis (←OP1$_{(31)}$) (↓2.2$_{(57)}$, 2.3$_{(59)}$).

Con2 A joystick shall be provided to allow the operator to control the movement of the robot base (←OP5$_{(32)}$) (↓2.2.2$_{(57)}$, 2.4.6$_{(66)}$).

Con3 The operator must be able to provide fine-grain enough movement of the joystick to control robot motion accurately enough to avoid obstacles and damage to the Shuttle or the robot (←OP5$_{(32)}$) (↓2.2.2$_{(57)}$, 2.4.6$_{(66)}$, 2.4.6.3.1$_{(67)}$)

Con4 The joystick shall be capable of being effectively operated by a man or a woman with average manual dexterity and strength as defined in IEEE Standard XX (←OP5$_{(32)}$) (↓2.2.2$_{(57)}$).

Con5 The operator shall be provided with a deadman switch that allows or inhibits robot movement. Movement must stop within 0.5 seconds after releasing the deadman switch (→H1$_{(36)}$, MAPS-SC2.1$_{(25)}$) (←OP2$_{(32)}$, OP3$_{(32)}$), (↓2.2.1.3$_{(57)}$).

> **Assumption:** The deadman switch will be used as the primary means for the operator to authorize and to stop robot movement.

Con6 The operator shall be provided with an emergency stop facility that stops all robot motion, including the manipulator arm and injection system, within 0.5 seconds of activating it (←OP3$_{(32)}$) (↓2.2.1.2$_{(57)}$).

> **Rationale:** While the deadman switch will be used to stop movement of the mobile base, the operator needs the ability to stop other moving parts on the robot in case of emergency. The emergency stop button, which will be directly connected to the safety fuse, also provides a backup to the deadman switch (which is implemented through software) in case the robot does not stop when the deadman switch is released because of a software error, system design error, or hardware failure.

Con7 Upon request, the joystick controller shall initiate a joystick calibration (↓2.2.2.1$_{(58)}$, 2.3$_{(59)}$).

Con8 A person with a high school education must be able to learn to operate the robot accurately and safely with two hours of training and practice (↓4.3, 2.4.6.2$_{(66)}$).

1.4.5 Displays

Dis 1 The GUI and other control panel displays shall provide the oprator with enough information about the status of the robot and the work area that the operator is able to avoid hazards and to perform necessary operational tasks as determined by the operator task analysis (↓2.2.3$_{(58)}$, 2.3$_{(59)}$).

Dis 2 The displays must be understandable and usable by the average high school graduate after thirty minutes of training (↓4.3).

1.5 Hazard List and Hazard Log

1.5.1 Accident Definition

An accident is an unacceptable loss, as defined by NASA Shuttle program management. Unacceptable losses and their severity levels are:

Level 1

A1-1: Loss of orbiter and crew (e.g., inadequate thermal protection)

A1-2: Loss of life or serious injury in processing facility

Level 2

A2-1: Damage to orbiter or to objects in the processing facility that results in the delay of a launch and/or result in a loss of greater than TBD dollars.

A2-2: Injury to humans requiring hospitalization or medical attention and leading to long-term or permanent physical effects.

Level 3

A3-1: Minor human injury (does not require medical attention or requires only minimal intervention and does not lead to long-term or permanent physical effects)

A3-2: Damage to orbiter that does not delay launch and results in a loss of less than TBD dollars.

A3-3: Damage to objects in the processing facility (both on the floor or suspended) that does not result in delay of a launch nor a loss of greater than TBD dollars.

A3-4: Damage to the mobile robot.

> **Assumption:** It is assumed that there is a backup plan in place for servicing the orbiter thermal tiles in case the TTPS has a mechanical failure and that the same backup measures can be used in the event the robot is out of commission due to other types of damage.

1.5.2 Safety Policy

General Safety Policy All hazards related to human injury or damage to the orbiter must be eliminated or mitigated by the system design. A reasonable effort must be made to eliminate or mitigate hazards resulting at most in damage to the robot or objects in the work area. For any hazards that cannot be eliminated, the hazard analysis as well as the design features and development procedures, including any tradeoff studies, used to reduce the hazard level must be documented and presented to the customer for acceptance.

Hazard level will be determined by worst potential severity. Hazards that can result in human injury or damage to the orbiter must be eliminated or mitigated if they are not judged to be physically impossible or they are caused by *physical* conditions that are judged to have a likelihood of occurrence of more than one in a million over a 20 year period. All types of software (logical) errors will be considered to be possible and likelihood arguments cannot be used to reduce safety effort related to those errors. A qualitative evaluation of software-related hazard likelihood is acceptable, but as with quantitative evaluations, must be justified to Shuttle Program management and cannot be based simply on the use of testing and good software engineering processes.

1.5.3 Hazard Log

The following hazards have been identified for the mobile robot. Only those hazards related to the operation of MAPS have been evaluated in detail for this example intent specification. A complete system hazard analysis would require full analysis of all the hazards.

H1: *Violation of minimum separation between mobile base and objects (including orbiter and humans.)*

Subsystem:
MAPS, vision system, proximity sensing system, motor controller
location system, visual and aural alert system, operator displays and controls
Operation Phase: movement from one work zone to another
High-Level Causal Factors:
Uncommanded or unintended motion;
Not stopping when commanded or not stopping fast enough;
Operator issues command that violates minimum separation between robot and object;
Mobile base commanded to unsafe position by TSS;
Movement commanded when a proximity-sensing or other safety-related hardware system is inoperable;
Object moves into robot path.
Level and Effect: A1-2
Safety Constraints

Mobile base must move only when commanded (←MAPS-SC1$_{(24)}$, MAPS-FR2.4$_{(22)}$);
Mobile base must stop when commanded (←MAPS-SC2$_{(25)}$, SF-FR2$_{(30)}$ SF-FR1$_{(30)}$);
Mobile base must not be commanded to an occupied position (←MAPS-SC3$_{(25)}$);
The operator shall supervise all robot base movement (←OP1$_{(31)}$);
The operator shall authorize all robot base movements before they are performed, including movements commanded by the TSS (←OP2$_{(32)}$, Con5$_{(33)}$);
The operator must have information about objects in robot path and the ability to stop the mobile base within 0.5 sec (←OP2$_{(32)}$, OP3$_{(32)}$, Disp1$_{(33)}$, Con5$_{(33)}$, Con6$_{(33)}$);
Movement warnings must be provided (←MAPS-FR6$_{(23)}$, MAPS-SC9$_{(26)}$, AS-FR1$_{(31)}$);
Mobile base must not move if any safety-related subsystem is not operational (←MAPS-SC8$_{(26)}$, SF-FR3$_{(30)}$, SF-FR4$_{(30)}$);
The motor controller must be able to stop the motion of the mobile base within 0.2 seconds of receiving a STOP command (←MC-SC1$_{(27)}$);
The maximum velocity of the robot must be no more than 30 cm/sec (←MC-SC2$_{(27)}$);
The proximity sensing subsystem shall send a signal to the safety fuse in the event of contact with any external object (←PSS-FR1$_{(30)}$);
It must be possible to move the mobile base out of the way manually in case of an emergency (←MB-SC3$_{(20)}$).

Analyses Performed:
Actions Taken:
Status:
Verification:
Final Disposition (Closed/Open): **Status:**
Design Engineer:
Remarks:

H2: Robot movement with stabilizers extended

Subsystem : MAPS, stabilizer legs
Operation Phase: Movement from one work zone to another
High-Level Causal Factors:
Robot moves without retracting stabilizers
Level and Effect: A3-4
Safety Constraints:
Mobile base must not move if stabilizers are extended (←MAPS-SC5$_{(25)}$);
Stabilizers must be retracted during all mobile base movement (←MAPS-SC5$_{(25)}$ ↓2.6.4$_{(73)}$).

Analyses Performed:
Actions Taken:
Status:
Verification:
Final Disposition (Closed/Open): **Status:**
Design Engineer:
Remarks:

H3: *Robot base becomes unstable*

Subsystem(s): MAPS, stabilizers
Operation Phase: All
High-Level Causal Factors:
Stabilizers not deployed while arm extended;
Stabilizers retracted while arm extended
Robot falls over while crossing covers or other obstacles
Level and Effect: A1-2
Safety Constraints:
Manipulator arm must move only when stabilizers are fully deployed
(←MAPS-SC4$_{(25)}$, MAPS-SC5$_{(25)}$ ↓2.10.2$_{(81)}$);
Stabilizer legs must not be retracted until manipulator arm is fully stowed
(←MAPS-SC7$_{(26)}$).
Analyses Performed:
Actions Taken:
Status:
Verification:
Final Disposition (Closed/Open): **Status:**
Engineer:
Remarks:

H4: *Manipulator arm hits something*

Subsystem(s): TSS, MAPS, vision system, arm controller, proximity-sensing system
Operation Phase: All
High-Level Causal Factors:
Arm commanded into an object;
Mobile base moves without arm being completely stowed
Level and Effect: A2-1, A2-2
Safety Constraints:
The manipulator must be stowed before movement starts (←MAPS-SC6$_{(26)}$, ↓2.10.2$_{(81)}$);
The mobile base must be able to ensure accuracy of 10 cm for positioning and 1 mm for tile servicing (inspection and injection) tasks (←MB-SC1$_{(20)}$);
The TSS must not move the arm unless the vision system is operational (←TSS-SC1$_{(21)}$);
The TSS must not command the arm into contact with any object unless required for tile servicing (←TSS-SC2$_{(21)}$);
The proximity sensing subsystem shall send a signal to the safety fuse in the event of contact of arm with any external object (←PSS-FR1$_{(30)}$);
The manipulator arm must keep the inspection and injection tools steady enough to allow accurate operation (←MA-SC1$_{(28)}$);
Movement of the manipulator must be capable of being disabled by the operator

or by MAPS (←MA-SC2$_{(28)}$).

Analyses Performed:
Actions Taken:
Status:
Verification:
Final Closeout (Closed/Open) Status:
Engineer:
Remarks:

Hazard: *Damage to the robot caused by robot component operation or failure*

Subsystem :
Operation Phase: All
High-Level Causal Factors: Mobile robot operates with low oil level, . . .
Level and Effect: A3-4
Safety Constraints:
When the safety fuse is in the Halt state, the mobile base must not be capable of performing any kind of movement (←SF-FR2$_{(30)}$, MAPS-SC1.4$_{(24)}$).
Analyses Performed:
Actions Taken:
Status:
Verification:
Final Closeout (Closed/Open) Status:
Engineer:
Remarks:

Hazard: *Explosion*

Subsystem :
Operation Phase:
High-Level Causal Factors: DMES achieves explosive mixture
Level and Effect: A1-2
Safety Constraints:
The mobile base design must protect against fire and explosion (←MB-SC2$_{(20)}$)
Analyses Performed:
Actions Taken:
Status:
Verification:
Final Closeout (Closed/Open) Status:
Engineer:
Remarks:

H7: *Contact of human*

Subsystem: Injection system, TSS, vision system
Operation Phase:
High-Level Causal Factors: DMES released in wrong place
Level and Effect: A2-2
Safety Constraints:
Mobile base must not move while DMES system is in operation (←OP2$_{(32)}$);
Chemicals must not be injected without providing a warning to humans in the area (←TSS-SC3$_{(21)}$);
The injection system must not be operated unless the mobile base is stopped in the work zone and the manipulator arm has moved the injection tool to the proper tile (←TSS-SC4$_{(21)}$)
DMES subsystem operation must be inhibited when the manipulator arm is stowed or in motion (←IS-SC1$_{(29)}$)
Analyses Performed:
Actions Taken:
Status:
Verification:
Final Disposition (Closeout Status):
Engineer:
Remarks:

H8: *Inadequate thermal protection*

Subsystem: Injection system, TSS, vision system, MAPS, workcell controller
Operation Phase: All plus operation of Orbiter
High-Level Causal Factors:
Damaged tiles not detected;
DMES not applied correctly
Level and Effect: A1-1
Safety Constraints:
The job (instructions) provided to the mobile robot must not result in any tiles being missed in the inspection or waterproofing process (←WCC-SC1$_{(19)}$);
Analyses Performed:
Actions Taken:
Status:
Verification:
Final Disposition (Closeout Status):
Engineer:
Remarks:

16. Preliminary Hazard Analysis

This section provides an example of a hazard analysis used in an intent specification. Other types of hazard analyses or analyses of other system-level properties (e.g., security) could and should also be part of an intent specification. The information provided by this hazard analysis is used to generate safety-related functional requirements and design constraints.

17. MAPS System Limitations

Limitations may be related to basic functional requirements that cannot be completely implemented, to environmental assumptions, or to accepted risks, i.e., hazards that cannot be completely eliminated, mitigated, reduced to an acceptable level, or in some other way resolved satisfactorily. Such limitations may affect the design of the operational procedures and entries in the user or operator's manual. In a complete intent specification, links be provided to both the reason for the limitations (e.g., part of the safety analysis or a description of the environment) and to any relevant operational procedures and user manual entries. This section will probably not be completed until the system development is complete.

[Incomplete – examples only]

L1: Accuracy of positioning is limited by the accuracy of the information provided to MAPS by the Location System (→H1, H4).

L2: Accuracy of positioning is limited by the accuracy of data provided to the Location System on the position of the orbiter in the OPF (→H1, H4).

> **Assumption:** This limitation can be partially controlled through operational procedures.

L3: Because the location system can only work while the robot base is stopped, operator display information about the current position with respect to the commanded route of travel may be inaccurate.

> **Assumption:** It is assumed that the operator will be told about this limitation and will rely primarily on the vision system during robot movement (↓5.1, 5.2). The display of the commanded route of travel will be used only to understand the computer's intentions.

1.8 Verification and Validation

1.11.1 Review Procedure, Results, Participants

Level 2

System Design Principles

[illegible] decisions in the level below presents any basic principles upon which the system [illegible] describes how Level 1 requirements are achieved, including any "derived requirements" and design features not related to the Level 1 requirements, and describes how the design constraints are enforced. English is used to provide this information for MAPS as it appears to be the most appropriate for this particular system. However, other types of engineering notations could be used, e.g., a combination of English and [illegible] might be most appropriate for specifying the design and rationale behind the design of some types of control algorithms.

Note again that the order in which the levels are completed is implied by the numbering [illegible] focus first on the higher levels [illegible] parallel. The important part is that at the end of the development process, all the levels are complete so that system assessment is possible (such as a system safety evaluation for a safety critical system) and so that operations and system evolution and maintenance can proceed efficiently and safely.

In this level, only the specification for the mobility and positioning are completed although enough is provided about the other components [illegible] required to complete the specification.

2.1 TTSS Component Interface Design

[This section for the interface specification has been completed for MAPS only.]

The TTPS components interact in the manner shown in Figure 2.1.

2.1.1 Tile Servicing Subsystem

TSS ⇒ MAPS

Maps-Move Used to command robot movement. The parameters indicate a route that MAPS is to follow (a set of waypoints), with the last point on the route being the desired work zone.

Maps-Disable Used to indicate to MAPS that movement is currently not legal. For example, this would be used to indicate that DMES application has not been completed or that the manipulator arm is not ready to be stowed.

Maps-Enable Used to indicate to MAPS that movement is currently legal. This message is used to reverse the Maps Disable message.

MAPS ⇒ TSS

Status-Message Used to return the success or failure of the Maps Move command. A status message is also generated any time Computer Mode is entered or exited. The message will contain a code indicating the success or failure of the commands, the latest position of the robot, and the command to which the status message is responding (if any) (↑TSS-FR2.3$_{(21)}$).

2.1.2 Display

MAPS ⇒ Display

MAPS-operating-mode Sent whenever the MAPS operating mode changes. Contains the new operating mode.

Figure 2.1:

Display-Position-Report Sent any time MAPS reads the scanner and determines a new position for the robot. The parameters represent the location of the robot (X,Y, and θ) with respect to world coordinates. This information can be displayed numerically or graphically.

Display-Request-Move-Permission Sent prior to making any move. The route specified must be displayed to the operator, preferably in a graphical fashion. The route consists of a number of points, beginning with the current robot location. The set of waypoints contains X,Y,θ coordinates of each waypoint that makes up the route. A maximum of 20 waypoints can be provided. In addition to displaying the route for the operator's review, the following textual message should be displayed:

> "Permission to move along the displayed route is requested. Please depress and hold the deadman's switch to authorize this move. You may lift the deadman's switch at any time to suspend this move."

Display-error Sent any time an error condition is encountered.

2.1.3 Control Panel

Control Panel ⟹ MAPS

Set-Mode-Operator-Mode Used to switch MAPS into Operator Mode.

Set-Mode-Computer-Mode Used to switch MAPS into Computer Mode.

Disable-Operation Used to disable MAPS operation. The message will normally be used during maintenance, for example, if some type of maintenance or checking operations are performed on the joystick.

Enable-Operation Issued at powerup and after a Disable-Operation command.

2.1.4 Joystick

MAPS ⟹ Joystick

Joystick-init Initializes the hardware to read values from the joystick. Sent once at powerup.

Joystick ⟹ MAPS

Joystick-zero Sent in response to a Joystick-init command. Records the current offsets as the zero X,Y, θ position. This should be called once with the joystick in the home position (offsets may be hardwired later).

Joystick-stat Sent in response to a Joystick-init command. It contains the status of the joystick, either operational or not operational (i.e., unplugged).

Joystick-pos Sent as a move command to MAPS whenever the joystick stops in a non-neutral position and the deadman switch is depressed or whenever the joystick returns to the neutral position. Includes the position of the joystick in x,y,θ values, with a range limit of -128 to +127.

Joystick-Button1 Sent whenever joystick button 1 is depressed or released.

Joystick-Button2 Sent whenever the joystick button 2 is depressed or released.

2.1.5 Log Manager

MAPS ⇒ Log Manager

Log Logs events identified by a "log code" into the log file.

2.1.6 Motor Controller

MAPS ⇒ Motor Controller

Reset: Reset the motion control board to its default (powerup) state. Should be called before any other actions are performed with the board. Sets the acceleration and deceleration for all four motors to the same value. Also sets the maximum velocity (centimeters per second). The velocity is measured at one of the wheel contact points. Velocity must be in the range of 0 to 30 centimeters/second.

Move-velocity (X,Y,θ): Used for velocity mode. When received, the motor controller performs the kinematics on the body relative (x,y,θ) velocity specified in (in/sec, in/sec, radians/sec), and sets the appropriate wheel velocities. This routine causes motion to occur.

Move-relative (X,Y,θ): Used for position mode. When received, the motor controller performs the kinematics on the body relative (x,y,θ) desired position (inches, inches, radians) and then moves the mobile base suing the acceleration and velocity values from set_acceleration and set_velocity, respectively.

Stop: Causes the vehicle to decelerate to a complete stop. The motors remain on and servoing. In velocity mode, all velocities are set to zero.

Motors_off: Turns all four motors off to a freewheeling state. Any queued commands will be flushed.

Motors_on_velocity: Turns on all four motors and initializes them for velocity servoing mode. Initial velocities are set to zero.

Motors_on_position: Turns on all four motors and initializes them for position servoing. The position queue is flushed.

Motor Controller ⇒ MAPS

Motion-status: Sends the current motion status: (1) the movement mode, (2) the on/off status of each of the four wheel motors, (2) indication that an error has occurred, and (3) completion of a movement. Sent whenever the status changes.

2.7.1. Stabilizers

MAPS ⇒ Stabilizers

Legs-Down: Causes the stiff legs to be deployed. If the stiff legs are already deployed, the message has no effect. In either case, the error-status parameter returns a success or failure code.

Legs-Up: Causes the stiff legs to be retracted. If the stiff legs are already retracted, the message has no effect. In either case, the error-status parameter returns a success or failure code.

Position-Request: Request for the stabilizer leg controller to provide the current status of the stabilizers.

Stabilizers ⇒ MAPS

Stabilizer-Status-Message: Sent in response to a legs-down, legs-up, or position-request message or whenever the status of the stabilizers changes.

2.8.1. Laser Scanner

MAPS ⇒ Scanner

Get-Scanner-Position: Requests the latest position calculated by the scanner

Scanner ⇒ MAPS

Send-Position: Provides the current position (x,y,θ) in world coordinates. Sent in response to a Get-Scanner-Position message.

2.1.9 Safety Circuit

MAPS ⇒ Safety Circuit

Read-safety-circuit: Request for the safety-circuit status.

Safety Circuit ⇒ MAPS

Safety-Circuit-Status: Sent in response to Read-Safety-Circuit message or whenever the safety circuit status changes.

2.1.10 Arm Controller

MAPS ⇒ Arm Controller

Check-Arm-Position: Request for arm status.

Enable-Arm-Movement: Enables arm movement.

Disable-Arm-Movement: Disables arm movement.

Arm Controller ⇒ MAPS

Arm-status: Sent in response to any command from MAPS.

2.1.11 Motion Alert System

MAPS ⇒ Motion Alert System

Check-alert-system-status: Requests alert system status.

Activate visual-alert: Sent to initiate a visual alert.

Deactivate visual-alert: Sent to stop a visual alert.

Activate aural-alert: Sent to initiate an aural alert.

Deactivate aural-alert: Sent to stop an aural alert.

Motion Alert System ⇒ MAPS

Alert-system-status: Sent in response to a check-alert-status message or whenever the alert system status changes.

221.1 OthSystem Interactions

2.2 Controls and Displays

2.2.1 Control Panel

1.2. The control panel provides the operator with the ability to issue commands to the TSS, to MAPS, and to other system components as defined in Section 2.1 and to check their status (↑Con1$_{(32)}$).

> **11.2.** Common actions such as setting Operator or Computer Mode are implemented using button, dials, or switches rather than requiring more tedious and time-consuming keyboard inputs or even mouse clicks (which can lead to repetitive strain injury). Keyboard and mouse entries should be limited to infrequent activities or those that cannot be implemented using buttons, switches, or dials.

2.2. The control panel includes an emergency stop button that directly activates the safety fuse (↑1.4.2.11.1) and shuts down power to all the Tessellator components at most 0.5 seconds after it is pushed. The emergency stop button must be located where it is always within the operator's reach and … (↑Con6$_{(33)}$).

3.2. A deadman switch is used to authorize or stop mobile base movement. The deadman switch is activated by two joystick buttons, one of top and one on the bottom of the joystick handle. Movement does not occur unless one or both buttons are depressed and stops within 0.5 seconds after the button(s) is released (↑Con5$_{(33)}$, MAPS-SC2.1$_{(25)}$, MAPS-SC2.2$_{(25)}$).

4.2. The user interface can invalidate certain operator options (e.g., disable menu choices or buttons) when such operations are not legal or are unsafe. For example, selection of Computer Joystick mode is possible only when the safety fuse is not in the HALT state.

> **Rationale:** Although MAPS should ignore such illegal or unsafe commands, an extra level of protection is provided by this redundancy. Care must be taken, however, not to block any operator options that might be needed by the operator, particularly in an emergency.

2.2.2 Joystick

(↑Con2$_{(33)}$, Con3$_{(33)}$, Con4$_{(33)}$, Con7$_{(33)}$)

2.2.2.1 The joystick controller must be initialized prior to use (at powerup). This involves setting the maximum velocity; x, y, and θ thresholds, max throw constants, and speed factor ($\rightarrow$2.4.6.3.1$_{(67)}$). Defaults are provided but they may be reset at this time. Joystick calibration may also occur at this time.

2.2.2.1 The operator drives the robot by deflecting a joystick in the direction the operator would like the robot to travel. Deflection of the joystick away from the operator results in forward robot motion while deflection towards the operator results in backward robot motion. Deflection of the joystick to the left and right produces corresponding robot motions to the left and right.

2.2.2.3 The robot is rotated by rotating the joystick handle. Rotation of the joystick handle in a clockwise direction results in clockwise (as viewed from above) rotation of the robot. Likewise, counterclockwise rotation of the handle results in counterclockwise robot rotation.

2.2.2.4 Speed is controlled according to the amount of deflection of the joystick. Motion is proportional such that a small deflection of the joystick results in a slow movement while a larger deflection results in faster motion.

2.2.2.5 The joystick has a neutral position that signals the joystick is not commanding any motion. The joystick provides its position relative to this neutral position in the form of x, y, and θ.

2.2.3 Displays

The displays provide the following information: position of the robot, position of the legs (deployed or not deployed), position of the arm (stowed or not stowed), the route provided by the TSS, the status of the safety fuse and the reason for being in the halt state if it is, a view of the area ahead of and around the robot, and pictures of the tiles (in case the TSS needs help to evaluate the state of a tile) ($\uparrow$Disp1$_{(33)}$, TSS-FR2.1$_{(21)}$, MA-FR2$_{(28)}$, $\rightarrow$2.13.2$_{(87)}$).

3 Operator Task Design Principles

The Operator Task Analysis should be tightly connected to the system design principles. Many of the design principles come directly from the task analysis while some of the operator tasks come from system design features.

3.1 Preliminary OTA for MAPS

T1 Enter instructions for TSS work cell Controller about Shuttle position and inspection sequence.

T2 Powerup and initialize Tesselator

- T2.1 Initialize laser scanner and make any laser scanner bar code changes
- T2.2 Set normal and emergency acceleration and deceleration values
- T2.3 Calibrate joystick
- T2.4 Set Operator Mode parameters (max velocity; X,Y,θ threshholds determined during joystick calibration)

T3 Set or change MAPS operating mode.

- T3.1 Determine appropriate mode.
- T3.2 Select mode.

T4 Monitor Computer-Controlled Movement

- T4.1 Read displayed route
- T4.2 Authorize all mobile base movement
  - T4.2.1 Check that stabilizers are retracted
  - T4.2.2 Check that the manipulator arm is stowed
  - T4.2.3 Read and check displayed route
  - T4.2.4 Press deadman switch
- T4.3 Monitor movement
  - T4.3.1 Monitor movement on screen
  - T4.3.2 Release deadman switch if obstacles are observed in the path
- T4.4 Monitor display for status messages and process error messages

T5 Control mobile base movement and positioning using the joystick

T5.1 Switch to manual mode if in computer mode

T5.2 Check screen for obstacles

T5.3 Check that stabilizers are retracted

T5.4 Check that the manipulator arm is stowed

T5.5 Depress deadman switch

T5.6 Operate joystick

T5.7 Release deadman switch and return joystick to neutral position

T5.8 Process error messages

T6 Check tile state on screen of Work Cell Controller if TSS asks for help

T7 Monitor tile servicing

T7.1 Inhibit manipulator arm movement.

T7.2 Enable manipulator arm movement.

T8 Handle errors and failures

T8.1 Handle safety fuse reset

T8.1.1 Query fuse for cause (→2.15.3$_{(91)}$)

T8.1.2 Take corrective action

T8.1.3 Reset fuse after problem has been fixed (→2.15.4$_{(91)}$)

T8.2 Process system error messages

T8.3 Notify maintainance about breakdowns

T8.4 Manually stow manipulator arm

T8.5 Manually extend or retract stabilizer legs

T8.6 Manually turn off wheel motors and/or disengage wheels from drivetrain

T8.7 Press emergency stop if unsafe conditions occur

2.4 Movement and Positioning Design Principles

2.4.1 MAPS Initialization

During initialization, MAPS resets the motor control interface (→2.9.8$_{(80)}$); initializes the joystick (→2.2.2.1$_{(58)}$); establishes that the robot is in a proper and safe startup state (the safety circuit is in the SAFE state (↑MAPS-SC8.1$_{(26)}$, 2.15.1$_{(91)}$), the mobile base is stopped (→2.8.2.1$_{(77)}$), and the Laser Scanner and Alert systems are operational (↑MAPS-SC8.1$_{(26)}$)); determines the initial position of the robot (↑LS-FR1$_{(27)}$); and sends a status message to the operator. MAPS does not accept any non-initialization commands (e.g., movement commands) until initialization is complete (↓).

2.4.2 Movement Control (General)

2.4.2.1 MAPS issues movement commands only if the safety fuse is in the SAFE state (↑MAPS-SC1.4.1$_{(24)}$), the manipulator arm is stowed (↑MA-FR2$_{(28)}$, MAPS-SC6$_{(26)}$), the stiff legs are retracted (↑MAPS-SC5.1$_{(25)}$), the joystick is in the neutral position (↑MAPS-SC1.1$_{(24)}$), the operator has depressed the deadman switch (↑MAPS-SC1.2$_{(24)}$), and the safety fuse and motion alert system are both operational (↑MAPS-SC8.1$_{(26)}$). MAPS activates a visual alert 10 seconds before mobile base movement begins and an aural alert 5 seconds before movement begins (↑MAPS-FR6$_{(23)}$, MAPS-SC9.1$_{(26)}$). Both are shut down in Computer Mode when the final destination is reached or the deadman switch is released and in Operator Mode when the joystick is returned to a neutral position (↑MAPS-SC9.2$_{(26)}$).

> **Rationale:** The aural and visual alert system is provided to prevent injury to any humans in the area. Because of the relatively low acceleration and velocity of the robot, five seconds should be adequate to allow humans to move out of the way. Alerts that begin too long before robot movement may lead to human delay is moving out of the way. The longer period for the visual alert is provided to allow humans to complete any critical actions before moving. These times may need to be changed on the basis of operational experience (↓6.1).

2.4.2.2 When informed by the TSS (↑MAPS-SC2.1$_{(25)}$), the operator (via the deadman switch) (↑MAPS-SC2.1$_{(25)}$, MAPS-SC3.2$_{(25)}$), or the safety fuse (↑MAPS-SC1.4.2$_{(24)}$)

that motion is not legal, MAPS stops all movement operations and inhibits any further movement operations until informed that movement is again allowed (↑MAPS-SC1.4.2$_{(24)}$, MAPS-SC2.1$_{(25)}$, MAPS-SC3.1$_{(25)}$, MAPS-SC8.1$_{(26)}$). Once movement becomes legal again, MAPS starts up in Operator Mode (↑MAPS-FR3.1$_{(23)}$).

> **Rationale:** Starting up movement in the previously active mode was considered but rejected for the following reason. There may be an extended period of time between disabling movement and enabling it again. The operator may not correctly remember that MAPS was in computer mode, for example, and try to drive the robot by depressing the joystick and deflecting the handle. This set of actions will enable movement control by the TSS (because the deadman switch is depressed) and all joystick commands will be ignored f mode confusion that could be dangerous under some scenarios. If the operator wants computer control to be active after a temporary stop, it will be easy to command it (←2.2.1.1.1$_{(57)}$).

2.4.2.3 The default acceleration and deceleration values are normally used (↑MAPS-C2$_{(23)}$), but acceleration and deceleration values can be changed via the user interface (↑MAPS-C3$_{(24)}$). An emergency deceleration value is used for an emergency stop, i.e., when the operator releases the deadman switch (↑MAPS-SC2.2$_{(25)}$).

2.4.2.4 When commanding movement, translation in the x-y plane (lateral movement) is performed first, followed by any required rotation. Either can be skipped if they are not necessary (↑MAPS-FR3.3$_{(23)}$).

2.4.2.5 **Definition o** A movement is considered complete only when the robot arrives in the desired work area. In Computer Mode, the work zone is assumed to be the last waypoint on the route. In Operator Mode, the robot is assumed to be in the work zone only when the following two conditions are both met: (1) the deadman switch is released and (2) the joystick returns to the neutral position. A new movement command must be issued for further movement to occur (↑MAPS-SC1.3$_{(24)}$).

2.4.2.6 While external position information will be provided to MAPS in world coordinates (↑TSS-FR2.2$_{(21)}$, LS-FR1$_{(27)}$), MAPS must issue commands in robot-relative coordinates (→2.9.6), Therefore, world coordinate inputs must be translated to robot-relative coordinate outputs. MAPS uses a standard package of matrix math routines to do this conversion. [Need to put the basic algorithm to be used for translation here.]

2.4. Position Determination (↑FR4)

2.5.1 Position determination occurs immediately after system initialization, when operator ... at the beginning and completion o ... Computer Mode, and ... joystick is returned to the neutral position in Operator Mode (↑LS-FR1$_{(27)}$, →2.8.2.1$_{(77)}$).

> **Rationale:** Position determination after a movement is used to provide feedback on previous commands in order to detect errors in carrying them out. MAPS must

dwelative displacement robot position be command to the motor controller. It is to assume that the robot position is the same as the last movement command .

2.3.2. Any time the robot position is determined, a message is sent to the user indicating the present location of the robot (↑MAPS-SC3.1$_{(25)}$).

2.4.4 Stabilization (↑MAPS-FR5)

2.4.4.1 Prior to movement being attempted, MAPS turns the drivetrain motors on (↑MAPS-SC5.3$_{(26)}$), ensures the arm is stowed (↑MAPS-SC6$_{(26)}$), disables arm movement (↑MAPS-SC7.1$_{(26)}$), and issues a command to retract the stabilizers (↑MAPS-SC5.1$_{(25)}$).

2.4.4.2 Once the robot has arrived at the commanded PS commands stabilizer deployment (↑MAPS-SC7.1$_{(26)}$), turns the motors off (↑MAPS-SC5.3$_{(26)}$). Once all stabilizers are PS enables arm movement (↑MAPS-SC4.1$_{(25)}$, MAPS-SC7.1$_{(26)}$). movement at completion of isfied in 2 .4.2.5$_{(62)}$.

2.4.4.3 In the event stabilizer retraction or deployment MAPS fails notifies the operator and the TSS of the failure (↑MAPS-SC5.2$_{(25)}$).

Rationale: The TSS needs to know so it does not send any arm movement commands. The operator needs to be informed so the failure can be diagnosed and repaired.

2.5 Computer Mode Operation (↑MAPS-FR 2)

2.5.1. **Initialization** Any time the operating mode changes to Computer Mode, before issuing any movement commands MAPS first selects position mode for the motor controller, determines the position and generates a status report to the TSS and operator (↑MAPS-SC3.1$_{(25)}$, TSS-FR2.3$_{(21)}$).

2.5.2. **Motion Control** In Computer Mode, the motors are controlled using position mode (↑MC-FR2$_{(27)}$, →2.9.5$_{(79)}$). MAPS makes all requests to the motor controller using θ-relative movement command, . Preset acceleration, deceleration, and velocity values are used. The normal stop command is used to effect a gradual stop when MAPS is completing a move the emergency stop for interrupted motion is used if requested by the operator through the deadman switch (↑MAPS-C2$_{(23)}$, MAPS-SC2.2$_{(25)}$).

2.5.4. Route Definition: The route shall ... relative to the -
rofnedraitoina imsespagci the TSS (↑TSS-FR2.2$_{(2)}$, AM PS-FR2.1$_{(22)}$). A route that contains zero length is logged as an error and a normal stop is commanded.

2.3.1. Definition: a ... to zero or more intermediate fial locations, and then a single movement to a .

2.3.4. If the desired movement consists o single route segment, the move is konwne rfomcotnhdeuccutreden at sotraliogcatt lione to the desired .
If the move consists of more than one segment, then the move is conducted as a sequence of straight line moves bet .

2.5.1. MAPS moves the robot along a straight line fied into the robot, considered the origin, to a point speci . Given A distance, M and a PS issues the appropriate commands to cause the robot to move a distance equal to $\sqrt{x^2 + y^2}$. If MAPS is given a rotation value θ degrees, MAPS instructs the robot to rotate relative to its starting position when the move command is given.

2.3.4. MAPS will need to calculate new coordinates during a move any time the operator releases the deadman switch or the robot pauses .

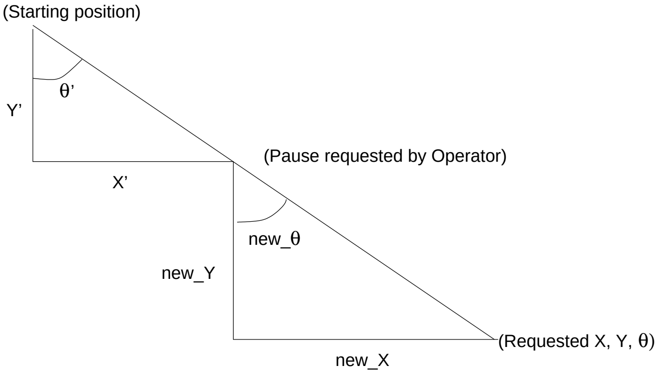


Figure 2.2: Calculation of Coordinates.

Given the current position, new X', Y', and θ' values are computed by

$$
\begin{aligned}
New\_X &= Final\_X - X' \\
new\_Y &= Final\_Y - Y' \\
new\_\theta &= Final\_\theta - \theta'
\end{aligned}
$$

2.5.4. If a move is calculated or commanded that results in a zero or near-zero (less than 10 centimeters) length, the move is not executed .

Rationale: This requirement is used to prevent commanding a near-zero length "jitter" and thus ... In addition, the accuracy limit of the Location System is 10 centimeters.

2.5.4. Mfilnt When operating in CoAmputer mode, M PS accepts movement commands from the TSS and issues motor commands to move the robot (↑MAPS-FR2$_{(22)}$, MA PS-FR2.1$_{(22)}$).

2.5.4.1 ABefore starting motion, M PS asks the user via the inter face for computer permission (↑MAPS-SC3.3$_{(25)}$). It does not begin the move until it detects that the deadman s released to the depressed position (↑MAPS-SC1.2$_{(24)}$). MAPS then continues along with the route as long the s witch remains depressed . If the deadman s Areleased, M PS stops all movement (↑MAPS-SC1.3$_{(24)}$) and reverts to Operator Mode (↑MAPS-FR3.1$_{(23)}$).

> **Rationale:** Releasing the deadman before the movement is complete is likely to result from the operator noticing possible obstacles in the computer-generated path. The operator takes control at this point (see also 2.4.2.2$_{(61)}$) .

2.5.4.2 A For each motion command (either a rotation or a translation), M PS takes a reading of current robot position (↑LS-FR wen$_{(27)}$), calculates the difference bet the actual robot location and the desired robot location, converts the difference into a robot relative move, and per forms the move. Following completion o f the move, M PS takes another reading of the actual location (→2.8.2.1$_{(77)}$)

> **Rationale:** With any physical motion, there is a very real possibility that the actual motion does not exactly match the intended motion. Feedback from the outside environment must accommodate this potential error.

"to close the loop" on the motion are achieved by using a set of tolerances . The built-in tolerances can be changed during system initialization (↑MAPS-C1$_{(23)}$) as If the desired location is not achieved, supplemental moves are computed and commanded up to the ma ximum number of attempts .

2.5.4.2.1 **Definition:** one attempt is a series of moves, each preceded by a reading and followed by a check of whether the target has been reached.

2.5.4.2.2 **Tolerances:** MAPS uses a loose set of tolerances for the intermediate locations and a set of tight tolerances for the final route location .

2.5.4.2.2.1 If the robot is moving via intermediate locations, a loose tolerance of 6 inches and 5 degrees is used for intermediate locations . If After 10 attempts the robot position is still outside the tolerance limits, M PS notifies the TSS and the operator and stops all motion .

> **Rationale:** Ten attempts should be adequate to reach the desired position. If ten attempts are unsuccessful, this probably indicates a problem that needs to be handled by the TSS or the operator.

[illegible] [illegible] the [illegible] current robot position and orientation are compared against the desired robot location and orientation. [illegible] 2 inches or 1 degree [illegible] tolerance) [illegible] 10 supplemental moves are calculated and attempted. [illegible] 10 supplemental moves the robot position is still outside the tolerance limits, MAPS [illegible] the TSS [illegible] user inter[illegible] and stops all motion (↑MAPS-FR2.2$_{(22)}$).

[illegible] [illegible] continues to move until one o[illegible] arrived at the desired destination, the deadman s[illegible] ↑MAPS-SC2.1$_{(25)}$), MAPS-SC[illegible] SAFE state (↑MAPS-SC1.4.2$_{(24)}$), or an error condition is detected.

[illegible] **[illegible]** MAPS [illegible] messages

- When [illegible] Mode is entered or e[illegible] PS generates a status message to the TSS [illegible] and the user inter[illegible].
- When MAPS completes a commanded move, the TSS [illegible] user inter[illegible] (↑MAPS-FR2.2$_{(22)}$).
- If MAPS fails to complete a commanded move, an error message is returned to the [illegible] user inter[illegible] ↑MAPS-FR2.2$_{(22)}$).
- [illegible] destination has been reached, MAPS [illegible] the TSS and the user [illegible] ↑MAPS-FR2.2$_{(22)}$).
- [illegible] message is received [illegible] SS when not operating in Computer mode, MAPS returns an error message to the TSS and to the operator (↑MAPS-FR3.4$_{(23)}$).
- [illegible] computer mode, MAPS [illegible] the operator (↑MAPS-FR2.4$_{(22)}$).

2.4.6 Operator Mode (↑MAPS-FR3$_{(23)}$)

[illegible] [illegible] operating mode changes to Operator mode and be[illegible] issuing any movement commands (↑2.8.2.1$_{(77)}$), MAPS [illegible] at the [illegible] and in the neutral position (↑MAPS-SC[illegible]$_{(24)}$), [illegible] velocity mode [illegible] (→2.9.[illegible]$_{(79)}$), [illegible] determines the position o[illegible] ↑LS-FR [illegible] $_{(27)}$), and generates a status report to the TSS and operator (↑MAPS-SC3.1$_{(25)}$).

[illegible] [illegible] operating in Operator Mode, all move requests are made through a move-velocity command (↑MC-SC2$_{(27)}$). A multiplier (speed-factor) is used [illegible] increase or decrease the velocity in [illegible]. [illegible] changed interactively during MAPS [illegible]cution. Stopping motion is achieved by issuing a mo[illegible]velocity request o[illegible] ↑EA4).

[illegible] and **Rationale:** Move velocity commands are more appropriate [illegible] an operator

control[illegible]rally e -
[illegible] more effective and e . It should also reduce training requirements, particularly when an emergency or high stress situation occur (↑Con8$_{(33)}$, MC-FR2$_{(27)}$).

[illegible] [illegible] Maps converts operator deflections o
movement commands to the motors (↑MAPS-[illegible]R $_{(22)}$, M[illegible] PS-FR3.2$_{(23)}$)[illegible]ranslation
world coordinat[illegible] coordinates is per paragraph 2.4.2.6$_{(62)}$.

[illegible] MAP[illegible] parameters that can be reset during operations (↑Con3$_{(33)}$).

- *Maximum velo*[illegible] velocity that can be commanded by the
in any direction. The units used[illegible]re inches per second an[illegible] and radians
[illegible]er second ↑EA4, M[illegible] PS-C3$_{(24)}$).

- *X, Y, and θ thresholds*: These thresho[illegible]d values give the minimum amount o
[illegible] moved
the centered positi[illegible] values are determined during .

[illegible] return to the same absolute lo -
[illegible] "z[illegible] mechanics are such that the
[illegible] variable ."[illegible] result, the
[illegible] undeflected
this difference.

- *Joystick maximum throw constant*[illegible] order to provide a proportional
[illegible] relative to the -scale deflection must be cal-
culate[illegible] one
[illegible] number that the
[illegible] scale along the indicated a .

- *Joystick speed factor*[illegible] system integrator to select
[illegible] during run -time operations. The value
i[illegible]ernally visible and [illegible] inter
[illegible] an operator . All movement commands are multiplied by this value
prior to being sent to the motor controller (↑MAPS-C3$_{(24)}$, M[illegible] PS-SC2.2$_{(25)}$).

[illegible]ceptable speeds are set
[illegible] o [illegible]
[illegible] different speed ranges .

[illegible] [illegible] be scaled into a percentage o
po[illegible] reading to the total possible deflection is -
culated. This percentage is the[illegible]plied to the ma possible velocity to yield a scaled veloci[illegible] zero and the ma velocity, proportional to the reading supplied.

[illegible] [illegible] mobile base motion ceases
neutral position (↑MAPS-SC2.3$_{(25)}$, M[illegible] PS-SC3.2$_{(25)}$). [illegible]tions are ignored
[illegible] (↑MAPS-SC1.2$_{(24)}$).

2.4. Movement Control Mode Selection

At any time, MAPS is in one of the following modes only one o Initialization, Computer Mode, Operator Mode, and .

2.4.1. Initialization Mode MAPS enters initialization mode on power up and after resets (↑MAPS-SC1.5(24)).

Rationale: which the robot ... repair ... changing the state of requiring the entire initialization sequence and ensuring the robot is in a safe state for movement .

2.4.2. Operator Mode MAPS transitions to Operator Mode from Initialization Mode (↑MAPS-FR3.1(23)), after a temporary shutdown ↑MAPS-FR3.1(23)), when the deadman switch is released, or upon receipt of the Operator to change to Operator Mode (↑MAPS-FR2.5(23)). If a movement message is received from the TSS while operating in Operator Mode, that message is ignored and an error message returned to the TSS (↑MAPS-FR3.4(23)).

2.4.3. Computer Mode MAPS changes to Computer Mode only upon receipt of a message from the operator (←2.1.3(51)) (↑MAPS-FR2.3(22)). If a joystick command is received while operating in Computer Mode, that command is ignored and an error message returned to the operator (↑MAPS-FR2.4(22)).

Rationale: If the operator wishes to change to Operator Mode while the TSS is generating movement commands, the fastest and best way to do this is to release the deadman switch. Accidental movement of the joystick from its neutral position when in Computer Mode should not result in a new Mode or movement command (joystick the . Operators should be trained to release the deadman button in an emergency rather than to move the joystick. While moving the joystick may be a more natural action under stress, allowing such movement to result in movement of the robot ... to avoid inadvertent robot movement.

When MAPS receives a message to change to Operator Mode, all current waypoints and movement messages are discarded. Any subsequent computer-controlled movement messages require a new route command from the TSS (↑MAPS-SC1.3(24)).

Rationale: The most likely reason for the operator to interrupt Computer Mode is that the route displayed, or the operator has detected a problem with the route such as unsafe conditions along the route . In addition, the robot position or environment may have changed while in Operator Mode, and previous movement messages may be obsolete.

2.7.4. Halt Mode MAPS enters Halt Mode when the system detects that its environment is unsafe, i.e., when it detects that the safety state is violated. MAPS transitions to Initialization Mode after the Halt Mode when safety returns to SAFE state (↑MAPS-SC1.5$_{(24)}$).

Rationale: While the robot is not operational, subsystems or the environment may change state from that assumed by MAPS. After leaving Halt Mode, the transition back to Computer or Operator mode requires Initialization mode for confirmation of subsystems and updating environment state in MAPS.

2.4. Information and Error Logging

MAPS provides a central log of events (including both errors or successful moves) (↑MAPS-FR7$_{(23)}$, →2.14$_{(89)}$). The following events are logged:

- A move or command is completed successfully.
- The safety changes to the unsafe state.
- The safety changes to the SAFE state.
- MAPS enters Computer Mode.
- MAPS enters the Operator Mode.
- A transition into Computer Mode is interrupted and cancelled.
- A transition into Operator Mode is interrupted and cancelled.
- MAPS operation is enabled.
- MAPS operation is disabled.
- MAPS operation is stopped due to the operator releasing the deadman switch during a move.
- MAPS [illegible] operation.
- MAPS begins movement along a segment other than the first in computer mode.
- MAPS completes movement along a segment other than the final in computer mode.
- MAPS begins movement along the first segment.
- MAPS completes movement along the final segment.
- MAPS attempts a retry of the move.
- The number of attempts to reach a location exceeds the threshold limit.
- MAPS completes a route successfully.
- A motor control error is detected.
- Joystick is disconnected.
- Joystick is deflected away from the neutral position, preventing MAPS from entering Operator Mode.
- Joystick failure occurs during motor control operation.
- The initialization of a subsystem fails.
- Retraction of stiff legs fails.
- Deployment of stiff legs fails.

– MAPS is unable to read [illegible] scanner data .

[illegible] position is read .

– MAPS is unable to read scanner data.

2.5 Workcell Controller

[The design principles for the workcell controller have not been created yet.]

2.6 Mobile Base

2.6.1 Tessellator's chassis and actuators are stiff. Tessellator's high stiffness design ensures the robot's accuracy (↑MB-SC1$_{(20)}$).

2.6.2 Omnidirectional wheels move the robot smoothly in any direction and over cable covers on the floor (↑MB-FR2$_{(19)}$, H3$_{(38)}$).

2.6.3 [illegible] rigid [illegible] provide a very stiff base [illegible] operate the manipulator (↑MAPS-FR3$_{(23)}$, H4$_{(38)}$). The base [illegible] and [illegible] on-board battery [illegible] nitrogen [illegible] (↑MC-SC2$_{(27)}$).

2.6.4 [illegible] can be commanded to descend [illegible] the base and contact the floor. Current threshold is used to determine contact and provide some indication of force. Once [illegible] reaches a particular [illegible] deployed to descend and contact the floor in order to provide a rigid [illegible] base. Before the mobile base moves, the stiff legs must be retracted. Current threshold is used to determine contact and provide some indication of force (↑H2$_{(37)}$, MAPS-SC5$_{(25)}$, MB-SC1$_{(20)}$) (←2.1.7$_{(53)}$).

Rationale: [illegible] based are not so [illegible] have a high durometer rating, they are compliant enough to affect accuracies and stability [illegible] manipulator arm [illegible] reach. [illegible] needed to lock out this compliance and provide a stable, non-compliant platform. In addition, in order to reduce the amount of [illegible] mobile base [illegible] required [illegible] (e.g., some tiles are above obstacles, such as [illegible], that the base cannot intrude upon), the manipulator arm must sometimes reach out beyond the perimeter of the base and additional stability is required under these conditions.

2.6.5 [illegible] the mobile base [illegible] materials [illegible] constructed [illegible] (↑MB-SC2$_{(20)}$, ↑H6$_{(39)}$).

2.6.6 Electrical compartments are sealed in aluminum enclosures and purged with gaseous nitrogen. Heat pipes cool the electrical compartments and the injection tool without circulating chemical-laden air through the electronic parts. (↑H6$_{(39)}$, MB-SC2$_{(20)}$)

Rationale: DMES is flammable as . Electrical components need to be isolated from the chemical .

2.7 Tile Servicing System

[The TSS design principles have not yet been created.]

2.8 Location Subsystem

2.8.1 The location subsystem provides the location of the robot in *world coordinates* (facility) with respect to a given position in the orbiter. To determine position with the required accuracy, the location subsystem uses a laser scanner and information from the vision system (see 2.12(85)) (↑LS-FR (27)).

2.8.2 A rotating eye-safe laser scanner reads bar-code targets that are precisely located in the facility. Triangulation from three or more of the bar code targets gives the robot position. As other location systems become available, this design may change.

Assumption: At least three bar code targets remain in sight of the location system at all times.

2.8.2.1 The laser scanner only takes position readings while the robot base is immobile (←2.4.1(61), 2.4.3.1(62), 2.4.5.4.2(65), 2.4.6.1(66)).

Rationale: The scanner triangulation calculations assume a static base and cannot correct the readings to take into account the robot base motion. If the positioning system changes, then this design principle may no longer hold.

Assumption: The scanner will be used for position determination at the beginning (the starting position) as well as for the final segment of each mid-course correction during computer-controlled movement.

2.8.2.2 The laser scanner must be initialized by the operator before use with the bar code reflector scanner codes (the location coordinates of the bar code reflectors). Any changes to these locations after initialization will be made by the operator (←T2.1(59)).

2.8.3 Reference Position correspondence is determined using three transforms. First, the orbiter position error that is known and measured as a normal procedure. This position and position error data provides the ability to compute an orbiter-to-facility transform. Second, the transform from the facility to the robot is given by the laser positioning system. Third, the vision system precisely identifies the work piece whose position on the orbiter is already known. Together, this information provides the ability to determine a precise robot-to-orbiter transform.

Rationale: Triangulation from three or more targets can give robot position to within centimeters, [illegible] which is precise enough to satisfy speci[illegible]. However, [illegible] tile positions are [illegible] The relative accuracy of the tile position can be [illegible] registered with the vision system [illegible] used for inspection [illegible].

2.9 Motor Controller

291 Mecanum wheels use a novel roller design to obtain three-degree-of-freedom motion in the plane, and pure rolling contact for accurate positioning, non -singular motions and precise final motions .

Rationale: The size constraints of the vehicle coupled with the close quarter operating in the OPF requires a locomotion system of navigation needed for high maneuverability (↑EA1(15), EA2(15)).

292 The locomotion drivetrains of the drive wheel hub has a diameter of consists of a brushless DC motor, for motor positioning, resolver and commutation, a brake, a cycloidal reducer providing 225:1 gear reduction with exceptional stiffness, and a locking hub that couples the output of the reducer to the wheel. The locking hub allows the operator to disengage the wheels from the drivetrain completely (↑MB-SC3(20), ←T8.6(60)).

Rationale: In an emergency, the ability to disengage the wheels allows for moving the machine out of by pushing the machine out of .

293 The drive system is able to move the robot over 10 cm high steps and up 20% grades (↑EA3(15)).

294 The drivetrain suspension is a simple rocker-arm design much like those on heavy construction equipment. This design is very simple and acceptable for the top robot speed of 30 cm/sec .

295 When commanded to do so, the motor controllers provide power to the motors in which drives the robot with a maximum velocity of 30 cm/sec . The motor controller accepts two types of commands . In *position* or *relative displacement* mode, the kinematics on the body relative (x, y,θ) desired position are computed and the robot is driven in the desired direction based on previously set acceleration and velocity values. In the second mode, the body relative velocity mode, (x, y,θ) velocity are computed and the appropriate wheel velocities are set. [More detail will be provided here on how these values are computed.] (↑MC-FR1(27), MC-FR2(27)).

296 All position (x,y) and rotation (θ) information must be provided to the motor controller in *relative* world coordinates (later 2 .4.2.6(62)).

29 The operator can set the normal and emergency acceleration and deceleration values or preset defaults can be used (↑MC-C1$_{(27)}$, T2.2$_{(59)}$). During a normal stop, the normal deceleration values are used. During an emergency stop, the robot will stop faster, using the emergency deceleration value (→MAPS-C2$_{(23)}$, MAPS-SC2.2$_{(25)}$).

30 The motion controller must be reset be - ing any error . It is safe to 3 seconds after the motion controller and the motion-generator properly (←2.4.1$_{(61)}$) .

2.10 Manipulator Arm

[illegible] [illegible] Tessellator customizes its up- [illegible] side o [illegible] camera [illegible] raises the [illegible] (the rest o ↑MB-FR3$_{(20)}$, [illegible] $_{(28)}$).

[illegible] k A physical interloc [illegible] used that does not allo the manipulator arm to be [illegible] stiff legs are retracted (↑H3$_{(38)}$, H4$_{(38)}$).

Rationale: [illegible] physical interloc- [illegible] constraints . S[illegible] may [illegible] physical [illegible] . Neither alone provide adequate assurance.

[illegible] [illegible] are deployed, the ma- [illegible] un [illegible]uration (↑H4$_{(38)}$, [illegible] PS-SC6$_{(26)}$). All [illegible]anipulator are designed to be manually operated should the need arise (↑MA-C1$_{(28)}$).

Rationale: [illegible] maintenance and servicing, it is e [illegible] .

[illegible] [illegible] to reach the tiles. [illegible] first, called Ma -Z, raises the arm vertically. A second vertical motion is [illegible] (↑MB-FR3$_{(20)}$).

Rationale: [illegible] because a single telescoping device could [illegible] combination o height, payload, and accuracy needed.

Atop these motions there is a 360 degree rotating motion.

[illegible] The manipulator [illegible] preloaded to [illegible] tools steady . All manipulator motions have absolute encoding to give [illegible] at all times, even in the event o ↑MA-SC1$_{(28)}$).

2.11 Injection Subsystem

2.11.1 The DMES injection system is controlled entirely by the TSS (↑TSS-FR1.3$_{(21)}$).

2.11.2 [Design principles not completed] (↑IS-FR2$_{(28)}$).

2.12 Vision Subsystem

2.12.1 The vision system is controlled entirely by the TSS (↑TSS-FR .2$_{(20)}$).

2.12.2 [Design principles not completed.] (↑VS-FR $_{(29)}$).

2.13 Digital Camera

2.13.1 At least one digital camera system is mounted in a position where it can provide the operator a view of the Tessellator robot. A second camera system is located on the mobile base and can transmit an image of the area in a 120 degree arc in front of the robot (↑DC-FR (27)).

Rationale: The digital cameras eliminate the need to make assumptions about [illegible] or not. The camera providing an image from above provides the operator with a view of the obstacles in the area all around the mobile base. The camera mounted on the mobile base itself provides the relative position of [illegible] the direction the operator should move the joystick [illegible] commands (↑H1).

2.13.2 (The images are sent directly to the operator interface ←2.2.3(58)).

2.14 System Log

[design principles not completed]

2.15 Safety Fuse

[illegible] [illegible] servo outputs and the motor [illegible] values, and [illegible] (smart ↑SF-FR1$_{(30)}$) [illegible]ively has t .

[illegible] [illegible] (event any parameter goes out o .g., motor current, enclosure [illegible]perature, or battery level), the sa [illegible] [illegible] (c ↑H5$_{(39)}$, SF-FR2$_{(30)}$).

[illegible] [illegible]or can query the sa [illegible]ions (↑SF-FR3$_{(30)}$, SF-FR5$_{(30)}$, OP4$_{(32)}$) (←T8.1.1$_{(60)}$).

[illegible] [illegible] (y a command ↑SF-FR4$_{(30)}$, ←T8.1.2$_{(60)}$).

2.16 Proximity Sensing

2.16.1 Proximity sensing (contact bumper strips) is used around the robot base and the manipulator arm for reactions (↑H1 (36), H4 (38)).

2.16.2 If the proximity-sensing system senses anything too close to the robot, it sends this information directly to the safety function (↑TSS-FR1 (20)).

Rationale: This is safer because instead of the operator alerted ... faster to stop the robot ... the operator can detect the receipt of the message from the proximity-sensing system and then release the deadman switch.

2.17 Aural and Visual Alerts

2711 The visual alert system has TBD colored flashing lights at TDB lumins visible from all locations at a TBM distance around the mobile base.

2721 The aural alert system provides a sound at TDB decibels ...

(↑AS-FIR$_{(3)1}$, AS-FR3$_{(3)1}$, MA PS-FR6$_{(23)}$)

2.18 Verification and Validation

This section includes requirements on and information about the verification and validation of the design principles included in this level of the Intent Specification.

2.18.1 Simulations

[*This section would include descriptions of simulations and either the results once they are completed or a reference to where the results can be found. Extensive simulations were done on TCAS, but we do not have the references or any information on the requirements (if any) that were developed for the simulations, so we have not included this information.*]

2.18.2 Experiments

2.18.3 Analysis

2.18.4 System Hazard Analysis

2.18.5 Other Validation Procedures

[*This section would include requirements for or descriptions of any other types of validation done on the system design.*]