Indoor Mapping

Hazard Analysis

Group 3

Abdel-Latif, Sari	0840264
Batth, Chanderdeep	0856000
Bishara, Marc	0858892
Elsaftawy, Mahmoud	0951912
Mansour, Ahmed	0857403
Wahid, Fahim	0965325

06/03/2014

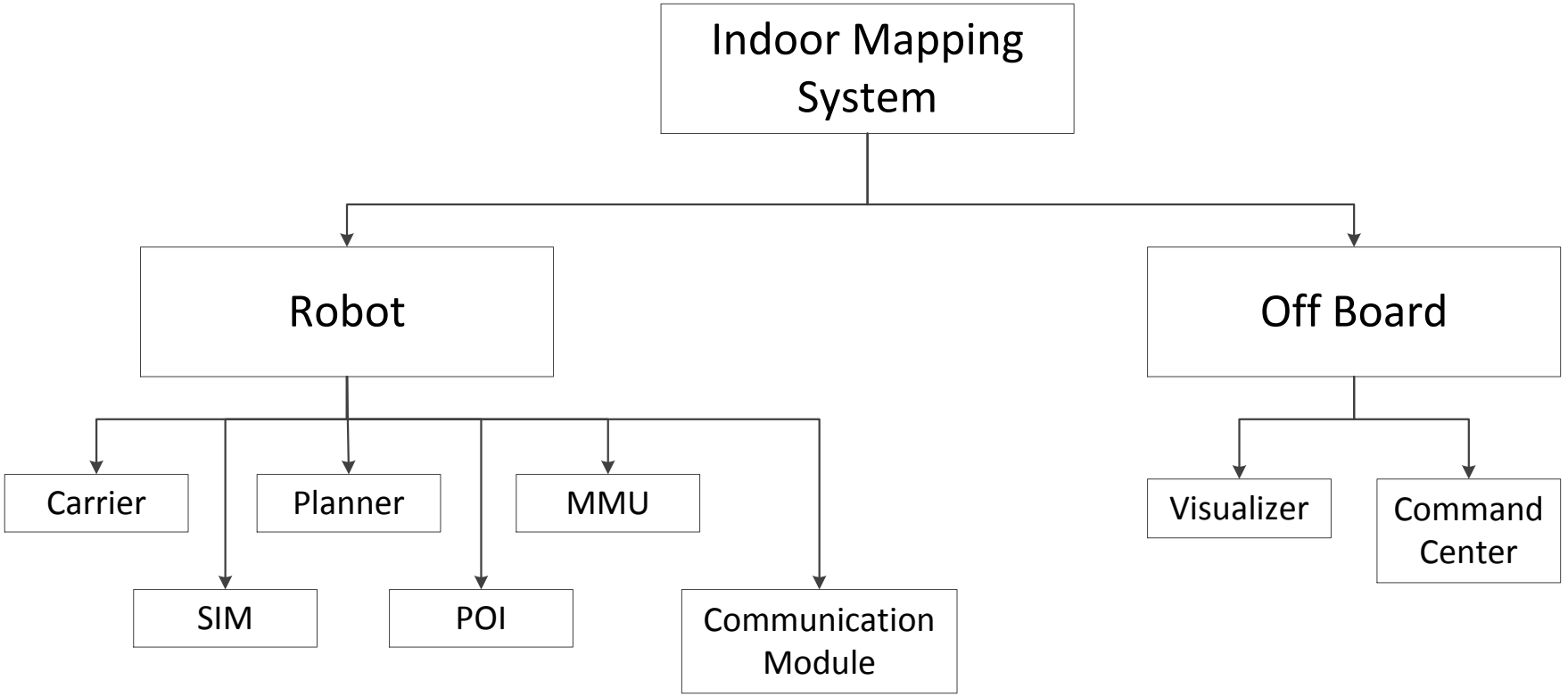
Revision Table

Version	Date	Author	Description
0.1	03/01/2014	M Bishara	Initial release
0.2	05/01/2014	M Bishara	Adding system modules breakdown and first entry in Hazard worksheet
0.3	06/01/2014	M Bishara	Added communication module
0.4	06/01/2014	F Wahid	Added Carrier Module
0.5	06/01/2014	A Mansour	Added MMU worksheet
0.6	06/01/2014	C Batth	Added POI worksheet
0.7	06/01/2014	M Elsaftawy	Added Planner FMEA Table
0.8	06/01/2014	S Abdel-Latif	Added Visualizer and Command Center
0.9	07/01/2014	F Wahid	Added SIM worksheet
1.0	07/01/2014	M Elsaftawy	Review and Minor Edits
1.1	07/01/2014	S Abdel-Latif	Formatting and Review
1.2	05/03/2014	C Batth	POI updated
1.3	05/03/2014	F Wahid	Carrier and SIM module updated
1.4	06/03/2014	S Abdel-Latif	Review and Formatting

Introduction:

This document details the results of Functional Failure Mode and Effect Analysis, hereby referred to with the acronym FMEA, which was conducted on the components of the indoor mapping system. The system's components are identified in this document to demonstrate the dependencies before leading into each component's FMEA analysis worksheet. The goal of this document is to identify modes of failure and risk mitigation steps that will be taken to prevent all hazards that can be predicted in the system's operation.

System Components Breakdown:



Failure Mode and Effect Analysis:

1. Carrier Module:

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Risk	Recommended Action	Ref.
E-Stop	Fails to stop the vehicle	Could cause physical accidents with surrounding environment	- Hardware not responding - Software bug	Catastrophic	- Have the carrier directly read from distance sensors and auto stop if unsafe distance detected	CAR_HA_01
E-Stop	Vehicle stopped after deadline	Could cause physical accidents with surrounding environment	- Hardware not responding - Response lag - Software bug	Catastrophic	- Increase the threshold for the distance to wall below which the E-Stop shall be triggered	CAR_HA_02
PID Controller	Reads undesired values from encoder	Will output undesired speed and angle	- Encoder not sensing - Delay exists in the encoder	Critical	- Give higher priority to the sensor reading task - Set upper limit for speed and acceleration	CAR_HA_03

1. Carrier Module: - Continued

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Risk	Recommended Action	Ref.
PID Controller	Lag in reading encoder value	Will output undesired speed and angle	- Encoder not sensing - Delay exists in the encoder	Critical	- Give higher priority to the sensor reading task - Possibly use interrupt to read encoder values	CAR_HA_04
PID Controller	Motor is slow to reach the desired value	Will output undesired speed and angle	- Too many gears - Stall and friction	Critical	- Oil the motors - Adjust the PID controller to compensate the delay	CAR_HA_05
Wheels Function	Wheel movement inconsistency	Slight difference in the two motor accuracies will cause the carrier to go off its specified course	- Difference in internal friction of each motor - Difference in surface friction	Marginal	- Directly control one motor, the Master, and let the other motor, the Slave, follow the Master by reading its encoder	CAR_HA_06

2. SIM (Sensor Interface Module):

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Risk	Recommended Action	Ref.
Distance to Wall Sensing	Detect incorrect distance	Incorrect map generated as well as inability to detect sub-halls	- Hardware not responding - Software bug - Missed response	Critical	- Quick Test option is available and recommended before use - Software check of unreasonable values	SIM_HA_01
Distance to Wall Sensing	Detect noise	Will generate noisy wall and/or false wall detection	- Noise in sensor - Vibration in Carrier - Too accurate sensor detecting microscopic roughness on wall surface	Marginal	- Software will use line of best fit instead of connecting each point	SIM_HA_02

2. SIM (Sensor Interface Module): - Continued

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Risk	Recommended Action	Ref.
Distance to Wall Sensing	Wall not detected	Could cause physical accident with the undetected wall	- Connection Failure	Catastrophic	- Use constant logging to check the sensor readings - Solder the wire	SIM_HA_03
Tracking Orientation and Distance Moved	Incorrect Distance and Orientation	Wrong sense of current location and generation of a not-to-scale map	- Inaccuracy in accelerometer and gyroscope	Critical	- Use encoder as secondary feedback - Use front distance sensor to calculate movement - Round orientation to the nearest 90 degree assuming hallways are right angled.	SIM_HA_04

3. Planner Module

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Risk	Recommended Action	Ref.
Driving Functionality	Unable to send commands to Carrier module	The Carrier module will only execute the last command sent to it and will eventually hit a wall	- Faulty communication line - Software bug - Buffer overflow	Catastrophic	Force system shutdown if more than three commands are not received by the Carrier module	PLN_HA_01
Path Planning	Reading faulty or inaccurate values from the distance-to-wall sensors	- Will cause the Planner to produce an incorrect path for the Carrier - May cause the Carrier to drive into a wall	- Inaccurate sensors - Slow processing speed causes delay in sensor readings which may lead to missing critical deadlines	Critical	Use multiple high quality sensors to reduce the probability of getting bad readings	PLN_HA_02
Lost in Space	Planner loses track of the Carrier location in the map	Planner will not be able to map the whole floor, therefore failing to meet system requirement SR_3.1	- Software bug - Defective IMU (Inertial Moment Unit) which causes big tolerances when keeping track of the system location	Critical	Perform system reset and restart mapping process	PL_HA_03

4. POI Module

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Risk	Recommended Action	Ref.
Image Capturing	Blurry/Unclear image taken	Unable to extract relevant information from the image	- Carrier moving too fast - Low lighting condition	Marginal	- Take multiple pictures at different angles - Ensure the hallway is well lit - Sharpen the images using Image Processing techniques	POI_HA_01
Object Detection	Fail to detect doors	- Failure to take an image of desired point of interest - No information extracted about desired point of interest	- Software bug - Program busy processing previous data	Critical	- Ensure use of effective object detection techniques - Create a thread for executing image processing portion of the module - Create a separate thread for OCR portion to ensure it does not block the main program	POI_HA_02
Image Capturing	Fail to capture tags associated with the door	Unable to extract information about point of interest	- Image captured too early	Critical	- Ensure top left point of door contour is at certain point on capture frame	POI_HA_03

Location Association	Failure to associate location data with OCR data, or vice versa	- Sending incomplete information - Unable to determine location of point of interest on 2-D map - Unable to determine information about point of interest on map	- Software bug	Critical	- Ensure that every data packet sent out contains full information - Incomplete data packets must be discarded and Planner must be notified to go back to certain location to retake an image	POI_HA_04
Communication	Failure to send/receive data to/from Communication Module	- No information about points of interest on 2-D map - Unable to obtain location data - Unable to send relation coordinates to Planner	- Communication failure between POI and Communication module	Catastrophic	- Use watchdog timer to ensure communication is active - Use of TCP protocol to ensure reliable connection and data transfer - Create a thread for consistent communication with the module	POI_HA_05
Character Recognition	Failure to retract correct information from an image	- Image not clear - Characters are too small to read	- Image captured from distance	Critical	- Zoom in on image -Sharpen image after zooming in - Save images as contours - Use of redundancy and majority voting scheme to ensure information is correct	POI_HA_06

MMU Module:

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Risk	Recommended Action	Ref.
2D map	The 2D map is out of tolerance	Map generated by the system will fail to meet minimum system requirements	- erroneous sensors - weak mapping algorithm	Catastrophic	Improve mapping algorithms and rerun the system through target environment	MMU_HA_01
Pose	The pose of the robot within the world is out of tolerance	- Map generation will have added error - POI module output will be false - Planner will fail to correctly navigate - Visual pose will be incorrect	- erroneous sensors - weak pose prediction algorithms	Catastrophic	Improve pose prediction algorithms and rerun the system through target environment	MMU_HA_02

5. Communication Module

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Risk	Recommended Action	Ref.
Buffering Messages	- Buffer overflow - Messages get corrupted	Missed communication can cause unintended behavior	Unknown	Marginal	Use large Buffer space dynamically allocated	COM_HA_01
Sending and Receiving	Failure to transmit message	Missed communication can cause unintended behavior	- Hardware line failure	Critical	Keep watch dog on communication lines	COM_HA_02
Watchdog on communication channels	Watchdog fails to trigger E-Stop	Critical communication errors un-noticed can cause unintended behaviors	- Software error	Catastrophic	- Keep watchdog on separate software thread. - Wire it to main power source to shut down system.	COM_HA_03

6. Visualizer

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Risk	Recommended Action	Ref.
Build 2D visual map	Visual representation is wrong	Visual 2D is incorrect and product is useless.	- Software bug - Algorithm used to build 2D map is faulty	Critical	- Run validation and testing to clear any bugs - Test algorithm and compare results to actual blueprints	VIZ_HA_01
Assign POI to 2D visual map	- POI data is incorrectly placed on Visual Map - POI data is faulty/corrupted	2D Visual map has faulty data and thus unusable.	- Software bug - Algorithm used to place POI on 2D map is faulty	Critical	- Run validation and testing to clear any bugs - Test algorithm and compare results to actual blueprints	VIZ_HA_02

7. Command Center

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Risk	Recommended Action	Ref.
Receiving Message	Communication lost with Vehicle messages corrupted	- No monitoring will be possible of vehicle - Faulty monitoring Data	- Vehicle out of reception range - Software Bug in receiving client	Critical	- Store local copies of monitoring data on vehicle - Have backup connection method utilizing internet instead of p2p connection - Run thorough validation and testing on off board software	COC_HA_01
Send E-Stop signal	Communication lost	Vehicle can't be stopped remotely	- Vehicle out of reception range and/or vehicle lost internet signal	Catastrophic	Have backup connection method utilizing internet instead of p2p connection	COC_HA_02