7309 – Systems Reliability Engineering

FMECA Report for Transforming Robotic System

Name: *Hareish Raghupathy*
SMU ID: *49005624*
Date: *11/14/2023*

Product Description:

We have seen groundbreaking innovations and improvements in the fields of AI, machine learning, robotics, and their computational performance over the recent years. There is AI enabled transportation for people autonomously and there are these personal robots being used currently for various tasks to aid in day-to-day tasks. Yet, there is no product that can provide both.

The solution for every separate problem exists but a single solution for all the problems does not. The key opportunity for our product is the creation of an ultimate entity which can prove to be one solution to a person needing both transportation and personal assistance. It is a revolution in terms of the integration as it brings transport and personal assistance with robotic technology to next levels.

The world has changed, people now carry an entity like a smart phone for all their needs instead of carrying a separate piece of tech for every need. A smart phone has replaced the need for carrying physical documents, wallets, and watches. The key to designing this system is the sole integration of the idea of transport and robotics to provide the ultimate assistant that can do every task for the people under their command. Since the system operates on electricity it also brings quality of life improvements as well as reduction of running cost in the longer run for the users.

Ground Rules and Assumptions:

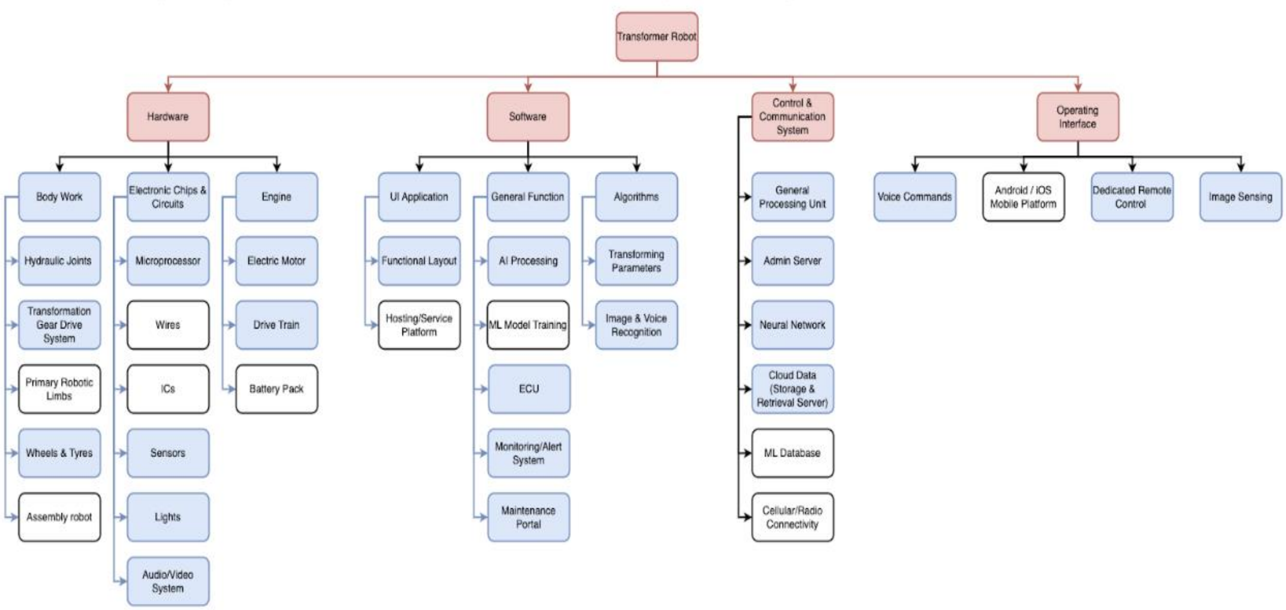
- The system has the advanced AI and ML models to interpret the human language.
- The system has access to all the AI libraries online and can make informed decisions by itself.
- The robotic system can physically transform into a two-wheeled, single seated vehicle when commanded.
- The system does not measure more than 7 ft in height and 2 ft in width.

- The system can carry only one passenger at a time with its hybrid vehicle-humanoid structure.
- The system can get into houses and transport its user on the motorway autonomously.
- The system has live updates to its firmware, AI, and ML models.
- The system is licensed for usage by the government and private firms.

Block Diagram:

<u>Component level Diagram:</u>

This is a high-level component view of the proposed system along with its subsystems. This can also be used to identify the Failure Areas along with the Hot Spots which can aid while planning for Mitigation.



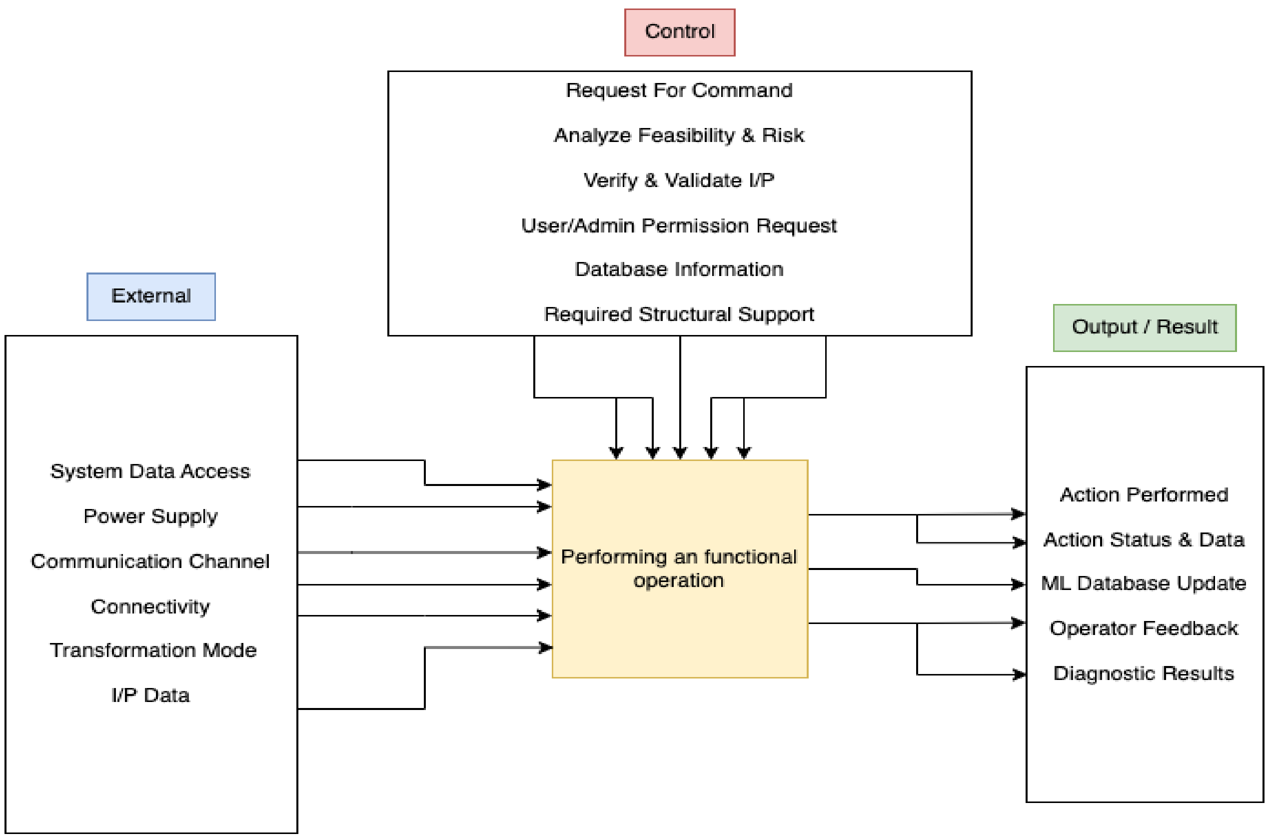
<u>System Level Decomposition for Traceability:</u>

1. Transformer Robot
    - 1.1 Hardware
        - 1.1.1 Body Work
        - 1.1.2 Electronic Chips & Circuits
        - 1.1.3 Engine
    - 1.2 Software
        - 1.2.1 UI Application Software
        - 1.2.2 General Function Software
        - 1.2.3 Algorithms
    - 1.3 Control and Communication System

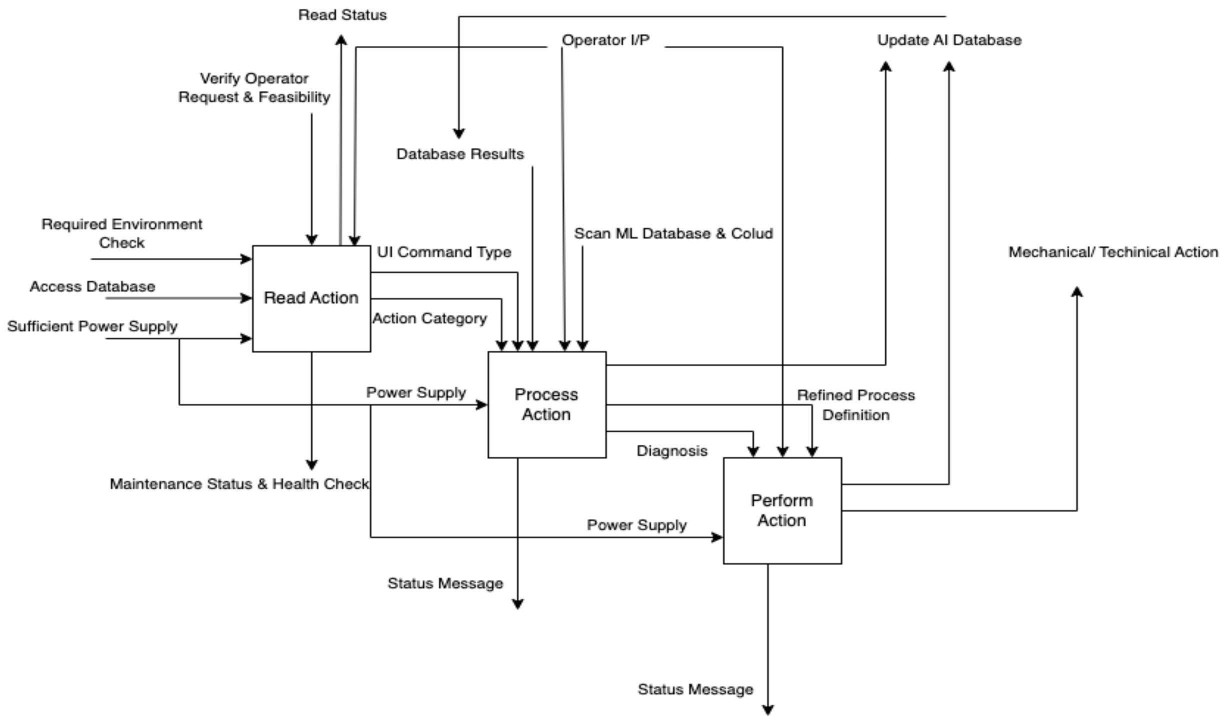
1.3.1 General Processing Unit
1.3.2 Admin Server
1.3.3 Neural Network
1.3.4 Cloud Data
1.3.5 ML Database
1.3.6 Cellular Connectivity
1.4 Operating Interface
1.4.1 Voice Commands
1.4.2 Android/iOS Platform
1.4.3 Dedicate Remote Control
1.4.4 Image Sensing

Functional level Diagram:

Here is the **functional layout for the system with respect to its inputs, controls, and outputs** for every command.



Diving deeper into it, we can see **how the inputs given by the user is processed by the system here at the lower level**:



Failure Mode Effect Criticality Analysis:
(Refer Excel for the FMECA Sheet)

These are the 14 failure modes identified in 7 components of the above system.

1. Electronic Chips/Circuits: [Traceability: 1.1.2]

- This part of the system could fail due to **over loading of microprocessor** due to data input leading to the system to perform wrong actions or no actions.
- **Integrated chips** are manufactured in large amounts today; hence it is possible for it to be instable due to various reasons in an operating environment. This could cause unresponsiveness which is plainly called 'not working' in customer terms; this could cause the user/customer to lose faith in the company's reputation.

2. Physical Body Work: [Traceability: 1.1.1]

- A problem with the **transformation gears** or **hydraulics** could influence the high-level transformation process of the robotic system and its transformational integrity. This could lead to the system's output to be out of phase with the input given or potential delay due to friction at the assembly level.

3. Engine: [Traceability: 1.1.3]

- Being an electric powered engine, an **electric surge** in the battery circuitry could cause the whole system failure due to shorting due to shut down or shorting.
- Battery health or **battery discharge rate** is a vital metric in our system which is a fully battery powered robotic vehicle. Any excessive charging or over clocking the

engine could accelerate it degradation rate easily. This, down the road affects the longevity and total uptime of the system.

4. UI Application: [Traceability: 1.2.1]

- This is the software component that enables the user to control the system interface and its actions. This is connected to the service provider's server that has all the functionality for the robot. An **overload caused in this server** could potentially break the communication between the user and system giving it no inputs to act on.
- Any **application bug** in this system might cause the input of an unexpected command while also increasing the down time as the bug must be fixed.

5. General Function Software Module: [Traceability: 1.2.2]

- This has the main software component at the functional level for the operation of the system. An **inaccuracy in AI or ML** module in this could lead to wrong or inaccurate data being sent to the action center of the system causing inappropriate actions or physical hazards.
- Failure in a **sensor** can have similar effect giving wrong or no inputs in some cases which affects or given no output for the command provided by the user.

6. Algorithm: [Traceability: 1.2.3]

- This compartment contains the development level coding for the individual components and the system at a higher level. Any disruptions or inaccuracy in the **Image** or **Voice recognition system** due to incompetent coding or sensors could lead to wrong inputs potentially causing accidents too.

7. Cloud Data (Storage/Retrieval): [Traceability: 1.3.4]

- A **could platform failure** due to issues like connectivity or network could lead to the failure in storing or fetching data from the cloud. This could cause performance issues with respect to the system's ability to make decisions based off the data which will in turn cause the system to idle.
- **Hacking of cloud data** is extremely sensitive to the whole system as it might lead to stealing of information or seizure of platform control causing safety and security related problems to the users and business alike.

Results/Recommendation:

Let us looks at some **mitigation methods and recommendations** for the above-mentioned failure modes in each of the 7 systems selected for this report.

The Pre-Risk Priority and Post-Risk Priority Number is indicated in the excel worksheet. The rubric followed for its computation is attached below:

Risk Priority Number = Severity x Occurrence x Detection

Severity: *The severity of the failure mode is rated on a scale from 1 to 10. A high severity rating indicates severe risk.*

Occurrence *(or* ***Probability****): The potential of failure occurrence is rated on a scale from 1 to 10. A high occurrence rating reflects high failure occurrence potential.*

Detection: *The capability of failure detection is rated on a scale from 1 to 10. A high detection rating reflects low detection capability.*

Src: RPN Scale Definition-IQA System

1. Electronic Chips/Circuits: [Traceability: 1.1.2]
- Micro Processor Overload:
- Introduction of a load divider circuit to prevent the overloading of the microprocessor.
- Overload alert mechanism to indicate the user in advance before the component gets damaged.
- Integrated Chip Instability:
- Introduction of a fuse relay circuit along with an emergency data recovery path if the instability is detected by the system.

2. Physical Body Work: [Traceability: 1.1.1]
- Transformation Gear:
- Add a pressure sensor to see if there is a change in operating pressure of the gear or an overload in torque.
- Hydraulic Joints:
- An additional step in operating manual to perform a pre-loading check before the operation to assess its real time load capability.
- Post the assessment, introduce an alert system to indicate the user if there is any fault in the hydraulics to prevent accident.

3. Engine: [Traceability: 1.1.3]
- Electric Surge:
- Couple a power stabilizing unit to the engine to mitigate the surge .
- Deploy a fuse relay circuit to safeguard against fire accidents as a secondary protection.
- Battery Health/Discharge Rate:

- Allow charging only via proprietary charger to optimize the charging as specified by the manufacturer.
- Over clocking the engine is restricted to the user beyond safe levels unless and until the customer accepts risks via submitting a request to the robot factory officially.

4. UI Application: [Traceability: 1.2.1]

- <u>Server Overload:</u>
- Deploy a load balancer to divide the incoming traffic into the application server.
- <u>Application Bugs:</u>
- Provide an alternate portal through which the user can still use the application without updates as the current update is ongoing. This reduces the down time as well.

5. General Function Software Module: [Traceability: 1.2.2]

- <u>AI & ML Processing:</u>
- Improve the AI & ML efficiency by giving special case human training to it especially in the identified defect areas.
- <u>Sensor Failure:</u>
- Implementation of an alert system to warn and indicate any failed sensor in the system.

6. Algorithm: [Traceability: 1.2.3]

- <u>Image Recognition:</u>
- Feedback loop to qualify the quality and information in the image taken before usage.
- <u>Voice Recognition:</u>
- Recalibrate voice recognition to the saved user's voice and eliminate the background noises before taking in the command to mitigate errors.

7. Cloud Data (Storage/Retrieval): [Traceability: 1.3.4]

- Cloud Platform Failure:
- Deployment of a secondary server and network as a backup during the event of a failure.
- Cloud Data Hacking:
- Protection measures through firewall and PEN testing methods against malware attacks.
- Use data encryption to mitigate the probability of hacks.

Note: Once all the above recommendation action are implemented the initial RPN total of 2580 is reduced to 438. (Refer Excel Worksheet)

References:

https://smu.instructure.com/courses/116810/files/folder/Class%20Project?preview=8221087 (In Class)
https://smu.instructure.com/courses/116810/files/folder/Class%20Project?preview=8221086 (In Class)
https://smu.instructure.com/courses/116810/files/?preview=8634414 (In Class: Slides 37 to 46 in particular)
https://smu.instructure.com/courses/116810/files/?preview=8374202 (In Class)
https://paperswithcode.com/method/rpn
https://missionreadysoftware.com/wp-content/uploads/2020/01/SFMEAoverview.pdf
https://feaforall.com/failure-modes/
https://www.iqasystem.com/news/risk-priority-number/

End of Report - Thank You!