e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

INTEGRATED FRAMEWORK TO IDENTIFY FAULT IN HUMAN-MACHINE INTERACTION SYSTEMS

Ashwin Kavasseri Venkitaraman[*1], **Venkata Satya Rahul Kosuru**[*2]

[*1]MS (Electrical Engineering), Independent Researcher, Fremont, CA, USA.

[*2]MS (Electrical and Computers Engineering), Independent Researcher, Sunnyvale, CA, USA.

DOI : https://www.doi.org/10.56726/IRJMETS30184

ABSTRACT

Safety is a critical concept that determines the viability of the technology and large-scale acceptance. With recent advancements in autonomous vehicles and eVTOLS (electric vertical take-off and landing systems), it is imperative to have robust safety strategies to identify and mitigate faults. A safety strategy needs to be undertaken before product development to ensure systemics failures and random faults are determined early in the development phase and risks are ensured to be within acceptable limits. This paper proposes an integrated framework to identify potential faults in generic human-machine interaction systems. For this reason, our study is limited to Level 4 autonomous systems with high driving automation as opposed to full driving automation. The study aims to provide a generic approach to achieving the targeted level of safety for a system. An integrated framework provides a path for continuous improvement and overlapping failure analysis methodologies. The paper encompasses Failure mode effect analysis (FMEA), Fault tree analysis (FTA), Preliminary hazard analysis (PHA) and System theoretic process analysis (STPA).

Keywords: Functional Safety, STPA, STAMP, FMEA, FTA, PHA, ISO26262, UL 4600.

I. INTRODUCTION

Human-machine interaction systems range from touchscreen and keyboards to fighter jets and submarines. The need for stringent regulations increases with complexity and hazard factor associated with improper functioning of these systems. In this paper, we discuss ISO26262 and UL 4600 safety standards that provide suggestive practices that help manufacturers present an auditable and evidence-based safety case (1). As part of the standard, we will discuss existing methodologies to identify fault and propose an integrated framework. The methodologies include Failure mode effect analysis for software and hardware that discusses single point faults, fault tree analysis that incorporates single and multi-point faults, preliminary hazard analysis provides a qualitative risk assessment and systems-theoretic process analysis that encourages a proactive analysis using STAMP (system theoretic accident modeling processes).

Fault in a system is termed as an undesirable event that causes the system to malfunction. Faults are generally perceivable, and, in some cases, they cascade with time. Faults can be caused due to hardware failures, software failures or external factors. Failures can be controlled or reduced at design stage leading to reduced number of faults. Safety concept to mitigate these faults need to be developed beyond limiting to loss of life or injury. It should encompass any unacceptable situations that can be prevented. (2)

Systems comprise of hardware and software; hence system failures are a result of either hardware or software faults. Hardware faults are random or systematic while software faults are only systematic. Considering that the nature of faults is different, it is imperative to have different means to identify faults, quantify and mitigate them.

Hardware faults can be quantified easily; however, they need to be addressed qualitatively as well. Software faults are mostly itemized and classified qualitatively as they are systemic in nature and do not have probabilistic values associated with their occurrence.

This paper discusses the different techniques in use to identify faults and provide an integrated framework.

FMEA is an inductive methodology to enumerate different ways the hardware/software can fail. FTA is a deductive methodology that associates probabilistic values to system components to derive the overall failure metric. STPA uses a control structure approach to identify unsafe control actions and causal scenarios.

PHA is a qualitative analysis methodology that is highly subjective in identifying and classifying faults.

II. OBJECTIVES OF RESEARCH STUDY

The objective of this research will primarily be to establish benefits and drawbacks of existing analysis techniques to detect fault; and propose an integrated framework with improvements.

The paper also proposes areas of improvement to each of the analysis techniques such as incorporating fuzzy logic in FTA, utilizing Model based design such as SysML or UML within STPA.

Research Questions

- What are the different analysis techniques used to identify potential faults in a system?
- Is there an overlap between different analysis techniques?
- Is there scope for improving current analysis techniques to keep-up with more automated systems?
- How can existing analysis techniques be integrated into a common framework for use across all human-
- machine interface systems?
- Is the proposed framework specific to a particular domain or can be used across different industries and domains?

Objective for Design FMEA

We discuss the different techniques used to determine potential faults and their effect on the overall system as opposed to identifying faults after their occurrence. Using lane-keeping feature as an example, however trying to keep the methodology as generic as possible for easy reuse in other applications.

A. Preliminary hazard analysis

Preliminary hazard analysis (PHA) is done prior to or in the initial stages of product development. It involves identifying faults together with discussing the features of the product.

Steps involved in performing PHA of a system:

a. Draw block diagram of system, interfaces, and system boundary.
b. List functions of the system
c. Identify deviations from intended operations
d. Classify impact of individual deviations on a system level.

Table 1: PHA template

Hazard Identified	Hazard Classification	Safety Goal	Safe State
Over/under steer	Critical	Vehicle should alert driver on deviating from lane and should remain within threshold to avoid crash	Detect and hand over control to driver
Driver did not react	High Impact	Lane keep assist system shall monitor driver alertness and provide warning to keep driver responsive	Warn driver and disable lane keep assist feature for rest of journey
Communication loss between steering column and actuator	Critical	System shall be robust to avoid communication loss and implement redundant communication channels	Warn driver and go to limp home mode
Torque provided more or less than needed	High Impact	Vehicle should alert driver on deviating from lane and should remain within threshold to avoid crash	Detect and hand over control to driver

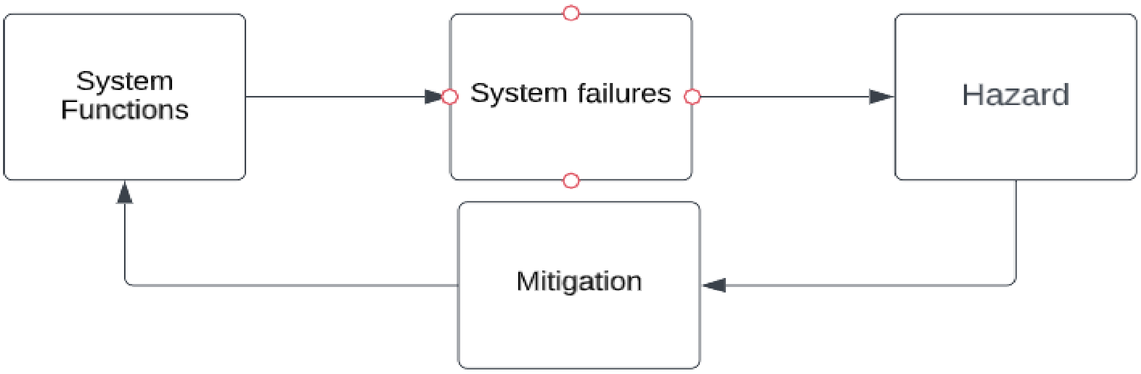

Figure 1: PHA architecture

Table 2: PHA on Lane-keep assist system

Hazard Identified	Hazard Classification	Safety Goal	Safe State
Oversteering	Severe	Maintain lane	Warn driver
Understeering	Critical	Maintain lane	Warn driver
Unintended steering action	Severe	Maintain lane	Warn driver
Unintended steering inaction	Critical	Maintain lane	Warn driver

B. Failure Mode Effect Analysis

Failure mode effect analysis (FMEA) can be classified as system FMEA, hardware FMEA, process FMEA and software FMEA. Considering a generic framework with the intent of achieving an inductive analysis methodology, we tweak existing SAE guidelines to achieve the spirit of adhering to ISO 26262.

Steps in generic FMEA – (3)

a. List components (hardware or software), functions or process steps
b. Identify failure mode
c. Analyze impact of failure to higher level system
d. Quantity the failure in terms of severity (S), occurrence (O), and detection (D)
e. Obtain risk priority number (RPN) to prioritize faults
f. Propose mitigation mechanisms
g. Reassess impact and risk priority number

Table 3: FMEA template

Component	Failure Mode	Impact of failure	S	O	D	RPN	Mitigation
Steering column	Over/understeer	Can result in crash	8	4	5	160	Redundant sensors to detect lane markings, robust software design reviews and using hardware with low failure rate
Communication bus	Missing message, loss of communication, checksum/counter loss	Vehicle goes to limp mode	7	6	3	126	Alert the driver to pull over, service the vehicle
Actuator	Unresponsive or over sensitive	Unintended steering motion action/inaction	8	3	7	168	Increase reaction time within reasonable limits and reduce sensitiveness of the motor/actuator system

C. Fault Tree Analysis

Fault tree analysis (FTA) is a deductive approach that assigns probabilistic values to individual failures, assuming the components fail independently. FTA assigns the system failure metrices and reliability values based on a stochastic combination of failure rates of individual elements.

Steps involved in developing FTA –

a. Identify System failure modes
b. Identify failure of components that could result in system failure
c. Relate component failure to system failure using logical and relational operators
d. Populate them in a block diagram
e. Assign reliability values and other safety metrics to each component
f. Obtain system level failure and reliability metric based

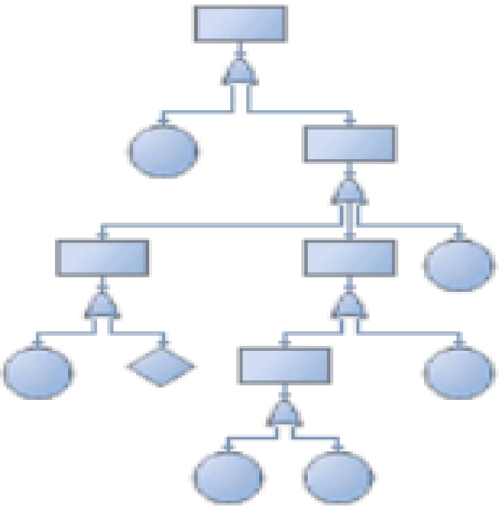

Figure 2: Sample FTA structure

D. Systematic-theoretic process analysis

Systems-theoretic process analysis approaches failures as restricted control problems, considering the failure modes as constraints within the boundary of which the system should effectively continue to respond. It includes human in the loop to identify failures, which is different from other failure analysis techniques discussed so far.

STPA uses a system engineering approach and has been often compared to FMEA, HARA, HAZOP, FTA. Unlike other approaches, STPA recognizes that system failure cannot always have a stochastic relation with component failures, especially when they are not independent or involves software or human interaction.

STPA technique can be applied during any stage of the system life cycle. When this technique is used for safety-guided design, it allows for safety constraints and requirements to be refined and traced to individual subsystems and components. (4)

STPA can be integrated system engineering process and into model-based system engineering.

The methodology cites several real-world examples of failures due to human error which is often not probabilistic.

Steps involved in formulating a STPA: (5) (6)

a. Identify unsafe control actions

In this step, all control actions that could lead to unsafe response are mentioned, each of which are the table is filled

b. Identify causal factors and create scenarios

Causal factors are elucidated for each hazard/fault case along with interaction of the components with other systems. For example, consider the faults of loss of communication to steer the vehicle; this could be due failure/malfunction of components or its interaction with other vehicle systems like adaptive cruise control.

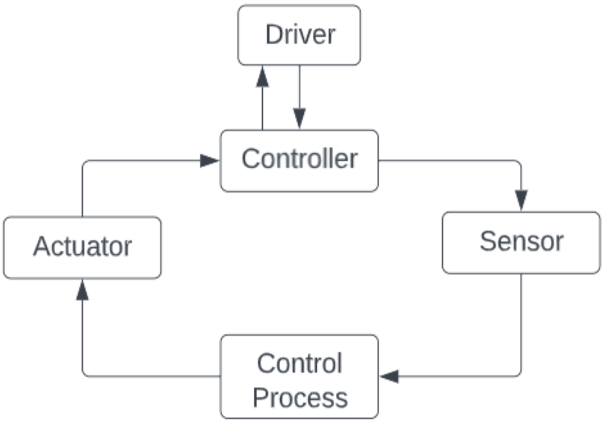

Figure 3: Sample STPA block diagram

Table 4: STPA on Lane-keep assist system

	Not providing causes hazard	Providing causes hazard	Incorrect timing/order	Stopped too soon/applied too long
Steering	Vehicle drives out of lane	Unexpected path deviation out of the lane	Steering request sent to vehicle control system earlier or longer than expected	Steering request sent to vehicle control system earlier or longer than expected
Torque	Vehicle drives out of lane	Unexpected torque to steering	Torque request sent to vehicle control system at incorrect time	Torque request sent to vehicle control system earlier or longer than expected
Communication	Vehicle control system is not aware of steer request, response unknown	**X**	Vehicle control system is not aware of steer request, Response unknown	**X**

STPA does not identify faults, instead it is used for hazard identification – which is a superset of faults. Hence, hazards are always referred to the system as a whole and not individual components.

III. INTEGRATED FRAMEWORK

Considering the traditional fault analysis techniques and STPA; weighing the pros and cons of each of these techniques, we would like to propose an integrated framework that uses system engineering and model-based design principles as baseline.

a. Overview

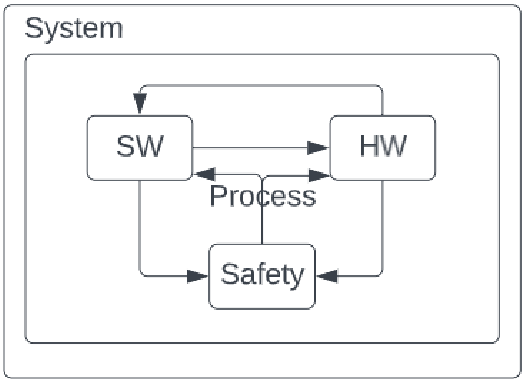

Figure 4: Integrated Framework

The framework involves considering each component of the system viz., software, hardware, safety, and process to be individual systems in themselves. Each of them having bidirectional traceability with –

a. Requirements

b. Safety metrices (reliability data, experimental failure rate, SW and HW architecture, severity, occurrence, detection, risk priority number)

c. System metrices (Code coverage, redundancy analysis, impact analysis)

d. Code

e. Hardware circuit

f. Test results

Table 5: Integrated framework analysis matrix

a	b	c	d	e	f
✓	X	✓	X	X	X
X	✓	✓	✓	✓	✓
X	✓	X	X	X	X
✓	X	X	✓	✓	✓
X	✓	✓	✓	X	X

b. Divide-conquer the analysis elements

In this we divide/classify the types of analysis techniques based on the nature of obtaining the fault conditions.

1) Qualitative analysis

Qualitative analysis is subjective analysis that is obtained mostly by discussion with focus groups, surveys case studies and discussions. In this, extensive deliberations are involved to identify anomalous behavior due to environmental conditions, unforeseen circumstances, abnormal human behavior, or response.

2) Quantitative analysis

Table 6: Integrated framework spreadsheet

Requirement	Component	Failure rate	S	O	D	RPN	Test data	Type of Fault
Steering controller shall arbitrate and provide steer requests based on sensor signal and camera feed data, considering vehicle speed.	Steering column	4x10e-6	8	4	5	160	Vehicle test	Primary
The Ethernet/CAN bus shall communicate the arbitrated steering requests to the actuator system	Communication bus	7x10e-6	7	6	3	126	Simulation test	Secondary
The actuator shall respond by providing	Actuator	3x10e-6	8	3	7	168	Vehicle test	Primary

requisite power to individual wheel motors to cause safe steering action.								

IV. RESULTS AND DISCUSSION

While PHA, FMEA and FTA have been traditionally used to classify faults, with increased complexity in systems it becomes imperative to explore new and robust analysis techniques. STPA is one such technique, that is useful in analyzing complex systems. STPA focuses on three basic concepts – safety constraints, hierarchical control structure, and process models.

In this paper, fault analysis methodologies have been discussed for lane-keep assist feature considering human in the loop. The analysis begins with identifying system level requirements, hardware and software specific requirements, processes, and relevant safety standards. Using this information, faults are identified and prioritized based on impact to overall system. STPA and integrated framework identifies unsafe control actions, analyses causal functions. The study can be extended not only other automobile functions, but other semi-autonomous systems that rely on human intervention as means to achieve safe state. The information does not represent an actual system design or proprietary information, but instead discusses means to analyze a complex system and achieve a fail-safe architecture.

The analysis identifies the safety constraints that were violated for a hazard to occur and investigates the inadequacy of the controls designed to enforce the safety constraints. (7)

The proposed framework combines STPA with traditional analysis techniques, while addressing gaps of traceability, errors or oversight in software architecture, attachment of test artifacts. Including these increases confidence in the work product and adherence to relevant safety standards.

The proposed methodology can also be utilized as a part of general system engineering methodology because the safety concept, safety goals and fault determination can be modified as and when the design, requirements, and product features change. Coverage analysis proposed in the integrated framework can reduce oversight in identifying failure modes/scenarios.

V. CONCLUSION

From this analysis it has been identified that systems do not have stochastic relation to the components that constitute it, especially when human factors and external factors are involved.

Additionally, though each fault analysis methods have their own pros and cos, there is a need to have overlapping fault analysis methods to reduce chances of oversight or utilize an integrated framework that encompasses humans, external conditions, system processes along with hardware and software factors.

The proposed integrated framework lays a foundation on achieving comprehensive fault analysis. However, it has scope for further development, to enable use for higher levels of autonomous systems (Level 4 and 5), aircraft systems and other systems moving towards complete automation. There is scope to develop a software tool that tracks development and modifications to individual safety case. The paper discusses FMEA, FTA, PHA and STPA as is, without considering the recent advancements in utilizing fuzzy logic, Markov chain, back-propagation, and other machine learning concepts. Future work can incorporate these recent advancements while discussing the framework.

While the study and proposed framework aims to be generic and easily transferable to different kinds of systems, a mindful approach should be undertaken for using it in some unique type of systems.

VI. REFERENCES

[1] https://ieeexplore.ieee.org/document/9256608

[2] http://psas.scripts.mit.edu/home/wp-content/uploads/2016/01/Systems-Theoretic-Process-Analysis-STPA-John-Thomas.pdf

[3] Society of Automotive Engineers. (1994). Potential failure mode and effects analysis in design and potential failure mode and effects analysis in manufacturing and assembly processes. (SAE J1739). Warrendale, PA: Author

[4] https://www.engr.colostate.edu/~sudeep/wp-content/uploads/j41.pdf

[5] Ana Elsa Hinojosa Herrera, Chris Walshaw, Chris Bailey, Chunyan Yin, "Failure Mode & Effect Analysis for Improving Data Veracity and Validity", 2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE), pp.100-105, 2019.

[6] Kohsuke Namihira, Hiroki Umeda, Sho Kurahayashi, Kazuhiro Sogawa, Kazuki Kakimoto, Naoko Okubo, Yasushi Ueda, "Visualization Method to Stimulate Ideas Leading to Failure Mode in Software FMEA", 2019 IEEE Aerospace Conference, pp.1-9, 2019

[7] Application of systems theoretic process analysis to a lane keeping assist system Haneet Singh Mahajan∗, Thomas Bradley, Sudeep Pasricha College of Engineering, Colorado State University, Fort Collins, CO, United States.