Data Driven Safety Analysis and Fault Prediction

Table of Contents

1. Preface

In the rapidly evolving automotive landscape, ensuring the safety and reliability of electronic control units (ECUs) is of paramount importance. The increasing complexity of automotive systems, coupled with the emergence of autonomous driving technologies, necessitates a robust and comprehensive approach to safety engineering. This document presents a data-driven methodology for addressing both conventional safety concerns and the emerging challenges posed by Safety of the Intended Function (SOTIF).

By harnessing the power of data and adopting a systematic approach to analysis, design, and validation, this methodology aims to enhance the overall safety and dependability of automotive ECUs. The insights and guidelines presented herein are intended to assist engineers, researchers, and practitioners in developing automotive systems that meet the highest safety standards and provide reliable performance under diverse operating conditions.

2. Fault Prediction and Protection

In a computing system, all information is represented by binary combinations of “0” and “1,” encoded as electronic signals. Systematic errors in such systems can be categorized into two types:

1. **Value Errors**: These occur when the binary value is incorrect due to transmission or transformation issues.
    - **Transmission Errors:** Errors caused during the transfer of data between devices, such as from external flash memory to internal RAM. For example, a binary combination "11101100" might change to "11101101" due to transmission equipment faults or external interference.
    - **Transformation Errors:** Errors arising during operations within a processor, such as incorrect results from an Arithmetic Logic Unit (ALU) due to faulty instructions.
      Value errors can affect both data and execution instructions, potentially leading to:
    - Deadlocks.

- Unauthorized memory access.
- Erroneous instruction execution.
  Detection and Prevention:
- Technologies like Cyclic Redundancy Check (CRC), Checksum, and Error Correction Code (ECC).
- Range and plausibility checks.
- Redundant data storage and calculations.

2. **Timing Errors**: These occur when binary signals do not appear at the required time.
   - **Internal Timing Errors:** Errors within the microcontroller, which are challenging to detect due to lack of a common time base.
   - **External Timing Errors:** Errors detected using input communication protocols with clock information.
     Detection and Monitoring:
   - Internal or external watchdog monitoring.
   - Window watchdog monitoring.

In summary, fault prediction and protection focus on identifying and addressing these errors to ensure system reliability and safety.

3. Data Driven Approach

A computing system or automotive ECU processes input signals to produce output signals via intermediate results (middle data). The relationships between these data can be expressed as:

Output Data = f(Input Data, Middle Data)

For example:

- Output Data 1 = f1(Input Data 11, …, Input Data 1i, Middle Data 11, …, Middle Data 1j)
- Output Data 2 = f2(Input Data 21, …, Input Data 2l, Middle Data 21, …, Middle Data 2p)

This approach focuses on two key data attributes:

1. **Value**: The quantity represented by the binary signal.
2. **Timing**: The expected occurrence time of the binary signal.

By concentrating on these attributes, the data-driven approach optimizes development activities, including:

- Designing middle data and their relationships to derive output data from input data.
- Allocating input/output data and middle results to software components and hardware devices.

- Establishing data flow, capacity, and control timing.

This systematic methodology forms the foundation of the system operation concept, which fully represents the required system using:

- Input data.
- Middle data.
- Output data.
- Relationships between these data.

Example Use Case: In an automotive braking system, input signals from sensors (e.g., wheel speed) are processed to generate middle results (e.g., deceleration rate), ultimately producing output signals to control brake actuators. This data-driven approach ensures efficiency and reliability in system design.

4. Data Driven Safety Analysis and FMEA

The Failure Mode and Effect Analysis (FMEA) identifies potential system errors (failure modes), their causes, and effects. In the data-driven approach, FMEA is guided by the system operation concept, which defines relationships between input, middle, and output data. For example:

Output Data 1 = f1(Input Data 11, …, Middle Data 11, …)

If the Output Data 1 is safety relevant, then the failure modes of Input Data 11, …, Middle Data 11 are safety relevant which have impact (effect) to the Output Data 1, anything else will not have any impact to the safety signal of Output Data 1 which has only two attributes: Value and Timing.

Improvements in Data-Driven FMEA:

1. **Defined Granularity**: Focuses analysis on critical data and their relationships, avoiding unnecessary complexity.
2. **Efficiency**: Reuses system design elements and aligns risk analysis with ISO 26262 classifications.
3. **Accuracy**: Recursive application ensures comprehensive coverage of failure modes and their propagation through the system.

Risk Analysis: Failure modes are rated based on severity, probability, and controllability, using ISO 26262 classifications:

- Severity (S): Impact of failure modes (e.g., S3 = total loss of functionality).
- Probability (E): Likelihood of occurrence (e.g., E4 = high probability).
- Controllability (C): Likelihood of control (e.g., C3 = difficult to control).

This structured approach ensures consistent and reliable safety analysis, enabling developers to identify and mitigate risks effectively.

5. Conclusion

This document presents a data-driven methodology for enhancing the failure Mode and Effect Analysis (FMEA) by focusing only data, this approach provides a comprehensive solution to modern safety engineering challenges.

Key benefits include:

- Standardized and efficient development processes by reusing the system operation concept.
- Accurate and complete FMEA analysis by focusing only data.
- Practical application of industry standards by clearly defining safety criteria.

As automotive technology advances, particularly in autonomous driving, adopting data-driven strategies will be essential for creating reliable and safe systems. By focusing on data attributes and their relationships, this methodology ensures robust safety engineering, paving the way for a safer and more reliable automotive future.