

Methods for Analyzing Severity Mitigation in FMEA

Samer Abbas and John Joyce
Ford Motor Company

ABSTRACT

Severity-mitigating mechanisms (typically software-based) detect failures in a system and perform functions in order to reduce the severities of failures. Various approaches to FMEA analysis of severity-mitigating mechanisms exist within the industry. Three are compared and contrasted. Each method is compared against its ability to capture the three fundamental failures of a system that has severity-mitigating mechanisms:

1. a failure occurs and mitigating action is taken,
2. a failure occurs and mitigating action is not taken,
3. no failure occurs but mitigating action is taken.

One method is advocated over the others because it: uses existing FMEA formatting; addresses all three cases; supports consistent linkage between FMEAs in a hierarchy of systems with any number of layers.

CITATION: Abbas, S. and Joyce, J., "Methods for Analyzing Severity Mitigation in FMEA," *SAE Int. J. Engines* 10(2):2017, doi:10.4271/2017-01-0325.

INTRODUCTION

Severity-mitigating mechanisms have been implemented for decades in automotive systems. Severity-mitigating mechanisms are typically software based, recognize failures in a system and change function to reduce the severity of the failure. Examples include:

1. Calculated wheel speed values are considered implausible and Antilock Control is disabled to mitigate the severity of failure modes caused by wheel speed sensor failures.
2. Differences between multiple measures of accelerator pedal travel are compared and arbitrated to mitigate the severity of failures modes caused by accelerator pedal sensor failures.
3. Measured yaw rate values differ from estimates based on other sensors and Electronic Stability Control is disabled to mitigate the severity of failure modes caused by yaw rate sensor failures.

The mechanisms typically span several layers of a hierarchy of system considering vehicle behavior and/or behavior of a major system (e.g. powertrain, brakes, steering), and/or behavior of a low-level component such as a sensor or actuator. Sometimes failures of logic devices are also considered.

There is ubiquitous use of FMEAs in the industry in the development of systems that have severity-mitigating mechanisms, but there are diverse approaches as to how severity-mitigating mechanisms are analyzed in FMEAs.

This diversity can present difficulties because different engineering activities may use different approaches. As the automotive mobility industry moves towards fully autonomous vehicles, severity-mitigating mechanisms play an increasingly significant role in the designs of fail-safe and fail-functional vehicles. The complexity and hierarchy of systems considered also increases. Alignment of approaches for analyzing severity-mitigating mechanisms in FMEAs is desirable.

To support improving industry alignment, this paper:

- Introduces three approaches to FMEA analysis of severity-mitigating mechanisms.
- Describes the details of supporting FMEA entries for each approach.
- Compares the approaches, identifying pros and cons of each.
- Recommends one approach over the others.

THREE APPROACHES

Overview

The three methods of analyzing severity-mitigating mechanisms are identified as:

1. Co-opting the "Detection" Column
2. Preserving the "Detection" Column
3. Adding "RED" and "Mitigated Severity" Columns

Co-Opting the “Detection” Column

- Used for many years successfully by brake controls suppliers on a wide range of applications
- “Detection” column is used to assess how effective a software function is in mitigating a failure during system operation.
- Typically used in a hierarchy of two layers of FMEAs (system and component)

Preserving the “Detection” Column

- Limited but successful use within Ford Chassis Engineering with some supplier partners.
- Preserves the use of “Detection” column to assess engineering activities during development - not system behavior during operation.
- Considers three distinct failure modes:
 1. Failure occurs and mitigating action is not taken
 2. Failure occurs and mitigating action is taken
 3. No failure occurs but mitigating action is taken

Adding “RED” and “Mitigated Severity” Columns

- Method proposed by suppliers as an outcome of joint AIAG/VDA FMEA discussions
- Introduces several new columns to FMEA format
- Key columns for risk assessment are: “RED” and “Mitigated Severity”

Method 1: Co-Opting the “Detection” Column

The Verband of the Automobilindustrie (VDA) FMEA method divides detection measures into two types:

“Detection measures which will be carried out in a development accompanying way, and reveal potential failure causes already during the development on a concept or a prototype respectively”[1]

“Detection possibilities, which inhere in the product(system) or will be recognized by the operator(customer). They point to the potential failures or the potential failure causes respectively, which have occurred during operation, so that further potential failure effects will be avoided.”[1]

The detection, or D, value “is a criterion for the probability, which allows to detect the malfunctions occurred in spite of all preventative measures already during the development”. [1] Paired with the above defined detection measures, the detection value can represent the likelihood of a failure being detected during pre-production or post-production (by the operator or diagnostic mechanisms in place).

Brake suppliers, drawing from the VDA FMEA method, have co-opted the detection column of the FMEA to capture the effectiveness of software-based severity-mitigating mechanisms. This approach involves two layers of FMEAs:

1. A component (lower) layer

2. A system (upper) layer

The component layer FMEA is a conventional FMEA of components that assesses the risks of component-level failures. The detection ratings at this layer, associated with each component-level failure cause, reflect the effectiveness of the detection controls to detect and prevent the failure prior to use.

The system layer FMEA assesses the system and vehicle level effects of the component failures. The failure modes at this layer are vehicle and/or system level failures caused by component failures, which are listed as failure causes. The detection rating at this layer is used to assess the software effectiveness in mitigating the component failure.

Table 1. Example of a Component-Layer FMEA Entry (partial)

Failure Mode	Failure Cause	Detection Measure	D
Incorrect wheel speed sensor output	Broken solder joints on signal wire-sensor interface	Continuity Check after Endurance Testing	1

Table 2. Example of a System-Layer FMEA Entry (partial)

Failure Mode	Failure Cause	Detection Measure	D
Unintentional traction control event	Incorrect wheel speed sensor output	Electrical monitoring of wheel speed sensor	2

Using this method, two cases of failures involving severity-mitigating mechanisms are analyzed:

1. Failure occurs and mitigating action is not taken
2. Failure occurs and mitigating action is taken

The risk of these two cases is assessed through the RPN number which would combine the Severity (quantifies the severity of the failure when mitigating action is taken) and the Detection which quantifies the risk that the mitigating action is not taken.

Method 2: Preserving the “Detection” Column

Another approach to assessing severity-mitigating mechanisms in FMEA works within the existing AIAG FMEA [2] framework to assess three cases represented as distinct failure modes:

1. Failure occurs and mitigating action is not taken
2. Failure occurs and mitigating action is taken
3. No failure occurs but mitigating action is taken

Since each case is assigned a failure mode, a severity, occurrence and detection quantifies the risk of each. Assuming a base failure with no mechanism in place, S-base representing the severity and O-base representing the occurrence, the influence on risk that severity-mitigating mechanisms have using this method can be illustrated relative to the base failure case.