

Assessing Severity of Failure Modes in FMEDA

Explanation:

Assessing the severity (safe/dangerous) of failure modes is integral to safety analysis methodologies such as Failure Modes and Effects Diagnostics Analysis (FMEDA) and is utilized to evaluate critical safety metrics like the system's safe failure fraction (SFF).

Failure mode here refers to how failure occurs. The safe state of the system is to be defined by safety experts and corresponds to a state where the user is safe.

But what exactly does it mean for a failure mode to be classified as safe or dangerous? To understand the practical impact of failure modes, consider the brake system of a car as an example.



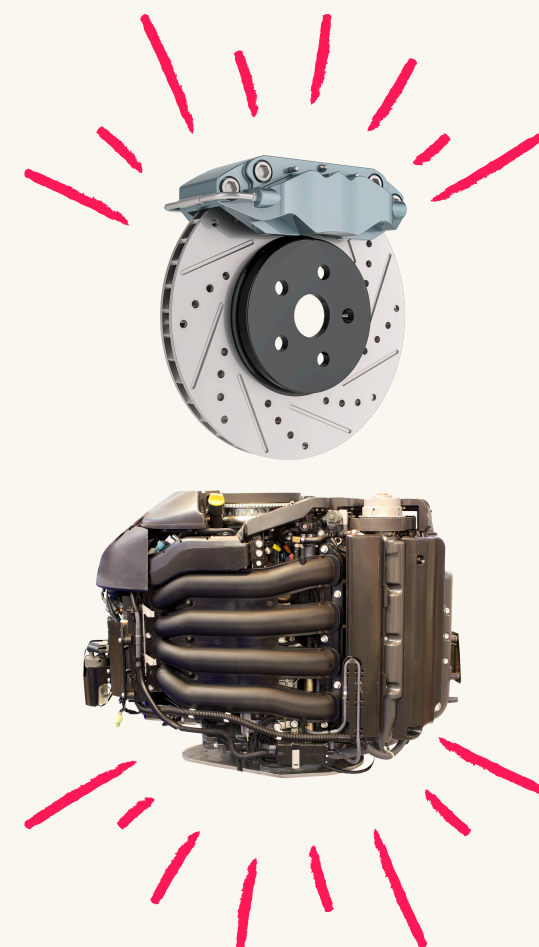
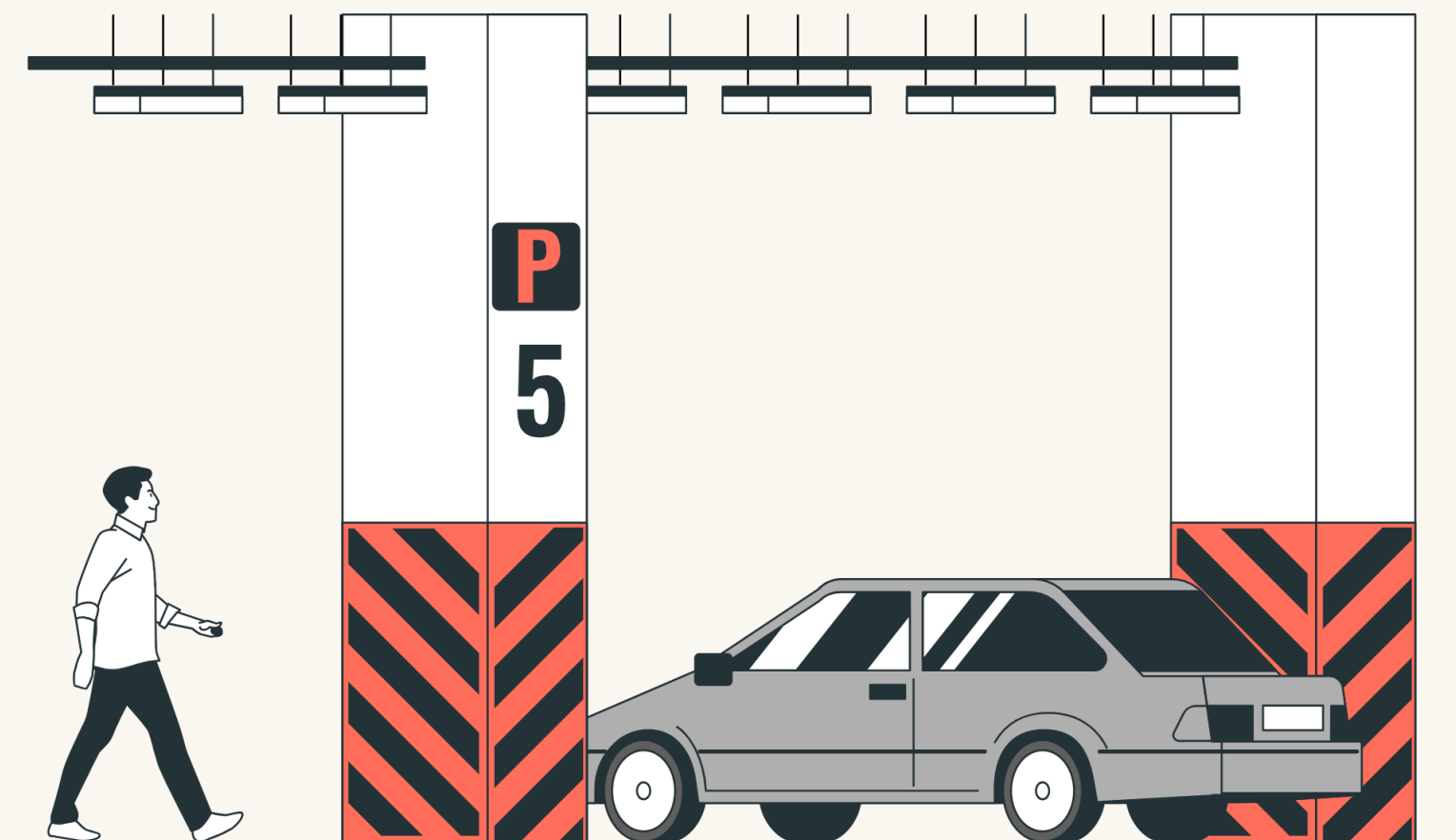
SWIPE

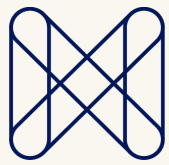




Illustrative Scenario #1: Safe Failure Mode (Car Parked):

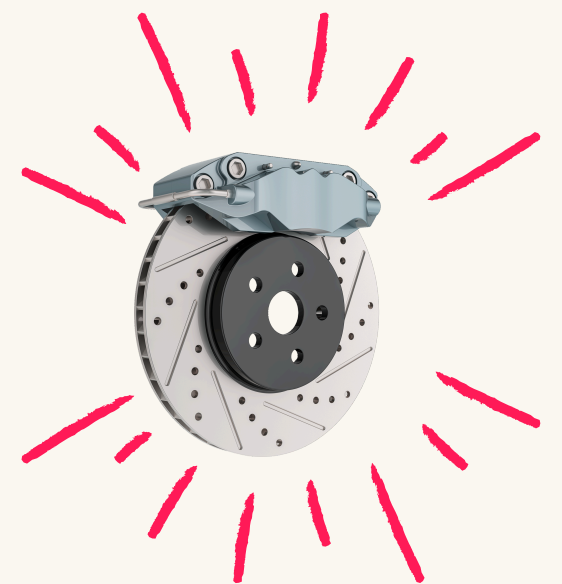
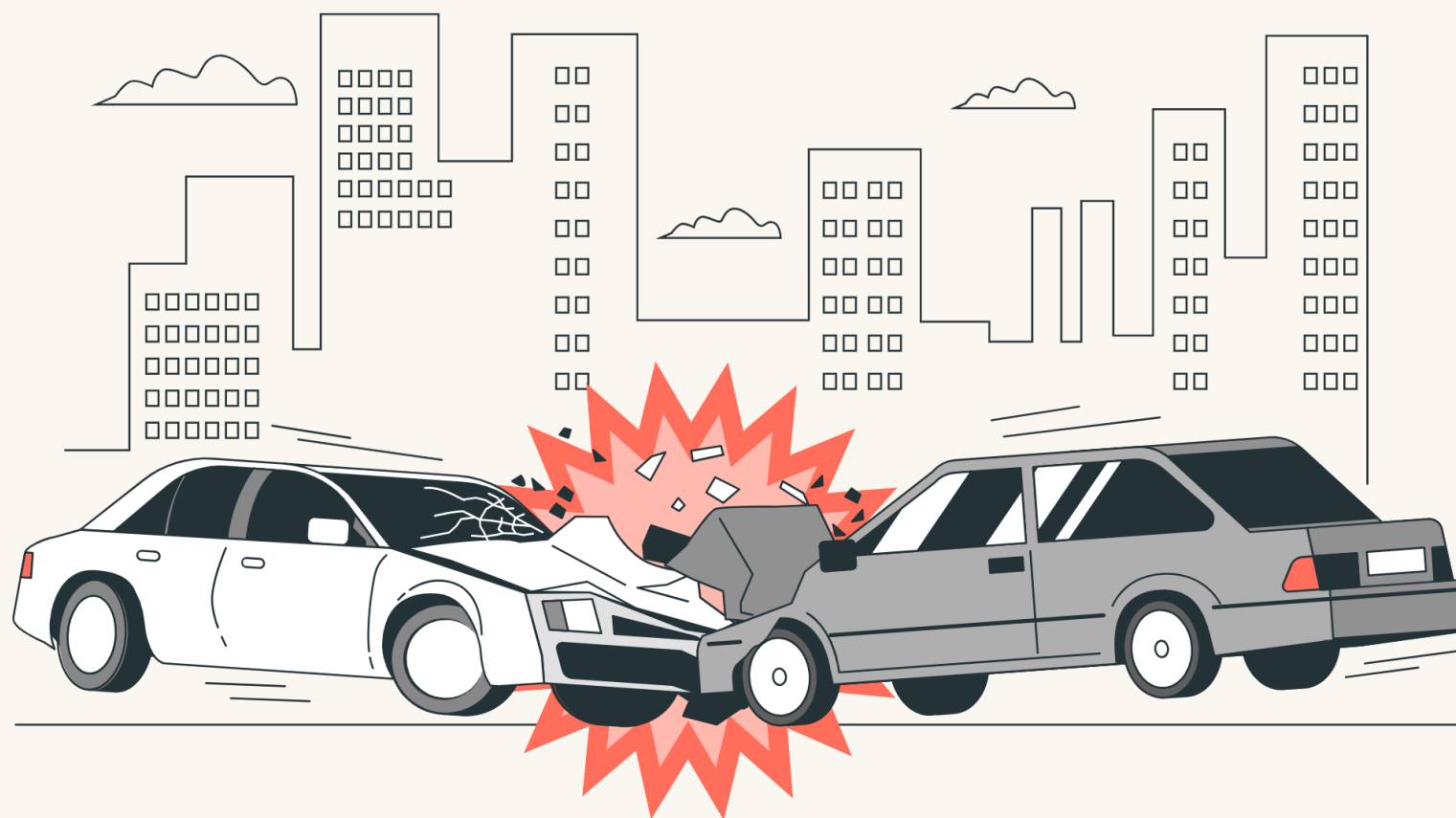
Picture a car parked in an underground parking lot, with the driver about to initiate ignition. However, a failure mode occurs, disabling both the brake and the engine, leaving the car stationary. As a result, the car is stuck in a state that we consider safe, despite the loss of braking. The failure mode can thus be classified as safe since the system stays in a safe state.





Illustrative Scenario #2: Dangerous Failure Mode (Car in Motion):

While a stationary car is safe (as in the previous scenario), a moving car must retain braking capability to be considered safe. Now, envision a failure mode that impairs only the car's brakes. In such a case, the driver could start driving without the ability to brake. In this situation, the system (car) exits its safe state and puts the driver in danger. Indeed, one can imagine, for instance, that this situation could lead to a collision of the car.





Understanding the severity of failure modes:

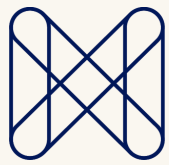
When assessing the severity of failure modes, it is essential to consider their impact within the context of operation. For instance, the failure mode that immobilizes a stationary car in the parked scenario may be deemed safe, as it prevents the vehicle from entering hazardous situations. However, the failure mode in the moving car scenario could pose a significant danger, highlighting the importance of contextual evaluation in assessing the severity of failure modes.

During FMEDA, functional safety engineers evaluate the severity of failure modes based on factors such as potential consequences and operational context. By considering these nuances, engineers can accurately assess the severity of failure modes and implement appropriate mitigation measures.



SWIPE





modelwise 
modelwise.ai

#Bi-Weekly Bytes:
Visual Chronicles

Assessing Severity of Failure Modes in FMEDA

Key takeaways:

- Failure mode severity is needed for safety metrics evaluation (like SFF)
- Dangerous failures are the failure that can put the system in a non-safe state
- The safe state of a system is to be defined by safety engineers

#BiWeeklyBytes by Modelwise. Follow to learn more about
FuSa!



Like this to
discover more
FuSa insights!



Comment below
with your topic
suggestions!



Send this to
someone who might
find it interesting!