Estimating Diagnostic Coverage in Functional Safety

Introduction:

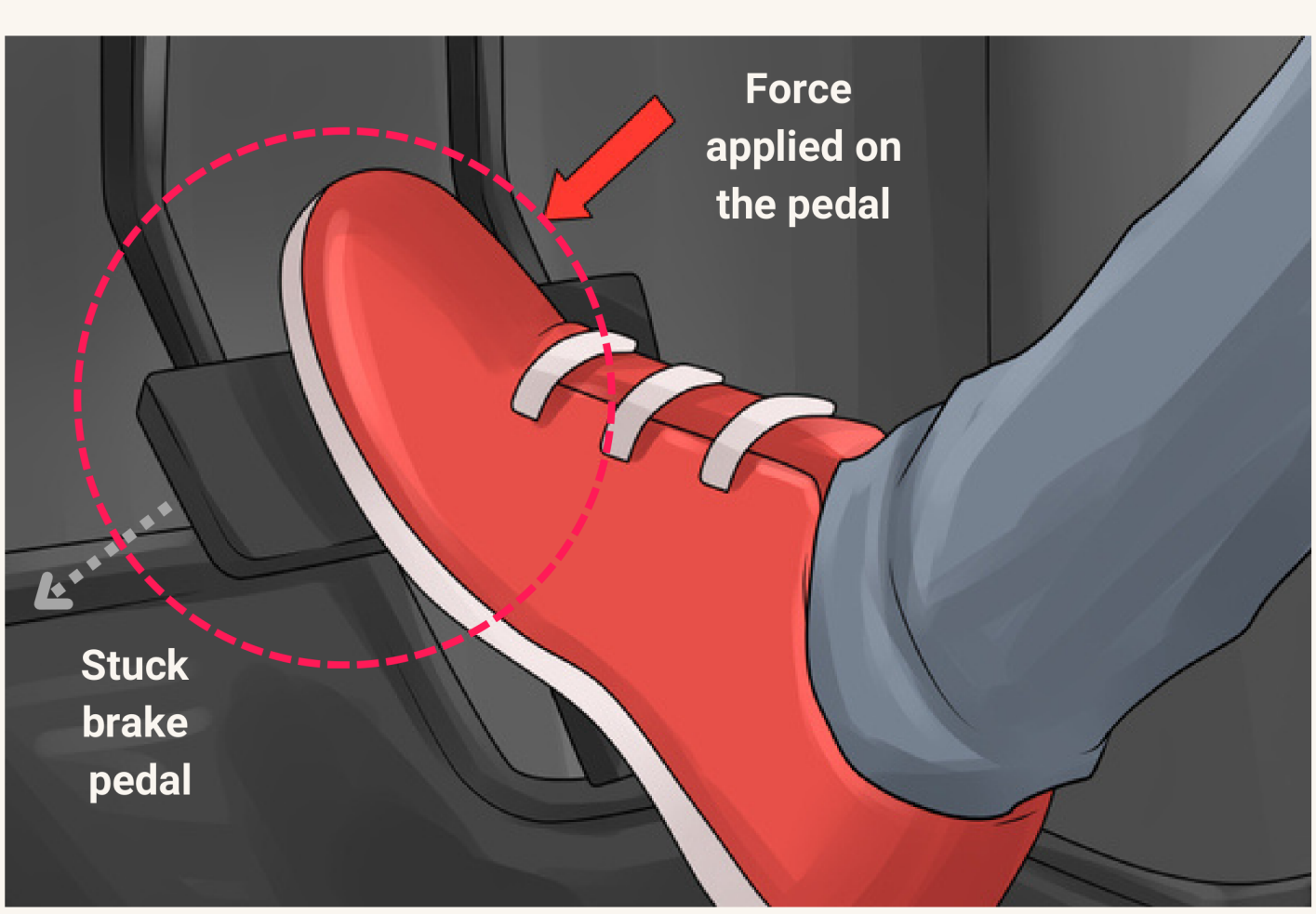
Diagnostic Coverage (DC) is a critical safety metric that is the fraction of dangerous detected failure of a system. In practice, it is challenging to predict all the possible manners a function can fail and to develop a diagnostic function that covers them all. As a result, estimating the fraction of failures that a diagnostic function might miss is difficult. So, how do we approach achieving an accurate estimation of diagnostic coverage?

For this reason, standards propose to approximate the coverage of a diagnostic function based on its detection principle and the frequency of the function's test. Let us illustrate this using a car's brake system.

SWIPE

Illustrative Example #1: Brake Pedal Stuck:

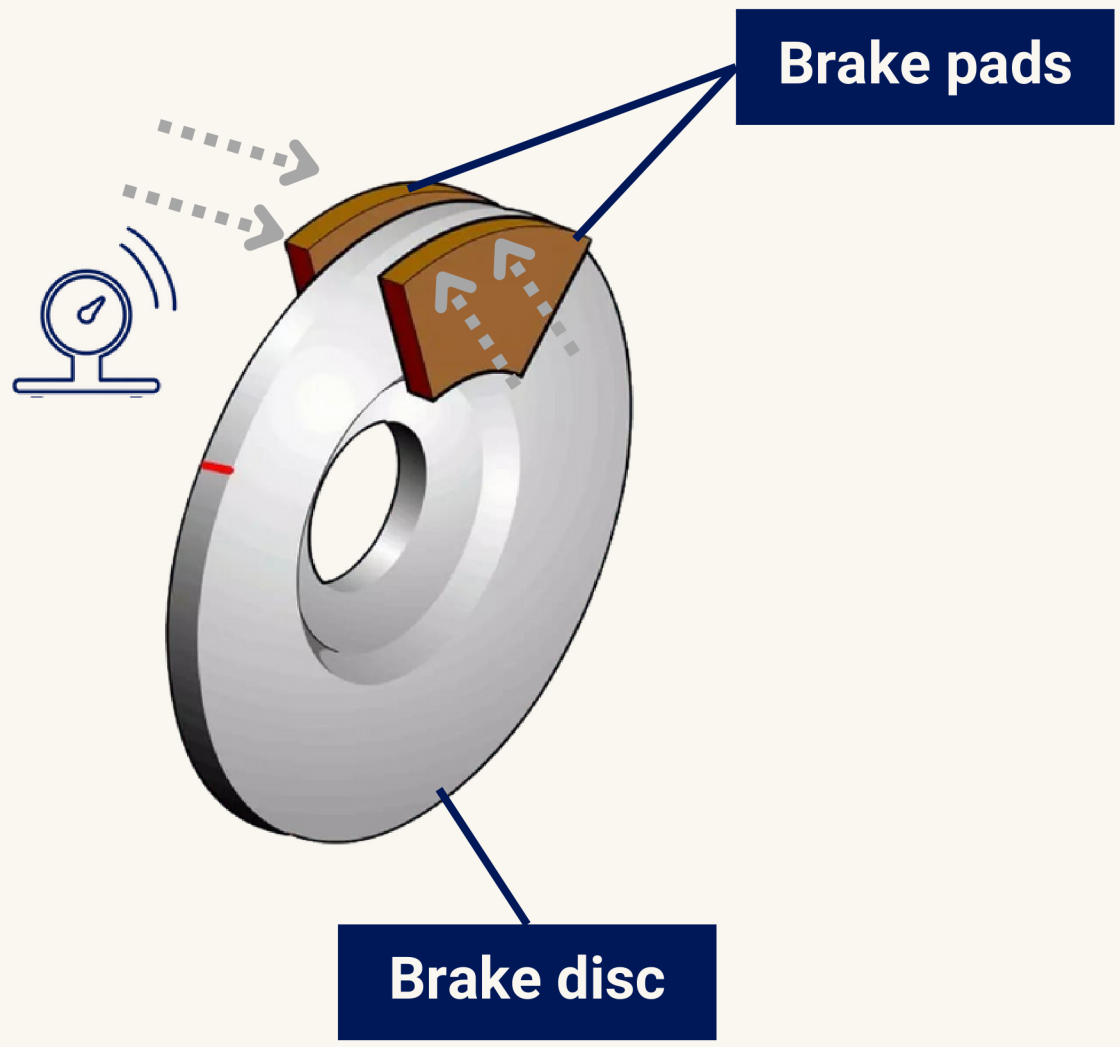
A rudimentary diagnostic method could rely on the brake pedal: if it is stuck, we know the brake cannot be used and is therefore failing in some way. This basic method, which, depends on the driver's physical feedback, tests the brake functionality every time the driver tries to push the brake pedal and therefore provides a low diagnostic coverage (let’s assume 60%).



Illustrative Example #2: Brake Pads - Motion Check:

A more precise diagnosis than checking the motion of the brake pedal (example 1) would be checking if the brake pads* are moving as intended using a dedicated diagnostic function whenever the brake pedal is pushed. This provides a medium diagnostic coverage (let’s say 90%).

Dedicated diagnostic function checking the motion of the brake pads

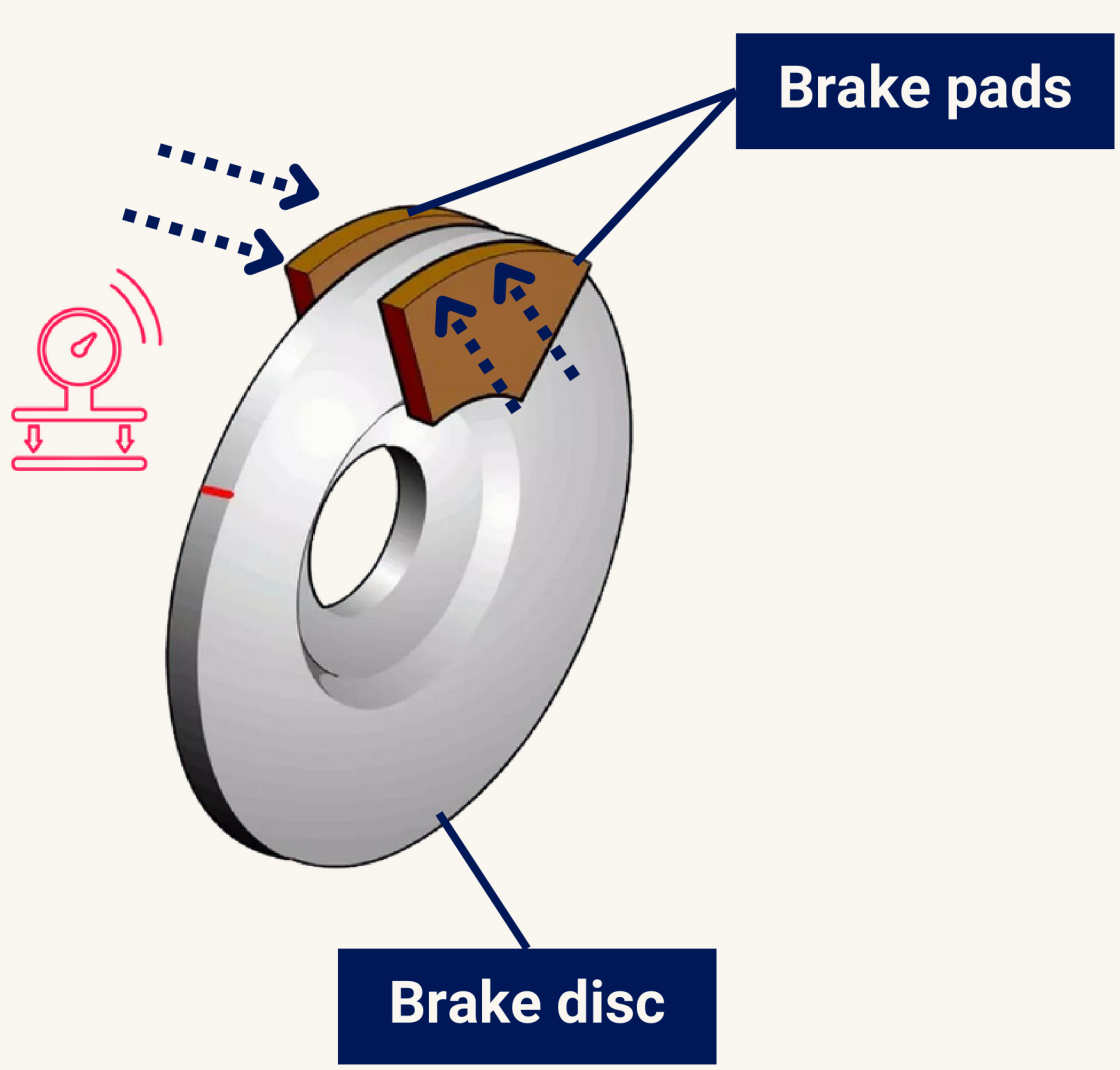


*In a car, braking is achived by clamping the disc/drum using braking pads

Illustrative Example #3: Brake Pads - Measuring Clamping Force:

An even more precise diagnosis than checking the motion of the brake pads (example 2) could be measuring the force applied by the pads on the brake disk using an advanced dedicated diagnostic function. This function can check if the brake system is applying the necessary force to stop the car effectively when trying to brake, providing a very high diagnostic coverage (let's say 99%).

Advanced dedicated diagnostic function measuring the clamping force of the brake pads



In-depth understanding:

Functionless Diagnostic
Although the sophistication of a diagnostic method improves its coverage, it’s possible to diagnose issues even without a dedicated diagnostic function.

For instance, we previously considered the brake pedal getting stuck (example 1) as a way to diagnose brake malfunction. The stuck pedal is a result of a brake malfunction, but it is not a designed function of the braking system; it's an unintended behavior.

Similarly, we can diagnose a failing light bulb when it doesn’t light up. Not lighting up is not a function of the light bulb; it indicates a failure.

SWIPE

modelwise
modelwise.ai

#Bi-Weekly Bytes:
Visual Chronicles

Estimating Diagnostic Coverage in Functional Safety

Key takeaways:

- Precisely determining the exact coverage of a diagnostic function is very challenging.
- Diagnostic coverage can be approximated using the principle of the diagnostic method and the frequency at which the function is tested.
- Having no diagnostic function doesn’t mean failures won't be detected (or perceived).

#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!