Diagnostic Coverage in Functional Safety

Explanation:

Diagnostic coverage (DC) is a safety metric that characterizes the effectiveness of detecting a dangerous failure. According to IEC 61508, diagnostic coverage is defined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures.

To understand the practicality of the concept, let’s delve into an example involving the brake system of a car.

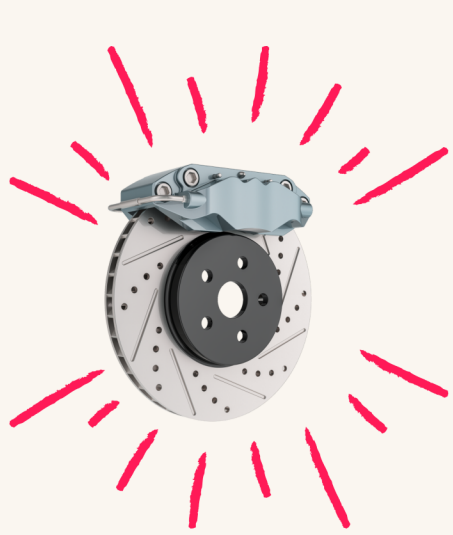
SWIPE

Illustrative Scenario #1: Undetected Brake Malfunction:

Imagine a car parked in a parking lot. Unbeknownst to the driver, a failure mode has disabled the brake system while leaving the engine functional. When the driver returns, starts the car, and begins driving, they are unaware of the brake malfunction. This creates a dangerous situation as the car is now in motion without the ability to stop, potentially leading to an accident.

Illustrative Scenario #2: Detected Brake Malfunction:

Now, let's consider a similar situation where the car is parked in a parking lot. A failure mode occurs that disables the brake system. However, this car has an inbuilt diagnostic system that detects the brake malfunction. As soon as the brake system fails, the diagnostic system identifies the issue and alerts the driver with a warning light on the dashboard. As a result, the driver is informed of the brake issue even before they start driving.



Brake Malfunction

In-depth understanding of diagnostic coverage:

The awareness of a potential safety malfunction does not render its cause (the component's failure) safe, but it can help the system or its user avoid an actual dangerous state. This can significantly reduce the risk of accidents or harm. In the scenario #2, while the failure mode that disabled the brake is still dangerous since the driver has the potential to drive without brakes, the detection of the malfunction and the driver's awareness prevent the car from entering a dangerous state, thus mitigating the actual risk of an accident.

It’s important to note that diagnostic functions, which achieve these failure detections, are not necessarily primary functions of a system. Therefore, their failure is not typically reported in Failure Modes and Effects Analysis (FMEA). By understanding and implementing effective diagnostic coverage, engineers can design systems that not only perform their intended functions but also maintain a high level of safety and reliability throughout their operational life.

SWIPE

modelwise
modelwise.ai

#Bi-Weekly Bytes:
Visual Chronicles

Diagnostic Coverage in Functional Safety

Key takeaways:

- Diagnostic Coverage: This safety metric measures the effectiveness of a system in detecting functional failures.
- Diagnostic Functions: These functions are responsible for identifying failures within the system.
- Risk Mitigation: While detecting a failure does not eliminate the possibility of accidents or harm, it significantly reduces the associated risks.

#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!