BLOG/BILLINGHAM, UNITED KINGDOM | MAY 2021

What do I claim is my Proof Test Coverage?

Blog by Rafal Selega

Rafal Selega, Senior Functional Safety Consultant, ABB

Many safety devices are designed with efficient internal diagnostic capabilities, with some smart transmitters having diagnostics that can detect over 90% of all device failures. Typically a good proof test procedure with three-point calibration can detect up to 97% of all transmitter failures.

But what happens when these two testing outcomes come together into the requirements of the Probability of Dangerous Failure on Demand (PFD_{avg}) calculation? Do we simply assume the same maximum test coverage as identified in the above example regarding the value of 90% for internal device diagnostic and 97% for Proof Test Coverage will always apply?

Diagnostics and Dangerous Failure Rates
As per the Failure Mode and Effect Analysis (FMEDA) report for a suitable Safety Integrity Level (SIL) capable transmitter, and as an example, let's consider a pressure transmitter which has an automatic diagnostic that can detect λ_{DD} = 313 FIT (Failures in Time) out of a total of declared dangerous failures λ_D = 347 FIT. The diagnostic coverage of such a test can therefore be calculated as: 313/347 which yields a 90% Diagnostic Coverage (DC) where DC = λ_{DD}/λ_D. So, on face value a high DC coverage claim for this device, but what is the effect of this test coverage on an operating SIS?

In the scenario where the automatic diagnostic feature is disabled in the SIS Logic Solver, then the example FMEDA information indicates that 338 FIT will be detected by an appropriate **proof test** and the test coverage therefore **becomes higher i.e. 338/347= 97%.** The numbers here essentially show that the proof test activity can detect an additional 25 FIT failures (338-313), compared to the number of failures that are detected by automatic diagnostics. This is because the proof test can detect some failures of the device which normally cannot be detected by the diagnostics. For example, "signal drift" failures are not normally detected by the automatic diagnostics associated with a single transmitter; but they can be detected by the proof test, using the "three point" calibration method.

By comparison, where the diagnostic feature is implemented in the SIS, then the proof test is able to detect 338 FIT, as already indicated above, but we must recognize that 313 FIT will have already been detected by the diagnostics. Therefore we cannot “detect” failures which are already detected, and the transmitter is very likely to be repaired by the time of the proof test schedule if the diagnostics have already detected a failure. So, we are really detecting 25 FIT out of the remaining 34 FIT (347 FIT Total minus 313 FIT with Automatic Diagnostics) which remained undetected after the automatic diagnostic process.

So, the proof test coverage on implementation of the diagnostic test would in reality be:
25 FIT / 34 FIT = **74% instead of the earlier 97% claim** (where the diagnostic feature is disabled within the SIS). In addition, the remaining 9 FIT (34-25) will stay undetected until the device is renewed.

Diagnostic Capability Considerations
We should be careful when assessing the Proof Test coverage for devices with automatic diagnostics. Keep in mind that the failures which are already detected by automatic diagnostics cannot be recounted as “detected” during the scheduled proof test. If we neglect this fact in the required PFD_{avg}/PFH calculations, then might lead to overly optimistic results which may well impact on our claimed risk reduction for the operating plant.

The effect of the wrongly assessed test coverage might even be bigger for the logic solver devices where automatic diagnostic coverage is usually above 99%. It is also likely that the proof test will not be able to detect any extra random hardware failures comparing to those already detected by automatic diagnostics. In such cases the proof test coverage might be around 0%.

So, for SIF Designers and Approvers, the above criterion for application of appropriate Test Coverage of the SIF devices must be considered when calculating the PFD_{avg}/PFH for the SIF.

For further information please email me at rafal.selega@pl.abb.com or see Functional safety lifecycle services