EXECUTIVE SUMMARY

Functional safety standards provide definitions of two different categories of failures: random failures and systematic failures. These were created during the standards committee discussions of failure types to be modeled in the probabilistic failure analysis. It was decided that random failures are counted in the probabilistic failure rate analysis and systematic failures are not counted.

Systematic failures were considered to be a direct result of some design or procedure problem. They occur when a set of circumstances happen to reveal the fault. The committee thinking was that systematic failures could be permanently “fixed” by a change in a design or a procedure. It was assumed that the fix would always be completely effective. After the fix, the failure would not happen again and therefore any such failures should not be counted.

Many companies establish programs to record and analyze failures. A failure rate analysis is performed to determine device failure rates. One problem observed while reviewing these studies is that many people have completely different interpretations of the definitions of random versus systematic failures. In some cases most failures are classified as systematic. This creates a dangerous bias in field failure rate analysis.

At some sites, those performing the analysis have realized that failures classified as systematic do prevent safety devices from performing their safety function and are therefore dangerous. These failures occur under conditions which seem to occur randomly and can be modeled with exactly the same probabilistic analysis. These failures impact the probability of dangerous failure and they certainly should be counted in any failure rate analysis.

This thinking is realistic as systematic failures may not be effectively corrected even when changes to the design or the procedures are made. If a systematic failure is effectively corrected then, in future data collection, the quantity of failure reports will decrease and will reflect the change. If the change was not effective the data will show that as well. Any updated field failure rate analysis will then reflect the improvement or not. So most engineers now understand that to improve safety and achieve realistic measurement of safety:

- All failures must be counted in failure rate analysis and
- All failures must be reviewed to determine if the failure can be practically prevented in the future.
INTRODUCTION

Functional safety standards provide definitions of two different categories of failures: random failures and systematic failures. These categories came into being during the standards committee discussions of failure types to be modeled in the probabilistic failure analysis that was being defined as a performance measure for safety instrumented functions during the late 1990s. There was a common consensus at the time that it was not practical to apply probabilistic analysis methods to systematic failures such as software faults. The committee decided that random failures would be counted in the probabilistic failure rate analysis and systematic failures would not be counted.

Systematic failures were considered to be a direct result of some design or procedure problem. They occur when a set of circumstances happen to reveal the fault. The committee thinking was that systematic failures are not random and could be permanently “fixed” by a change in a design or a procedure. After the fix, these failures would not happen again and therefore should not be counted. If design and procedure changes are not totally effective, the practice of not counting systematic failures creates an optimistic bias in the field failure analysis results.

Another factor that impacts field failure analysis results is that many people have completely different interpretations of the failure class definitions. Some people classify most failures as systematic. This creates another potentially dangerous bias in field failure rate analysis results.

However, after reviewing and studying actual failures in the plant over several years, many safety engineers have realized that failures classified as systematic do prevent safety devices from performing their safety function and are therefore dangerous. These failures do occur under certain conditions which seem to occur randomly. These failures can be modeled with exactly the same probabilistic analysis as other random failures. Furthermore, it was recognized that these failures impact the probability of dangerous failure. They certainly should be counted in any failure rate analysis [1].

This thinking is quite realistic as systematic failures may or may not be effectively corrected even when changes to the design or the procedures are made. If a systematic failure is effectively corrected then, in future data collection, the quantity of failure reports will decrease and reflect the change. If a systematic failure is not effectively corrected or it is judged that any change would be impractical, the quantity of failures will not decrease. Any updated field failure rate analysis will reflect the
impacts of actions taken or not taken. So most engineers understand that to improve safety and achieve realistic measurement of safety:

- All failures must be counted in failure rate analysis and
- All failures must be reviewed to determine if the failure can be prevented in the future by taking practical actions.

DEFINITIONS FROM THE FUNCTIONAL SAFETY STANDARDS

What are random failures? What are systematic failures? IEC 61508:2010, Part 4, 3.6.5[2] defines a random failure as “failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.” IEC 61508:2010, Part 4, 3.6.6[2] defines systematic failure as “failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.”

The definition of systematic failure was changed in IEC 61511:2016[3] which states “failure related to a pre-existing fault which consistently occurs under particular conditions, and which can only be eliminated by removing the fault by a modification of the design, manufacturing process, operating procedures, documentation or other relevant factors.”

These definitions give a good insight into the differences between the two failure categories but do not give enough detail to provide a good basis for each classification. Given that failures are categorized into two groups, every failure must go into one group or the other. The definitions should be mutually exclusive. As these definitions are not mutually exclusive, they have the potential to confuse those persons sorting and analyzing failure reports. Or perhaps the committee never intended failures to be in one category or the other. Are some failures both random and systematic? Are all failures both random and systematic?

EXAMPLES

Example 1

A failure occurred where a de-energize to trip remote actuated valve closed and shut down the process during normal operation. The failure was traced to the PLC logic solver (rated to 50 °C) where an output module failed de-energized. A component in the output module, a transistor, had failed such that it could no longer conduct current. The ambient temperature was hot, 55 °C. An X-ray of the transistor showed a burned out bond wire likely due to environmental electrical overstress.
A survey written by exida and issued by the International Society of Automation (ISA) had results for this example as shown in Figure 1. Approximately 23% of the survey respondents classified this failure as random and 77% classified this failure as systematic. The argument for classifying this failure as systematic was that the PLC device was being operated beyond the temperature rating even though this was not the stated cause of the failure. The argument for classifying the failure as random was that operation outside of the specified operating range was not the root cause of the failure. The failure was caused by electrical overstress. Even if the operating temperature had been 45 °C the failure would have occurred.

Although it may seem that there is a bias toward classifying failures as systematic, the systematic issue uncovered by the failure report should not be ignored. No product should be used outside of its specified operating limits. At this site, there appear to be problems with the engineering procedures used to check environmental ratings of the equipment against the expected environment. When the PLC was specified, either the engineer did not know the site temperature could reach 55 °C or the PLC rating was not checked. The procedures for checking device environmental specifications should be upgraded, or perhaps the procedure for characterizing the site environment needs to be improved. Until some effective action is taken, failures due to environmental overstress are expected.

So in this example, based on the actual root cause of the failure, the failure should be classified as random. At the same time, the occurrence of the failure alerts us to possible procedural issues that could be improved even though, in this case, the failure itself was not systematic.

Figure 1. Random or Systematic Survey Results for Failure Example 1.

Example 2

A maintenance technician routinely checks and adjusts the trip points on a motor shutdown relay. The procedures for checking and adjusting the relay were correct. All personnel are well
trained in the procedure. A failure occurred when a mistake was made with the adjustment. The trip point was set too high and the motor was not shutdown to maintain safety.

The ISA survey results are shown in Figure 2. Twelve percent of the respondents classified this failure as random. A larger group classified this failure as systematic and over 30% classified this as not a failure. The argument for random classification was that all procedures were correct and training was done. Therefore the human simply had a bad day and made a random error. The argument for systematic classification was that a human made the error and no hardware failed. The argument for not even counting this as a failure was that no hardware failed and procedures were correct. Therefore the failure did not fit either given definition and was not a failure.

![Figure 2. Random or Systematic Survey Results for Failure Example 2.](image)

In this example it was suggested that new procedures be established so that every adjustment made by one person would be “independently” checked by another person. This would cause a substantial increase in maintenance expense but could reduce failures of this type. The procedure change would have to be a site management judgement. Further, it may be decided that cost of the improvement was not justified. But in any case, the failure should be included in any probabilistic analysis.

### Example 3

During a proof test it was discovered that a float type level transmitter was stuck in position. However a light tap resulted in the transmitter giving a correct reading. The survey results are shown in Figure 3.
Figure 3. Random or Systematic Survey Results for Failure Example 3.

Almost 62% classified this failure as random. Almost 31% classified the failure as systematic and some said this was not a failure. The arguments for the systematic classification included “Float Level Transmitter did not have adequate reliability for this application” and “Incorrect design solution.” Arguments for the random classification cited no evidence of any systematic issue.

The root cause for this failure was not given and should be investigated. If the investigation shows ways to eliminate or reduce chances of this failure and if those improvements are effectively implemented, the future failure count will go down. Many sites however do not have the capability or time to do root cause analysis. Failures of this type may continue. In any case, the failure should be included from the failure count. It was a real failure that may have failed to initiate the safety function.

Example 4

During a proof test, a solenoid valve failed to vent an actuator as designed. When the solenoid coil was de-energized the solenoid did not release. The problem was first blamed on mechanical binding but it was noticed that a tap on the solenoid coil caused the solenoid valve to release and vent the actuator. The problem was traced to “residual magnetism” in the yoke of the coil. The survey results are shown in Figure 4.
Figure 4. Random or Systematic Survey Results for Failure Example 4.

These results are almost evenly split between the random and systematic classification. Arguments for systematic included “given the failure, it was obviously not adequate for the application” and “the design should have accounted for this.” This argument taken to its limit would classify every failure as systematic. Since there was no evidence of any systematic issue other persons classified the failure as random.

Residual magnetism susceptibility is a function of yoke material, yoke shape, duty cycle of applied power, ambient temperature and perhaps other variables [4]. A solenoid valve expert may be able to recommend a better choice for the device. In any case if it is practical to trace the problem further and take corrective action that should be done. The failure was real and should be counted in any field failure analysis.

Example 5

A calibration procedure for a pressure sensor was written with an error which caused the engineering units span parameter to be entered into the zero location. The sensor was badly out of calibration as a results of this error and failed to perform its function. Survey results are shown in Figure 5.
Figure 5. Random or Systematic Survey Results for Failure Example 5.

This example was written as a clear systematic failure yet there was some who classified this as random. Some classified this as “not a failure” indicating no further action should be taken. Most would argue that the bad procedure must be fixed.

In the survey there were 15 example failures, five of which are given above. One clear result from the survey is that few people agree on how to classify failures. Another conclusion seems to be that many are biased to classify failures as systematic or to otherwise exclude real dangerous failures by calling them “not a failure.”

SITE SPECIFIC FAILURE RATES

The quality of field failure reporting does vary from site to site. The ability and willingness to trace failures to root cause also varies from site to site. As shown in the examples above, these variables and others will impact device failure rates. A simple method can be used to measure the impact of the operational and maintenance process called the Site Safety Index (SSI) [5]. Failure rates are one of the measurements impacted by SSI [6].

CONCLUSIONS

It can clearly be concluded that:

- All failures must be counted when performing field failure analysis and
- All failures should be reviewed to see if the failure can be prevented by taking some practical action.

Failures might be prevented if:

- Device designs can be improved by the manufacturer.
• Device manufacturing processes can be improved.
• A device is replaced by another with higher strength.
• Operating procedures can be improved.
• Documentation can be corrected and improved.
• Other improvements such as better training can be done.

When these improvements can be implemented, the SSI will increase and actual failure rate will decrease.

REFERENCES


