Causes and Costs of No Fault Found Events

Louis Y. Ungar
Advanced Test Engineering (A.T.E.) Solutions, Inc.
El Segundo, CA

Abstract
No-Fault-Found (NFF) events occur when a system level test, such as built-in test (BIT), indicates a failure but no such failure is found during repair. With more electronics continuously monitored by BIT, it is more likely that an intermittent glitch will trigger a call for a maintenance action resulting in NFF. NFFs are often confused with *false alarm (FA)*, *cannot duplicate (CNDs)* or *retest OK (RTOK)* events. NFFs are caused by FAs, CNDs, RTOKs as well as a number of other complications. Attempting to repair NFFs waste precious resources, compromise confidence in the product, create customer dissatisfaction, and the repair quality remains a mystery. The problem is compounded by previous work showing that most failure indications calling for repair action are invalid. NFFs can be caused by real failures or may be a result of false alarms. Understanding the cause of the problem may help us distinguish between units under test (UUTs) that we can repair and those that we cannot. In calculating the true cost of repair we must account for wasted effort in attempting to repair unrepairable UUTs. This paper will shed some light on this trade-off. Finally, we will explore approaches for dealing with the NFF issue in a cost effective manner.

Introduction
System level tests come in various forms and are run for various reasons. In production, system test is run to gain confidence that the product is ready for the end user, often called ready for issue or RFI in military parlance. It is also used to ensure continued operation and is implemented in the form of built-in test (BIT). By implication, a system test can also be considered to be running when the end user is performing normal system operation. He/she may observe anomalies and inconsistencies leading to a call for a repair action. System level test, as we use it in this paper will encompass all of these forms. When a system level test fails, one or more subsystem unit under test (UUT) is suspected of being at the root of the system failure. The repair at system level consists of replacing the suspected UUT or UUTs and sending replaced UUTs to a depot level repair facility, which is often the factory.

Figure 1 shows the outcome of failures found at system level test as they distribute between Persistent Faults and No-Faults-Found. *Persistent faults (PFs),* sometimes called *confirmed faults* are those that caused the system level test to fail and will cause the UUT at depot to also fail. We call them persistent faults to indicate that system level faults persist into the depot. In contrast, NFFs will pass the UUT test at depot. There are two categories of NFFs. As discussed in [1] the majority of system test failures result from system level false alarms (FAs). NFFs resulting from intermittent failures (IFs) are covered in great detail in [2].

Figure 1 also illustrates failures that escape system level test. They create NFF at the system level. A common occurrence of this phenomenon is a computer hang up, which is "repaired" by rebooting the software. No maintenance action is taken and none of the subsystems are returned to the depot or factory, so the NFF does not penetrate to the depot. Unless the problem repeats many times it is treated as a normal anomaly and what would probably result in NFF at the depot is avoided.

To avoid confusion, it is important to understand the terminology we use in this paper. *No-fault-found (NFF)* is a situation where the UUT passes the first test at the depot test station. *Intermittent failures (IFs)* are real failures that are exposed only under certain conditions. When they are not exposed, they result in NFFs.

False alarms (FAs) are indication at the system level of a failure where no fault exists. [3] Alternatively, FA can be defined as a call for maintenance action when none was needed. [1] System level FAs may send some subassemblies to depot for repair, or if the result is questioned, the same system level test is run again to gain confidence in the result. When the system level test is run several times, it increases the likelihood of distinguishing FAs from IFs, making it more likely that the UUT returned to the depot is a result of IF.

The repeated tests can result in *cannot duplicates (CNDs)* or inconsistent results of two or more tests. In response to CNDs, either no repair action is taken, or some subassembly UUTs are sent to repair. When the UUTs are tested at the depot, they may pass the test, a condition called *retest OK (RTOK)*. A UUT that malfunctions in a specific manner during system level testing, but performs that same function satisfactorily at the next level maintenance facility, is called a *Retest OK (RTOK)*. [4] All RTOKs are NFFs, but not all NFFs are alike. Some are the result of FAs that cannot be repaired (because they are not really faulty), others may be the result of *intermittent failures (IFs)*, which are real and repairable. It is important that we know the difference.

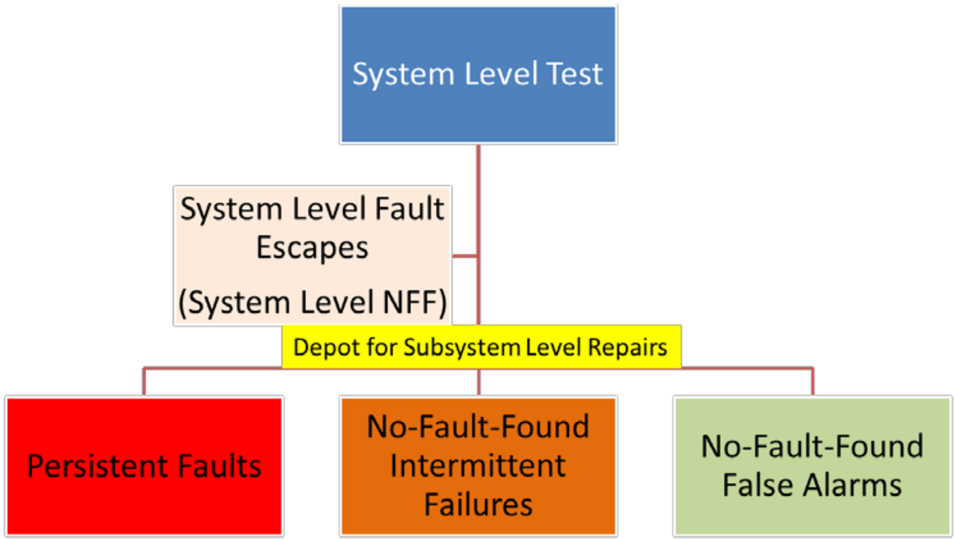


Figure 1 – Outcome of Failures Found at System Level

Another contribution to NFFs may be from *false rejects*. These are instances where tolerances, accuracies, calibration and other uncertainties within the system level tester caused the test to fail. In essence, perfectly good systems were judged to be faulty and consequently UUTs were sent to the depot. These UUTs are not faulty, will likely pass the depot test as NFF. Since no fault exists, these are also FAs. False rejects, however, can also be created by system level interaction failures that do not have an analogous cause within a single UUT. For example, due to some environmentally induced condition a system failure is detected, causing one or more UUT to be sent to the depot for repair. The failure may have required specific interaction of UUTs or it may have required a specific environment, neither of which can be created in the depot test. The result is NFF, but it is possible that different UUTs in the system would not have failed the same environmental condition. This implies that the UUT is flawed and in a strict sense repairable. In this case it would fall into the IF category rather than FA.

We need methods to distinguish between IFs and FAs. Repair of UUTs that are not faulty (i.e. FAs) is futile and the only logical corrective action is to return such UUTs to the system level. UUTs from false rejects, however, may not be clearly IFs of FAs and returning them to system level may pose damage and perhaps safety issues.

In this paper we will closely examine the causes of NFFs in order to draw such distinctions when possible. We will try to predict how many NFFs are IFs and how many are FAs. We will evaluate the cost of repairing NFFs, recognizing that many, indeed most NFFs are unrepairable and our time and resources are being wasted when we attempt to do so. Finally, we will consider various corrective strategies to deal with NFFs at the depot and calculate their economic performances.

What Causes NFFs?

UUTs at a depot repair facility experiencing NFF are caused by one or more of the following:

- Cannot duplicate (CNDs) that include both real failures and false alarms
- Retest OK (RTOKs)
- Measurement Uncertainty and Test Equipment Problems
- System level failures that are not detectable at the subsystem UUT level

- Intermittent Failures

Let us explore each of these causes deeper to find out whether the resulting UUT experiencing NFF is repairable at the depot (IF) or not (FA).

Cannot Duplicates (CND)

A CND can occur only when a test or a condition is repeatedly executed. Even a single disagreement of results is considered a CND. The following failures can cause CND events. [5]

1. ***Operator Error***
2. ***Latent BIT Design Error***
3. *Environmentally Induced BIT Error*
4. *BIT Transient Failure*
5. BIT Hard Failure
6. ***Latent Design Error Manifestation***
7. Transient (Functional) Failure
8. *Environmentally Induced Functional Error*
9. **Flight Line Test Equipment Error**
10. **Flight Line Human Error**
11. **Test Equipment Failure**
12. **Human Error at Shop Level**

Situations 1, 2 and 6 (***in bold italics***) are FAs and are not repairable at the depot. Situation 1 - operator error - may actually be the greatest contributor to FAs. A complex system requiring constant interaction with a human operator can conceivably find that operator pushing the wrong buttons or at the wrong time creating responses the operator does not expect. The operator can misinterpret such unexpected responses and (mistakenly) call for a repair action. Situation 6 – latent design error manifestation – may be a subtle design flaw that only exhibits itself in certain situations, often intermittently. This, however, is not an intermittent fault because there really is no faulty circuit element. The product does what it was designed to do – though not necessarily what you would want it to do.

Another manifestation of this CND situation can be caused by a *sneak circuit*, an unexpected path or logic flow within a system which can sometimes initiate an undesired function or inhibit a desired function. It can be caused by software, hardware, end user or a combination of these elements but because it is the way the circuit was designed, it is not a fault that can be repaired. Sneak circuits are design errors – situations that are difficult to uncover. The more functions performed by the system, the more likely that a sneak circuit will sneak up and create a FA. Here is an illustrative example. Suppose we have an electronic circuit whose job it is to tell the time when the user provides the position of the small and large hands on a classic analog clock. So when the user enters “small hand on 5, large hand on 9,” the circuit states “the time is 5:45. But due to a design error, when the user enters “small hand on 12, large hand on 12,” the circuit responds “the time is 12:00 noon.” This will be correct whenever the circuit is used during the day, but incorrect if it is used at midnight! It is important to recognize, however, that the uncovered error cannot be corrected by sending the circuit to the repair depot, and it is therefore a FA.

Environmentally and transient induced failures 3, 4 and 8 (*in italics*) may be caused by circuit failure behavior, but is usually temporary and no UUT repair is warranted. NFFs caused by these conditions are clearly FAs.

Test equipment and support personnel errors 9, 10, 11 and 12 (**in bold**) also send non-repairable UUTs to depot and should be considered FAs.

CND failures in BIT and in circuit function – Situations 5 and 7 - are most likely repairable.

Retest OK Produced False Alarms

Typically, RTOK is a result of a fail of BIT at the system level and subsequent passing of ATE at the depot level. Since RTOK compares the results of two distinctly different tests, RTOK NFFs result from different sources. The following RTOK events produce NFFs:

- *Misdiagnoses or False Diagnosis (FD***)** is a situation where the test incorrectly identified the replaceable unit containing the fault. [6] Such events are FAs.
- A more common source of RTOK NFF is *diagnostic ambiguity (DA)*. This is a situation that arises when the test is able to detect a fault, but the smallest fault group to which that fault can be isolated contains more than one repair item. In this case, in addition to faulty UUTs some good units will also be delivered to the next level of assembly and when these good UUTs pass the depot ATE test, they will be rendered NFFs. If all the UUTs removed from the

same system experience NFF, we cannot determine which one is due to an intermittent failure, so we will consider all the UUTs from the same system as having intermittent failures.

Measurement Uncertainties and Test Equipment Problems

Measurement uncertainties and test equipment problems can also create test results that are misleading. NFF could be caused by instruments on the tester rendering a good system as faulty, a concept referred to as *false reject (FR).* An FR may be due to incorrect selection or calibration of tolerances and test accuracy ratios [7], or it may be due to other test equipment problems. The FR would produce a NFF at depot, which would be a FA.

Similarly, the test equipment at the depot could experience a *false accept (FX)* condition. Similar to the FR, an FX is created by incorrect selection or calibration of tolerances and test accuracy ratios or it may be due to other test equipment problems. FX is NFF that contains a failure, but one that the depot tester cannot confirm. Returning the UUT to the system would continue to show it as faulty, but it does not fit either the FA or IF category exactly.

System level failures that are not detectable at the subsystem UUT level

Environmental conditions can play havoc with the UUT circuit, with the tester and with interpretation of BIT or other monitoring techniques. A good example of this occurs when avionics fail at high altitudes, but those failures cannot be repeated at the depot. In these cases it is not clear whether the UUT is experiencing IF or FA in the system, but since no such determination can be made at the depot, the UUT must be treated as FA. Attempts are sometimes made to simulate the environment by environmentally stressing the UUT, but there is no assurance that such actions result in replicating the failure.

Another common example of such faults is when a cable is temporarily or permanently disconnected within the system. The failure is not related to a single UUT and all UUTs returned to the depot as a result of this condition will be FAs.

Classifying Depot Level Repair Causes

Figure 1 identifies three categories of UUTs arriving at the depot, namely Persistent Faults, NNF IFs and NFF FAs. Table 1 shows the causes that would place a UUT in one of the categories. It also classifies UUTs as “Indeterminate” when it is not clear which category the UUT fits best.

In order to differentiate between IFs and FAs, we will explore each in detail.

Table 1- Classification of NFF Sources

Persistent Faults	No-Fault-Found (NFF) Intermittent Failures (IF)	No-Fault-Found (NFF) False Alarms (FA)	Indeterminate
Assembly faults within each UUT – Shorts, opens, missing components, wrong component, wrong component insertion	CND BIT Hard Failure	CND Operator Error	False accept conditions that occur when the depot tester inaccuracy renders a UUT as faulty. The UUT may in fact be faulty or not.
Parts faults – bad component, out of spec component	CND Transient (Functional) Failure	CND Latent BIT Design Error	System level failures not detectable at subsystem UUT level. Usually FA, but could be IF.
Functional failures from hard faults	RTOK Diagnostic ambiguity (DA) of all UUTs from same system if all UUTs are NFF	CND Latent Design Error Manifestation	Environmentally induced failures at operating conditions that are not available at the depot. E.g. failures at high altitudes only.
	Connectors – corrosion and wiring failures	CND Environmentally Induced BIT Error	Some system level cable becomes disconnected temporarily, perhaps due to corrosion.
	Components – IC crosstalk, electromigration, dielectric breakdown, metallization, ionic contamination, tin whiskers, wire bond lifts, creep corrosion, etc.	CND BIT Transient Failure	
	Printed circuit board – electro-chemical migration, via cracking, warpage and whiskers.	CND Environmentally Induced Functional Error	
	Component-PCB Interactions – solder problems, loads, manufacturing defects, socket problems	CND Flight Line Test Equipment Error	
		CND Flight Line Human Error	
		CND Test Equipment Failure	
		CND Human Error at Shop Level	
		RTOK Misdiagnoses or False Diagnosis (FD)	
		RTOK Diagnostic ambiguity (DA) of 2nd, 3rd, etc. UUTs sent to depot if 1st UUT is not NFF	
		False Reject -Measurement tolerances and uncertainties causing a good system to fails system test.	

Intermittent Failures

Figure 2 is a wishbone diagram showing the cause and effect of intermittent failures in electronic assemblies. [2] It details many of the factors that could create NFF IFs.

There have been a number of reports dealing with the occurrence of NFFs caused by IFs. For example, Sorensen [8] suggests that only 50% of all failures fall into the persistent failure category and IFs that cause NFFs is the other 50%. Since not all NFFs are caused by IFs, it is not clear from this analysis, where FAs are considered. Other studies are equally ambiguous, often using the terms “IF” and “NFF” interchangeably.

Perhaps a better understanding of FAs will yield some distinguishing characteristics from IFs.

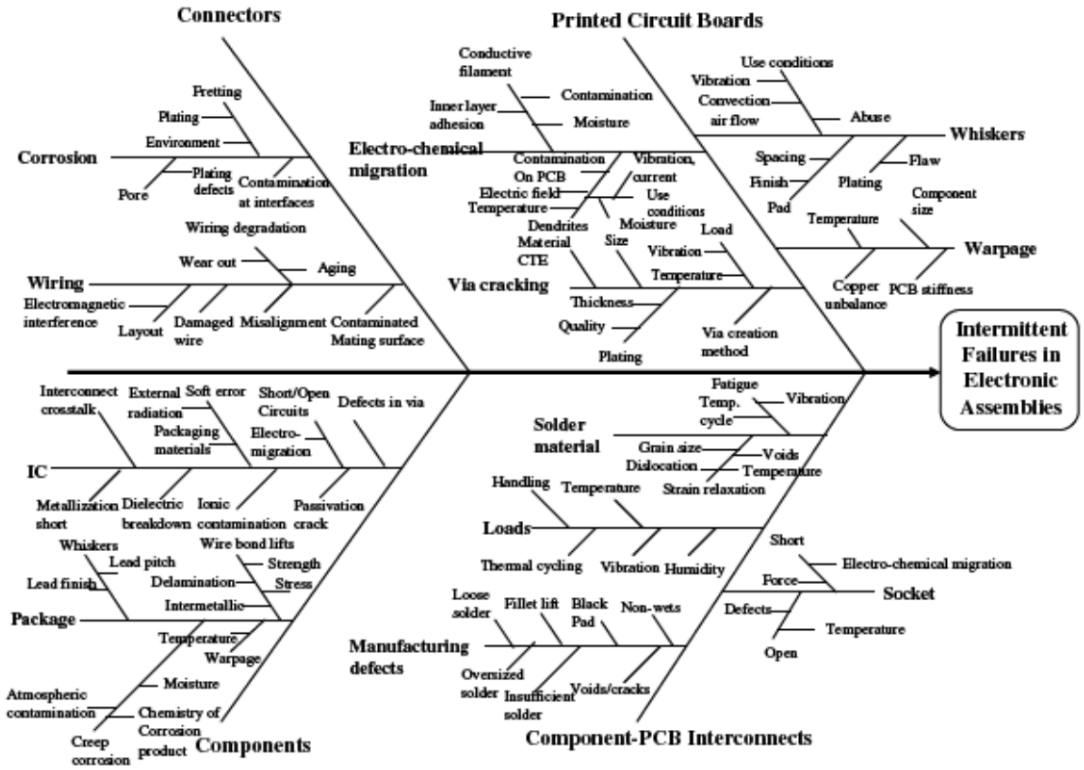


Figure 2 – Cause-and-effect diagram of intermittent failures in electronic assemblies [2]

False Alarms

FAs are caused by statistical occurrences of false positives. [1] Four possible outcomes to a test are considered, as shown in Table 2. A graphical representation of the Gaussian distribution is shown in Figure 3.

False positive (FP) or *Type I error* is an indication of a failure when in fact none exists.

Table 2- Possible Test Outcomes [1]

Test Outcome	***Label***	***Typical % of cases***
True Negative – Good UUT passes all tests.	TN	95%
True Positive – Faulty UUT fails one or more tests.	TP	95%
False Negative – A faulty UUT results in UUT passing the test. Also called "missed fault" or Type II error.	FN	5%
False Positive – A good UUT indicates that the test failed. Also called "false alarm" or Type I error.	***FP***	***5%***

While *false negative (FN)*, or *Type II errors* happen to be equal to FP in the Table 2 example and in the Figure 3 illustration, this relationship is not necessary. A coupling relationship between FP and FN, however, does exist. If one were to increase the fault coverage, TP, then in Figure 3 the origin of the T+ and T- axis would shift to the right, reducing the area under FN. This makes sense, since increasing fault coverage should indeed lower the number of missed faults. Because of the coupling between FP and FN, however, reducing the area under FN will also increase FP. The implication that a more comprehensive test creates more FPs appears ironic at first, but considering that tighter measurements result in higher number of anomalies confirms this notion.

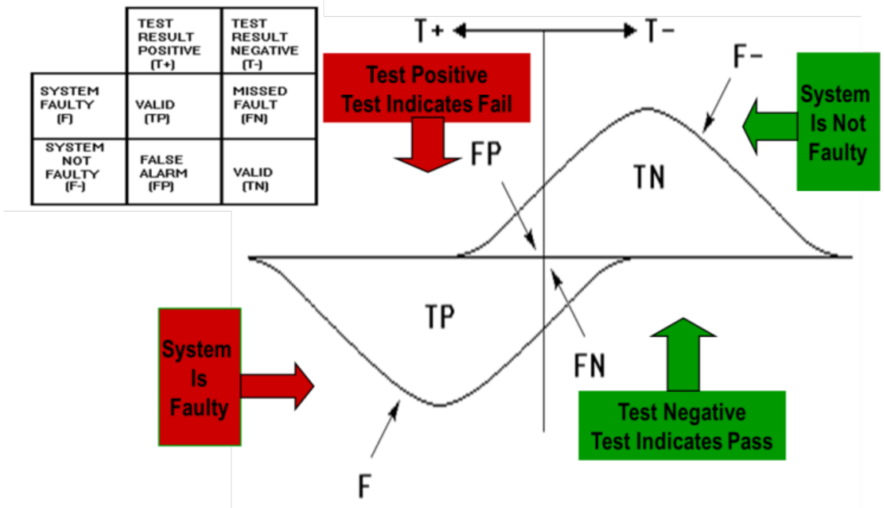


Figure 3 - Graphical representation of possible test outcomes [1]

While FPs may constitute only a small percentage of possible test outcomes (5% in Table 2), they can be responsible for a high percentage of the failing results being invalid. In [1] it was shown that even with 5% FPs, the invalid failing result (i.e. false alarms or FAs) can be as high as 77%. This implies that a system sent back to repair is actually fault free in 77% of the cases, and they will all result in NFFs.

Using Bayes formula in [1] the following impact of FA was revealed. We can calculate the probability of a valid faulty result, *P(F/TP)* as

$$P(F/TP) = P(TP/F)\,P(F) / [P(TP/F)\,P(F) + P(TP/F-)\,P(F-)] \qquad (1)$$

Where *P(F)* is the probability that the system is in fact faulty.
P(F-) is the probability that the system is not faulty. Clearly, *P(F-) = 1 – P(F).*
P(TP/F) is the probability that a “System Faulty” result is due to the existence of a fault.
P(TP/F-) is the probability that a system which is not faulty is still called out as faulty.
Also, it follows that if *P(F/TP)* is the probability of the ***valid faulty result***, then *P(F-/TP)* is the probability of the ***invalid faulty result***, which is another way of saying ***false alarm***. This can be quantified as

$$\text{Probability of False Alarm} = P(F-/TP) = 1 - P(F/TP) \qquad (1a)$$

As an example in [9], the following assumptions were used to calculate FA:

- The 95% fault detection will result in having 95% of the faulty system fail the test. P(TP/F) = 0.95
- 10% of the systems diagnosed as faulty are in fact good. FFA = P(TP/F-) = 0.10.
- Only 3% of the items tested are faulty. P(F) = 0.03. Thus the probability that a system is not faulty, P(F-) = 0.97.

Then the probability of a truly faulty system resulting from a test failing, P(F/TP) is

$$P(F/TP) = (0.95)(0.03)/[0.95)(0.03) + (0.1)(0.97)] = 0.23 \qquad (2)$$

The probability of ***invalid faulty result*** (FA) is

$$P(F-/TP) = 1 - P(F/TP) = 1 - 0.23 = \boldsymbol{77\%} \qquad (3)$$

This implies that in 77% of the case that a system test fails, the UUTs sent to the depot are FAs. The number of UUTs with FAs is actually greater because of diagnostic ambiguity and in some cases more than one UUT is sent to repair. Reducing the fraction of false alarms (FFA) in the above example to 2% (a typical specification, but hard to achieve goal for many systems), the probability of a valid faulty result in equation (2) would increase to about 0.60 and FA in equation (3) would decrease to ***40%***.

All NFFs

We would like to know the quantitative distribution of the categories of faults depicted in Figure 1 and Table 1. We estimate from equation (3) and from the discussion above that FA can range from about 40% to 77%. For the purpose of this paper we will approximate FA to be generated by ***60%*** of the systems that fail system tests.

Empirical data supports such high FA results. For example, for the military aircrafts F/A-18 A/B/C/D 75% of the CNDs resulted from false alarms. In some cases the units returned due to false alarms exceeded 83%. O-Level and I-Level wasted maintenance labor resulting from BIT false alarms during 1999 resulted in Unnecessary Aircraft Downtime of 2.96 years. [10] Other sources echo similar results [11], and one reported 100% false alarm for a particular system [12].

Using the diagnostic resolution of 90% isolation to a single module, 95% to 2 or less modules and 100% to 3 or less modules, of a 100 system failures, we have:

All modules removed = 100 + 2*(100-95) + 3∗(100–10) = 140 UUTs/100 system failures (4)

Assuming 60% of system failures were FAs and 100% of all ambiguous replacements were also FAs,

FA modules removed = (60% of 100) + 100% (2*5) + 100% (3∗10) = 100 FA UUTs/100 system failures (5)

Percentage of FA UUTs in the depot = 100/140 = ***71.4% of UUTs*** (5a)

Valid faulty modules = 140 -100 = 40 UUTs have persistent faults or IFs (6)

Percentage of non-FA UUTs in the depot = 40/140 = ***28.6% of UUTs*** (6a)

From the above, we have sufficient information to predict the probable of distribution of UUT arriving at the depot repair as shown in Table 3. It implies that while 28.6% of the UUTs are faulty (not FA) only half of those, [8] or 14.8% of the UUTs will fail the first time depot repair.

Table 3- Distribution of UUTs arriving at Depot Repair

Fault Type	**Derivation**	**Probable UUT Distribution**
No-Fault-Found False Alarms (NFF FAs)	Equations (1) thru (5a)	71.4%
Not False Alarm Faults (Not FAs)	Equations (6a)	28.6%
Persistent Faults	50% of non-FAs per [8]	14.3%
No Fault Found Intermittent Faults (NFF IFs)	50% of non-FAs per [8]	14.3%

Kinseng et al. [13] studied intermittent failure in cruise control modules used in automobiles. Empirical data showed that 96% of the modulus returned to the manufacturer due to customer complaints operated properly and passed the bench test. The study concluded that the depot test was "inappropriate" because it did not test the UUTs in an actual automotive environment. It is possible that the conclusions may have misinterpreted what the data suggests. When we include FAs the 71.4% from equation (5a) is not far from the 96% result. Considering that cruise control modules can be easily misused or misinterpreted by the driver (operator error), FA rates would likely be higher and if we also consider IFs, the NFF of 96% may well represent the actual NFF rate. FA already takes into account the "inappropriateness" of the test environment and is a real and expected cause of the NFF rate.

A survey of mobile phone 'No Fault Found' phenomenon in 2005 [14] concluded that 63% of devices returned had no faults. They were categorized as "struggling with functionality/usability" in 24% of the cases, as "device mis-sold / does not meet expectations" in 8% of the cases and as "handset configuration / setting issue" in the remaining 31% of the FA cases. A similar conclusion was found by [15]. These compare well with our prediction of 71.4%. Of the faults found, in 24% of the cases the fault was from hardware and in 12% of the cases a software fault was found. This is also close to our estimate of 14.8% persistent hardware faults.

We should also consider an inherent bias technicians may have when documenting the NFFs at the depot. When a technician decides to shot gun (repair based on a guess) a UUT that experienced NFF in the initial depot test, he/she is more likely to record this situation as a "repair" than a NFF. Since a correct repair and a NFF will both pass the test, the technician having expended time and parts for the repair will unlikely decide that the repair was unnecessary. Documenting this action as a correct repair will skew the NFF rate.

Cost Impact of NFFs

The same survey of mobile phones in the UK [14] determined that 63% of mobile phones returned to the factory in 2005 were NFFs. The "operators, manufacturers and retailers collectively covering administration, shipping and refurbishment costs" approached £35 per device. They projected that the cost to the UK mobile industry was £54,016,200 and more significantly a global industry cost of $4.5 Billion." Since 2005 when the study was conducted, the number of mobile phones has increased considerably without much mitigation in NFF rates and it is possible that the cost of NFFs in the mobile phone industry alone now tops $10 billion.

Other sources [16] put the cost of US Department of Defense NFF costs at $2 billion and US Air Transport Association estimates at $2.2 billion per year. What is also troubling is that according to this report most organizations don't know how much NFF costs them.

Similar NFF costs could plague all electronics markets, including computers, automobile electronics, control systems, communication systems, etc. The cost impact of NFFs can be monumental. They can result in increased utilization of equipment, parts, transportation and maintenance personnel often to no avail, create customer inconvenience and dissatisfaction, damage company reputation and in some cases create potential safety hazards. Inherently, NFF implies that either the product should not have been sent to maintenance or that maintenance does not have the resources to repair it. Both of these mandate a better handling of NFFs.

We can start our cost analysis by identifying major cost components of support at the system level: [7]

$$C_S = C_E + C_D + C_R + C_I \tag{7}$$

Where C_S = Cost of Support
C_E = Cost of Escapes
C_D = Cost of Detection
C_R = Cost of Repair (by module replacement)
C_I = Cost of Idle (Down) Time

If we assume that we repair the system by module replacement and that all the replacement modules are fault free, NFF in the depot repair impacts only the cost of repair, C_R. The replaced module (assumed to be faulty) is returned to the depot for repair because we believe that we can repair it for less than the cost of a new module. Our goal is to repair at a lower cost than procuring a brand new UUT, or

$$C_R = \min(C_N, C_r) \tag{8}$$

Where C_R = Cost of Repair (by module replacement)
C_N = Cost of a new module replacement
C_r = Cost of repairing the faulty module in the depot

The problem is that C_r is not known until some test and repair costs have been expended and even then we cannot be certain that the repaired unit will work in the system. In short, the assumption that $C_r < C_N$ cannot be taken for granted. The situation is even more complex when the retest at the repair facility results in NFF. Since many of the NFFs are FAs that can never be repaired, any attempt at repairing them would be futile. Returning them to the system without any repair is also risky and involves costs of administration, handling and transportation that will return no benefit for the cost. Moreover, reintroducing the NFF module into the system may in fact fail the system, creating a repeat of the entire pointless activity.

Since not all UUT repair cost is the same, let us divide the cost of repair into incremental parts as follows:

Let C_{dt} = Cost of testing the UUT in the repair depot to confirm faulty or not
(includes transportation, administrative and handling costs)
C_{t2} = Cost of retesting a UUT that experienced NFF with a change in test or environment
C_{r2} = Cost of repairing a UUT that failed with a change in test or environment
C_{rsg} = Cost of "shot gun" repair of a UUT based on assumptions
C_{st} = Cost of retesting the UUT at the System Level test
(includes transportation, administrative and handling costs)

Then the repair cost of persistent faults, C_{rPF}, is

$$C_{rPF} = C_{dt} + C_{r2} + C_{st} \quad (9)$$

The cost of repairing UUTs with NFF that is returned to the System Level without any repair, C_{rFA1}, is

$$C_{rNFF0} = C_{dt} + C_{st} \quad (10)$$

The cost of successfully repairing UUTs with NFFs by changing the test and/or its environment, C_{rNFF1}, is

$$C_{rNFF1} = C_{dt} + C_{t2} + C_{r2} + C_{dt} + C_{st} = 2*C_{dt} + C_{r2} + C_{t2} + C_{st} \quad (11)$$

The cost of successfully repairing UUTs with NFFs by shot gun assumptions, C_{rNFF2}, is

$$C_{rNFF2} = C_{dt} + C_{rsg} + C_{dt} + C_{st} = 2*C_{dt} + C_{rsg} + C_{st} \quad (12)$$

Cost of Various Strategies for Dealing with Depot Level NFFs

NFFs will comprise of FAs and IFs. The probability distribution will be as follows:

- Probability of NFF FA = 71.4%(71.4%+14.8%) = 71.4%/86.2% =82.8%
- Probability of NFF IF = 1 NFF FA = 17.2%

A good test strategy for dealing with depot level NFFs would be one that locates and identifies the root cause of intermittent failures in the approximately 17% of the NFFs and returns the nearly 83% FAs without incurring a great deal of cost. For a UUT's first time appearance in the depot and experiencing NFF we will have three different strategies:

1. Treat all NFFs as FAs and return all of them to the System Level.
2. Treat all NFFs as IFs and run a second, environmentally stressed test to attempt exposing faults
3. Rely on the technician to use an educated guess to find NFFs.

1. Treat all NFFs as FAs and return all of them to the System Level

This will be the correct assumption for 82.8% of NFF UUTs which are FAs, but the incorrect one for 17.2% of them that are IFs. Of the FAs, simply returning the UUT to system level will result in a correct repair. Retesting FAs at system level should again yield 71.4% FAs, so (100%-71.4%) of the FA UUTs will not be returned to the depot a second time and can be considered "repaired." Since this applies to the FA population only that comprises of 82.8% of the NFFs, the percentage of

UUTs repaired by this approach is (100%-71.4%)*82.8% = 23.7%. (13)

The benefit of Strategy 1, B_{r1}, will be the avoidance of replacing 23.7% of UUTs with new ones at a cost of C_N. The costs incurred include the test at depot and at the retest at system level for the first trip to the depot, ($C_{dt} + C_{st}$), plus the depot level test for the second trip for 23.7% less UUTs.

$$B_{r1} = (23.7\%)* C_N - [(C_{dt} + C_{st}) + (100\%-23.7\%)*C_{dt}] \quad (14)$$

For this strategy to be beneficial, we need to satisfy the inequality

$$(23.7\%)* C_N > [(C_{dt} + C_{st}) + (76.3\%)*C_{dt}] \quad \text{or}$$

$$C_N > 7.44* C_{dt} + 4.22*C_{st} \quad (15)$$

Equation (15) provides a decision criterion for determining if Strategy 1 is economically advantageous to deal with NFFs or not.

2. Treat all NFFs as IFs and run a second, environmentally stressed test on all UUTs to expose faults

Let q be the effectiveness of the environmentally stressed test expressed in percentage. That means that q% of the IF faults will be detected (and repaired) using this strategy. This benefit, however, will not apply to FAs. The cost of testing all NFF UUTs will include the initial depot test and the system level test of all NFF UUTs, plus the cost of repairing those IF faulty UUTs that are detected.

$$B_{r2} = 17.2\%* q*C_N - [C_{dt} + C_{t2} + 17.2\%*q*C_{r2} + C_{st})] \quad (16)$$

For this strategy to be beneficial, we need to satisfy the inequality

$$17.2\%* q*C_N > [C_{dt} + C_{t2} + 17.2\%*q*C_{r2} + C_{st})] \quad \text{or}$$

$$C_N > C_{r2} + 5.81/q* (C_{dt} + C_{t2} + C_{st}) \quad (17)$$

The coefficient of the second term in equation (17) will be governed by q. If the stressed test is very effective, say q=100%, equation (17) will be $C_N > C_{r2} + 5.81 * (C_{dt} + C_{t2} + C_{st})$, but if q=10%, equation (17) will only be effective for a very expensive UUT with $C_N > C_{r2} + 58.1 * (C_{dt} + C_{t2} + C_{st})$.

3. *Rely on the technician to use an educated guess to find NFFs*

As often happens, the technician facing NFFs is required to make a judgment call. In this strategy, we will allow her/him to pick the UUTs that should be repaired through a "shot gun" approach. We will assume that the repair technician will make the correct guess in 2/3 or 67% of the cases. (To justify this assumption, consider that an experienced technician is much smarter than coin flips of 50% probability but at the same time the dominance of FAs that cannot be fixed over IFs puts the odds against a correct shot gun repair.) Also, since the technician knows that only 17.2% of UUTs are repairable, that number will serve as a maximum number of UUTs that should undergo repair.

This approach should allow repair of 67% of the 17.2% IFs, while incurring costs of repair on 17.2% of the UUTs. All UUTs will be tested at both the depot and system test

$$B_{r3} = 67\%*17.2\%* C_N - [C_{dt} + 17.2\%*C_{rsg} + C_{st})] \qquad (18)$$

For this strategy to be beneficial, we need to satisfy the inequality

$$67\%*17.2\%* C_N > [C_{dt} + 17.2\%* C_{rsg} + C_{st})] \qquad \text{or}$$

$$C_N > 1.56 * C_{rsg} + (C_{dt} + C_{st}) \qquad (19)$$

The main factor in this strategy is the reliance on the experience and accurate assessment of the technician.

Examples for selecting the best strategy

In equations (14) through (19) the economics of repair is primarily determined by the relative cost of a replacement UUT, C_N, and the costs of test at depot and retest at the system test, namely $(C_{dt} + C_{st})$. Consider a few examples:

a) A computer consists of circuit boards, where C_N is typically around \$200. ATE test costs, C_{dt}, would probably not exceed \$20 and system level test, C_{st}, would also be about \$20. Cost of a stressed test, C_{t2}, will cost \$30. The stress test is 90% effective, q, and the cost of repairing circuit boards failing the stress test, C_{r2}, will be \$10. The cost of shot gun repair, C_{rsg}, will be \$20.

Strategy 1: \$200 >? 7.44* \$20+ 4.22*\$20 = \$148.80+\$84.40 = \$233 ***Not Advised***

Strategy 2: \$200 >? \$30 + (5.81/0.9)*(\$20+\$30+\$20) = \$30 + \$451.89 = \$481.89 ***Not Advised***

Strategy 3: \$200 >? 1.56*\$20 + (\$20+\$20) = \$71.20 ***Good Strategy***

Only Strategy 1 is beneficial.

b) An avionics box, where C_N is typically around \$3,000. ATE test costs, C_{dt}, is \$100 and system level test, C_{st}, is run with BIT and takes up operating time so it would cost about \$75. Cost of a stressed test, C_{t2}, will cost \$300. The test is 70% effective, q, and the cost of repairing circuit boards, C_{r2}, will be \$750. Assume that the cost of shot gun repair, C_{rsg}, will be \$200.

Strategy 1: \$3,000 >? 7.44* \$100+ 4.22*\$75 = \$744.00+\$316.5 = \$1,060.50 ***Good Strategy***

Strategy 2: \$3,000 >? \$750 + (5.81/0.7)*(\$100+\$300+\$75) = \$750 + \$451.89 = \$3,942.50 ***Not Advised***

Strategy 3: \$3,000 >? 1.56*\$200 + (\$100+\$75) = \$312 + \$175 = \$487 ***Good Strategy***

While both Strategy 1 and Strategy 3 are beneficial, Strategy 3 is better.

c) A scanner that dispenses radiation used in medicine consists of a number of circuit cards with a high replacement cost C_N, of \$10,000 per circuit board. Because of low volume depot level test cost, C_{dt}, is \$1,000 and system level test, C_{st}, is run with BIT and takes up operating time so it would cost about \$250. Cost of a stressed test, C_{t2}, will cost \$1,500. The test is 80% effective, q, and the cost of repairing circuit boards, C_{r2}, will be \$750. Assume that the cost of shot gun repair, C_{rsg}, will be \$500.

Strategy 1: $10,000 >? 7.44* $1,000+ 4.22*$250 = $7,440.00+$1,055 = $8,495 ***Good Strategy***

Strategy 2: $10,000 >? $750 + (5.81/0.8)*($1,000+$1,500+$250) = $19,972 ***Not Advised***

Strategy 3: $10,000 >? 1.56*$500 + ($1,000+$250) = $780 + $1,250 = $2,030 ***Good Strategy***

While both Strategy 1 and Strategy 3 are beneficial. Strategy 1 requires that circuit boards experiencing NFF get returned to the system, i.e. to the doctor's office or to the hospital. Considering that this is medical electronics, there is a potential safety issue and it may not be acceptable to adopt a strategy of simply returning UUTs that experience NFF to the organizational environment.

Summary and Conclusions

We have concentrated on the causes and costs of no-fault-found events and determined that they are both complex. NFFs occur mostly because of false alarms that send UUTs from the system level to depot level - where no corrective action is possible. Considering all UUTs returned to the depot, no more than about 30% to 40% exhibit permanent faults that can be repaired - the rest are NFFs. With more than 80% of NFFs being FAs, even in an ideal test scenario, IFs are difficult to detect, diagnose and repair. Since they constitute less than 20% of the NFFs and even lower percentage of all faulty UUTs, we asked whether it was even cost effective to treat IFs and FAs differently. We considered three strategies a) returning all NFFs to the field as if they were all FAs, b) try to repair all NFFs as if they were all IFs, and c) allow a smart technician, aware of the maximum number of IFs, to pick out and shot gun repair those he/she considers to be IFs. In each of these cases we related the breakeven cost to test and repair costs that each strategy would incur. We used three different electronic products with variations in UUT price and test costs as examples. In our examples, utilizing a technician, Strategy 3, was beneficial in all three cases. Treating all NFFs as FAs – Strategy 1 where all NFF UUTs are returned to the system level – was beneficial in two of the three cases. Since one of those cases involved medical electronics, we questioned the safety aspect of returning NFF UUTs to the field. Strategy 2, treating all NFFs as IFs and running additional stressing tests on all of them, did not yield benefit in any of the three products we considered.

Our analysis indicates that the overwhelming cause of NFF comes from FAs. Since repairing FAs is not possible, attempting to repair them is futile. Efforts made to identify IFs are more promising. Using a stressed test at the depot, however, does not appear as effective as relying on the analysis of an experienced technician. Perhaps this approach is beneficial because the technician is able to locate IFs. An automated test approach to locate and diagnose IFs would be preferred, but it doesn't appear that simply running stress tests accomplishes this. Characterizing IFs so that our confidence in finding them will be more effective and efforts along that line will mitigate NFF costs.

Further work on this subject should extend the model to include 2nd and subsequent returns of UUTs to the depot. At this point we can conclude that the real cost driver of maintenance is the large number of FA UUTs that simply waste resources. Eliminating FAs before they send UUTs to the depot would be an important step. The most important improvement is the reduction of diagnostic ambiguity. The test should isolate to a single UUT in ever higher percentage of cases. Typically in today's avionics, fault isolation to a single replaceable unit is in 90% of the cases. That should be increased beyond 95% of the cases.

It is difficult to achieve all these goals without purposely designing testable systems. Design for Testability (DFT) techniques have been documented [3], [17], [18], [19] and available through commercial tools [20] and courses [21]. Utilizing DFT for NFF mitigation should be studied in future endeavors.

References

[1] Ungar L Y. The True Nature of False Alarms, AUTOTEST '14, IEEE Press; 2014.

[2] Qi H, Ganesan S, Pecht M. No-fault-found and intermittent failures in electronic products, Microelectronics Reliability 48, Elsevier Ltd. 2008, p. 663-674.

[3] US Navy, MIL-HDBK-2165, Testability Handbook for Systems and Equipment, 31 July 1995, superseding MIL-STD-2165A, 01 February 1993. United States Department of Defense.

[4] Ungar L Y. Kirkland L V, Unraveling the Cannot Duplicate and Retest OK Problems by Utilizing Physics in Testing and Diagnoses, Proc. AutoTestCon, 2008.

[5] Simpson, WR. et. al, Prediction and Analysis of Testability Attributes: Organizational-Level Testability Prediction, RADC-TR-85-268, Rome Air Development Center, Griffis AFB, NY, 1986.

[6] Test Definitions, by A.T.E. Solutions, Inc. [online], Available from www.BestTest.com/BestTestDirectory/TestDefinitions/

[7] Dobbert M., Understanding Measurement Risk, First presented at the 2007 NCSL International Workshop and Symposium, http://cp.literature.agilent.com/litweb/pdf/5991-1265EN.pdf, 2012.

[8] Sorensen B. Digital averaging – the smoking gun behind 'No-Fault-Found,' Air Safety Week, Feb. 24, 2003.

[9] J. G. Malcolm, Practical Application of Bayes' Formulas, Proc. Annual Reliability and Maintainability Symposium, 1983.

[10] Office of the Assistant Secretary of the Navy, "Built-In Test, Design and Optimization Guidelines," TB # ABM 1001-01, October 2001.

[11] Bain K and Orwig D, Presentation: "F/A-18E/F BUILT IN TEST (BIT) MATURATION PROCESS", Presentation given October 10, 2000

[12] Hecht D of Boeing Aircraft Company, Diagnostic - Lessons Learned, Chart Presented at AutoTestCon 2007.

[13] Kimseng K, Holt M, Precht M. Physics-of-failure assessment of a cruise control module, Microelectronics Reliability 39, 1999, p. 1423-1444.

[14] Overton, D of WDS, Survey of Mobile Phones No Fault Found, http://www.wds.co/no-fault-found-returns-cost-the-mobile-industry-4-5-billion-per-year/, 2005.

[15] Adams C, Getting Serious About No Fault Found, Aviation Maintenance Magazine, pp 26-32, Feb / Mar 2014.

[16] Copernicus Technology Blog, Can you afford the cost of No Fault Found? http://blog.copernicustechnology.com/can-you-afford-the-cost-of-no-fault-found/, May 2014

[17] Surface Mount Technology Association / Testability Management Action Group, SMTA/TMAG Testability Guidelines TP-101E, http://www.smta.org/store/book_detail.cfm?book_id=437, 2014.

[18] IPC, IPC 1-14 DFX Standards Subcommittee IPC 1-14, DFX Standards Subcommittee, IPC-2231: Design for Excellence (DFX) Guideline During the Product Lifecycle, expected release Feb 2015.

[19] Ungar L Y. Economic Evaluation of Testability and Diagnosability for Commercial off the Shelf Equipment, AutoTestCon 2010.

[20] The Testability Director version 3.3, http://www.besttest.com/OurProducts/TestabilityDirector/, 2014.

[21] A.T.E. Solutions, Inc., Design for Testability and for Built-In Self Test tutorial course notes, last updated 2014.

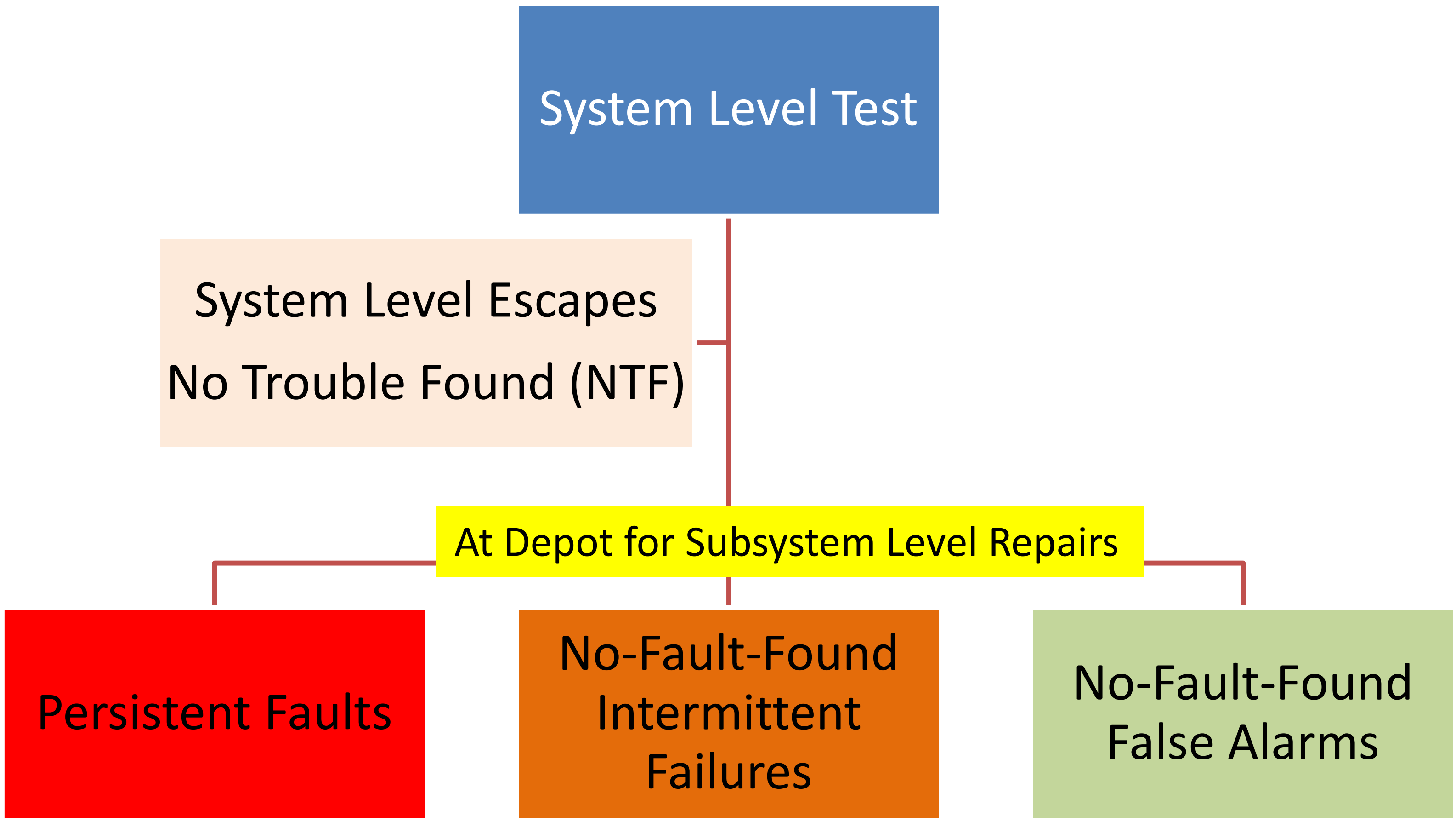
Causes and Costs of No-Fault-Found Events

Louis Y. Ungar

Advanced Test Engineering (A.T.E.) Solutions, Inc.

LouisUngar@ieee.org

Outcomes of System Level Failures



No-Fault-Founds (NFF) Explored

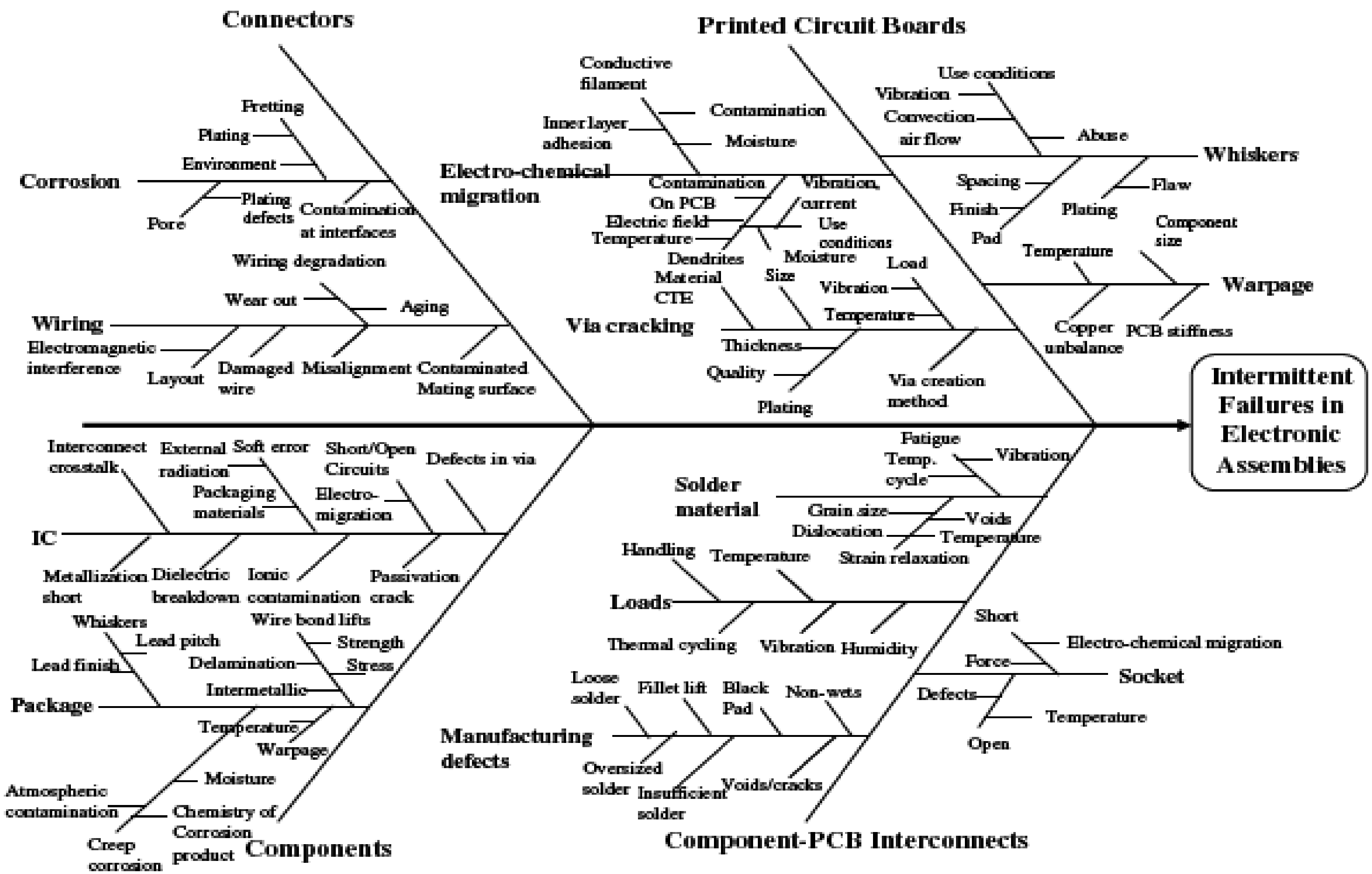
- System Level Test Results
  - System Level False Alarm (FA) = Depot Level NFF
- Causes of NFFs
- Quantifying NFFs
- Cost Impact of NFFs
- Strategies to Deal with Depot Level NFFs

Causes of NFFs

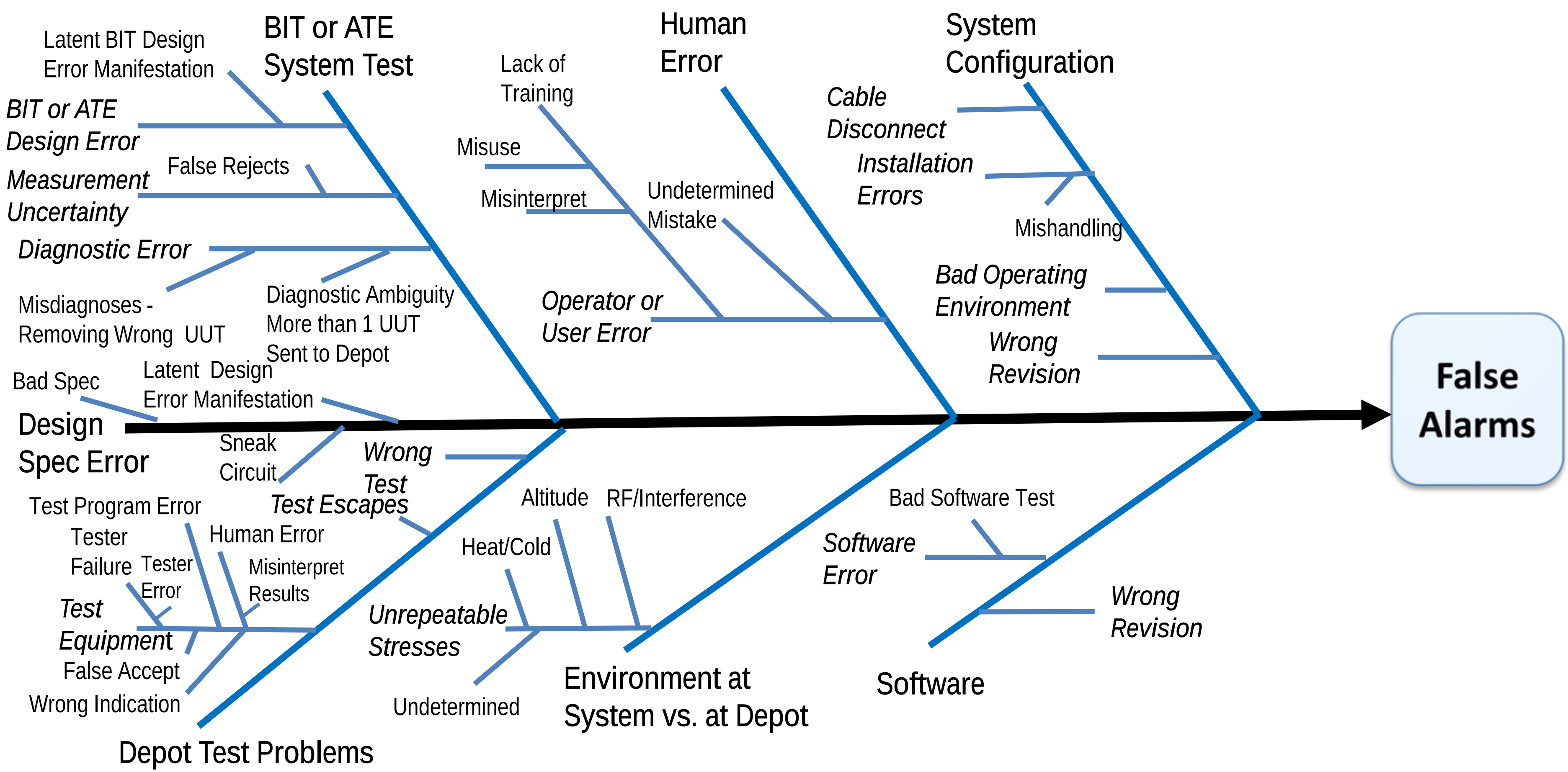
- Intermittent Failures (IFs)
  - At both System Level and at Depot Level
- False Alarms (FAs) from the System Level
  - FA at System Level becomes NFF at Depot Level

Causes of Intermittent Failures

Source: Qi H, Ganesan S, Pecht M, No-fault-found and intermittent failures in electronic products, 2008



Causes of False Alarms (FAs)



Quantifying NFFs

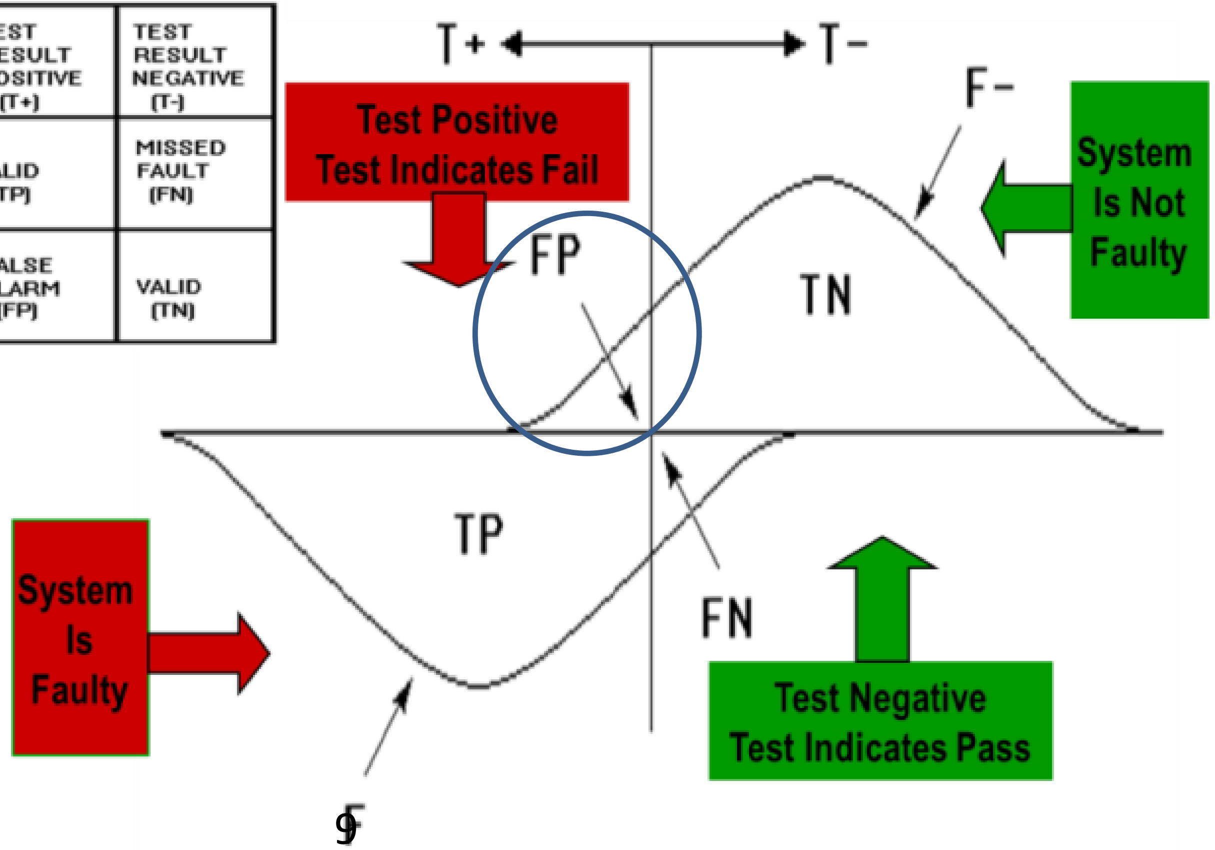
- False positives and Gaussian Distribution
- Bayes Formula with Example
- Calculating the likelihood of UUTs at depot being result of FAs
- Distribution of remaining faults between PFs and IFs
- Empirical confirmation of our calculations

CND Produced False Alarm Metrics

Test Outcome	Label	Typical % of cases
True Negative – Good UUT passes all tests.	TN	95%
True Positive – Faulty UUT fails one or more tests.	TP	95%
False Negative – A faulty UUT results in UUT passing the test. Also called "missed fault" or Type II error.	FN	5%
False Positive* – *A good UUT indicates that the test failed. Also called "false alarm" or Type I error.	***FP***	***5%***

Gaussian Representation of Test Outcomes

	TEST RESULT POSITIVE (T+)	TEST RESULT NEGATIVE (T-)
SYSTEM FAULTY (F)	VALID (TP)	MISSED FAULT (FN)
SYSTEM NOT FAULTY (F-)	FALSE ALARM (FP)	VALID (TN)



Bayes Formula

- Probability of an invalid faulty result, *P(F-/TP)*
  - This is the probability that a UUT in maintenance is a product of false alarm.
    - *P(F/TP) is the probability of **valid** faulty result*
    - *P(F)* is the probability that the system is in fact faulty.
    - *P(F-)* is the probability that the system is not faulty. Clearly, *P(F-) = 1 – P(F).*
    - *P(TP/F)* is the probability that a "System Faulty" result is due to the existence of a fault.
    - *P(TP/F-)* is the probability that a system which is not faulty is still called out as faulty.
    - *P(F/TP)* is the probability of a valid faulty result.
  - Using Bayes formula, the *Valid Faulty Result is*

$$P(F/TP) = P(TP/F)P(F)\ /[P(TP/F)P(F) + P(TP/F-)P(F-)]$$

  - And the Invalid Faulty Result (False Alarm) is
    $P(F-/TP) = 1 - P(F/TP)$

Bayes Formula Example

- An Example
  - The 95% fault detection will result in having 95% of the faulty system fail the test. P(TP/F) = 0.95
  - 10% of the systems diagnosed as faulty are in fact good. Fraction of False Alarm (FFA) = P(TP/F-) = 0.10.
  - Only 3% of the items tested are faulty. P(F) = 0.03. Thus the probability that a system is not faulty, P(F-) = 0.97.
- Using Bayes formula, the *Valid Faulty Result is*

  $P(F/TP) = P(TP/F)P(F) / [P(TP/F)P(F) + P(TP/F-)P(F-)]$

  $= (0.95)(0.03)/[(0.95)(0.03) + (0.1)(0.97)] = 0.23$
- And the Invalid Faulty Result (False Alarm) is
  - *P(F-/TP) = 1 - P(F/TP) = 1- 0.23 = **77%***

Reducing FFA to 2%
False Alarm becomes 60%

NFFs Due to FAs

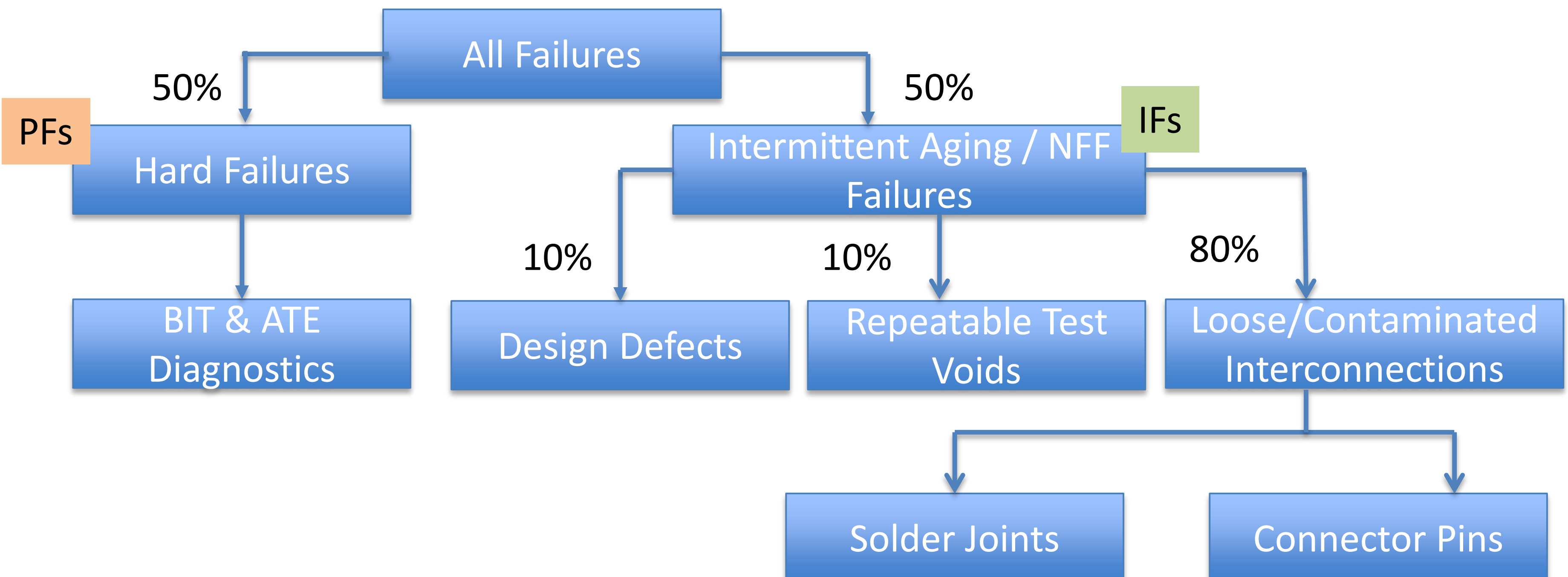
- Using the diagnostic resolution of 90% isolation to a single module, 95% to 2 or less modules and 100% to 3 or less modules, of a 100 system failures, we have:
  - UUTs removed = 100 + 2*(100-95) + 3*(100-10) = 140 UUTs/100 system failures
- Assuming 60% of system failures were FAs and 100% of all ambiguous replacements were also FAs,
  - FA UUTs removed = (60% of 100) + 100% (2*5) + 100% (3*10) = 100 FA UUTs
  - **Percentage of FA UUTs in the depot = 100/140 = *71.4% of all UUTs***

NFFs Due to FAs

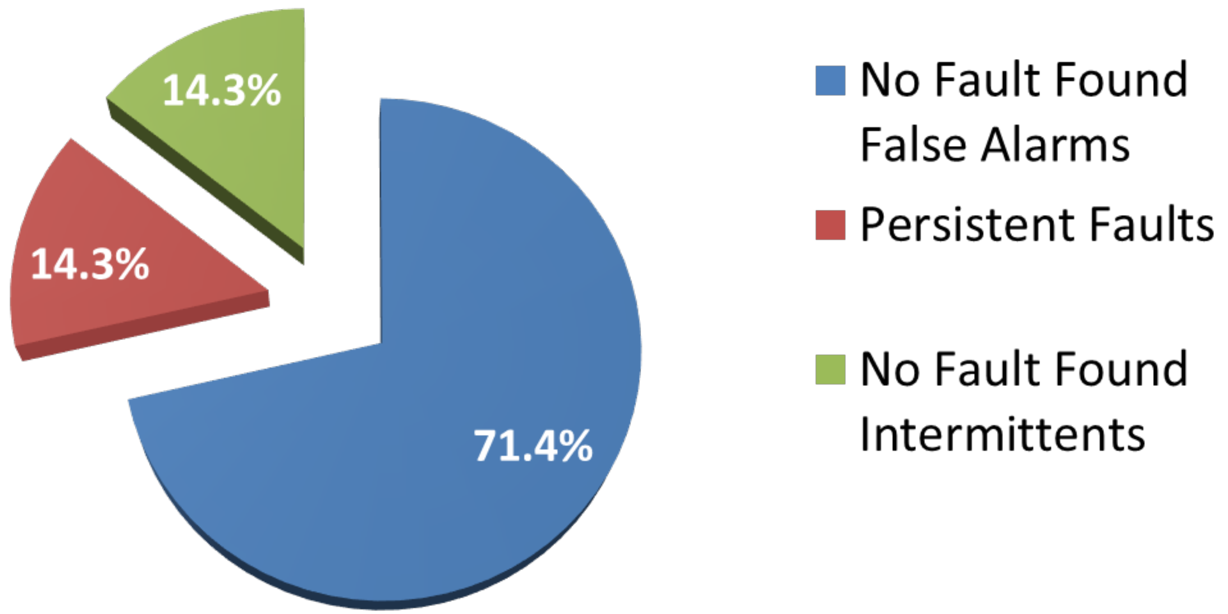
- Using the diagnostic resolution of 90% isolation to a single module, 95% to 2 or less modules and 100% to 3 or less modules, of a 100 system failures, we have:
  - UUTs removed = 100 + 2*(100-95) + 3*(100-10) = 140 UUTs/100 system failures
- Assuming 60% of system failures were FAs and 100% of all ambiguous replacements were also FAs,
  - FA UUTs removed = (60% of 100) + 100% (2*5) + 100% (3*10) = 100 FA UUTs
  - **Percentage of FA UUTs in the depot = 100/140 = *71.4% of all UUTs***

Permanent Failures (PFs) vs. Intermittent Failures (IFs)

Source: Sorensen B, Digital Averaging – the smoking gun behind 'No-Fault-Found,' Air Safety Week, Feb 24, 2003



Units Arriving at Depot Repair



Empirical Confirmation

- The F/A-18C was fielded with a built-in test (BIT) false alarm rate over 88% and a mean flight hour between false alarm (MFHBFA) rate of less than 1 hour.
  K. Bain and David G. Orwig, "F/A-18E/F Built-in-test (BIT) Maturation Process," Proceedings of NDIA Third Annual Systems Engineering & Supportability Conference, August 2000
  - **In some cases units returned due to false alarms exceed 83%.**
- Other services – Army, Navy, Marine Corps report upward of 67% false alarms.
- The V-22 displayed a BIT false alarm rate of 92% during its first Operational Test and Evaluation (OPEVAL) in 2000
  K. Westervelt, "Applying the Quality Function Deployment on the V-22 Osprey," 2010 IEEE Aerospace Conference, pp. 1-12, 2010.
- Boeing reported at AutoTestCon 2007 that some avionics on a military aircraft exhibited 100% false alarms.
- Automobile cruise control modules returned to factory – 96% NFF
  Kinseng K, Holt M, Precht M., Physics of failure assessment of a cruise control module, Microelectronics Reliability 39, 1999, p. 1423-1444.
- Mobile phones in 2005 resulted in 63% NFFs

Overton, D of WDS, Survey of Mobile Phones No Fault Found, http://www.wds.co/no-fault-found-returns-cost-the-mobile-industry-4-5-billion-per-year/, 2005.

Cost Impact of NFFs

- False Alarms Costs
- Empirical Cost Impact of NFFs
- Strategies to Eliminate NFFs

False Alarms Costs

- Each time we replace a good UUT we incur costs including:
  - Cost of replacement labor
  - Cost of reducing spare inventory
  - Cost of handling and administering replacements
  - Cost of the replacement unit
  - Cost of transporting replaced/replacement units
  - Cost of retesting replaced unit at the next level of repair (perhaps several times and under variations in environment, stress, etc.)
  - Administrative costs associated with the RTOK and a no fault found (NFF)
  - Possible replacement of subassemblies within a replaced UUT to attempt repair
  - Reexamining test procedures and programs to resolve the possible cause of RTOK
  - Stresses to UUT as a result of trying to resolve RTOK may reduce its reliability and may bring on early failures.

Empirical Cost Impact of NFFs

- Mobile phones NFFs estimated cost $4.5 Billion in 2005. Now about $10 Billion
- Overton, D of WDS, Survey of Mobile Phones No Fault Found, http://www.wds.co/no-fault-found-returns-cost-the-mobile-industry-4-5-billion-per-year/, 2005.
- US Department of Defense NFF cost $2 Billion and US Air Transport Association for commercial aircraft $2.2 Billion
  - Copernicus Technology Blog, Can you afford the cost of No Fault Found? http://blog.copernicustechnology.com/can-you-afford-the-cost-of-no-fault-found/, May 2014
- Computer Market?
- Automobile Electronics?
- Control Systems Electronics
- Home Monitoring Systems?
- Communication Systems?
- Other Electronics?

Strategies to Eliminate NFFs

1. Treat All NFFs as False Alarms and return all of them to system test
2. Treat All NFFs as Intermittent Failures and use environmentally stressed tests
3. Rely on Technician to use Educated Guess “Shot Gun”

	UUT < $200	UUT < $3,000	UUT > $10,000
Strategy 1	Not Advised	Good Choice	Good Choice
Strategy 2	Not Advised	Not Advised	Not Advised
Strategy 3	Good Choice	Better Choice	Better Choice

Conclusions

- NFFs are due to False Alarms (FAs) at System and Intermittent Failures (IFs)
- Ishikawa fishbone diagrams show the issues are complex
- Per Bayesian analysis more than 70% of UUTs at the repair facility are FAs
- The remaining divide evenly between approximately 15% IFs and 15% hard faults (PFs)
- The best strategy to deal with NFFs is to rely on technicians to decide
  - While also limiting shut gun approach to about 17% of NFFs
- It would be much better to arrest FAs at System Level
  - We need Design for Testability

Table 1- Classification of NFF Sources

Persistent Faults	No-Fault-Found (NFF) Intermittent Failures (IF)	No-Fault-Found (NFF) False Alarms (FA)	Indeterminate
Assembly faults within each UUT – Shorts, opens, missing components, wrong component, wrong component insertion	CND BIT Hard Failure	CND Operator Error	False accept conditions that occur when the depot tester inaccuracy renders a UUT as faulty. The UUT may in fact be faulty or not.
Parts faults – bad component, out of spec component	CND Transient (Functional) Failure	CND Latent BIT Design Error	System level failures not detectable at subsystem UUT level. Usually FA, but could be IF.
Functional failures from hard faults	RTOK Diagnostic ambiguity (DA) of all UUTs from same system if all UUTs are NFF	CND Latent Design Error Manifestation	Environmentally induced failures at operating conditions that are not available at the depot. E.g. failures at high altitudes only.
	Connectors – corrosion and wiring failures	CND Environmentally Induced BIT Error	Some system level cable becomes disconnected temporarily, perhaps due to corrosion.
	Components – IC crosstalk, electromigration, dielectric breakdown, metallization, ionic contamination, tin whiskers, wire bond lifts, creep corrosions, etc.	CND BIT Transient Failure	
	Printed circuit board – electro-chemical migration, via cracking, warpage and whiskers.	CND Environmentally Induced Functional Error	
	Component-PCB Interactions – solder problems, loads, manufacturing defects, socket problems	CND Flight Line Test Equipment Error	
		CND Flight Line Human Error	
		CND Test Equipment Failure	
		CND Human Error at Shop Level	
		RTOK Misdiagnoses or False Diagnosis (FD)	
		RTOK System level cable problem – UUTs connected by a faulty cable sent to depot.	
		RTOK System level software error	
		RTOK Diagnostic ambiguity (DA) of 2nd, 3rd, etc. UUTs sent to depot if 1st UUT is not NFF	
		False Reject -Measurement tolerances and uncertainties causing a good system to fails system test.	

Thank you

Questions?