Entwicklungsziel Zuverlässigkeit: MTBF ist nur der Anfang

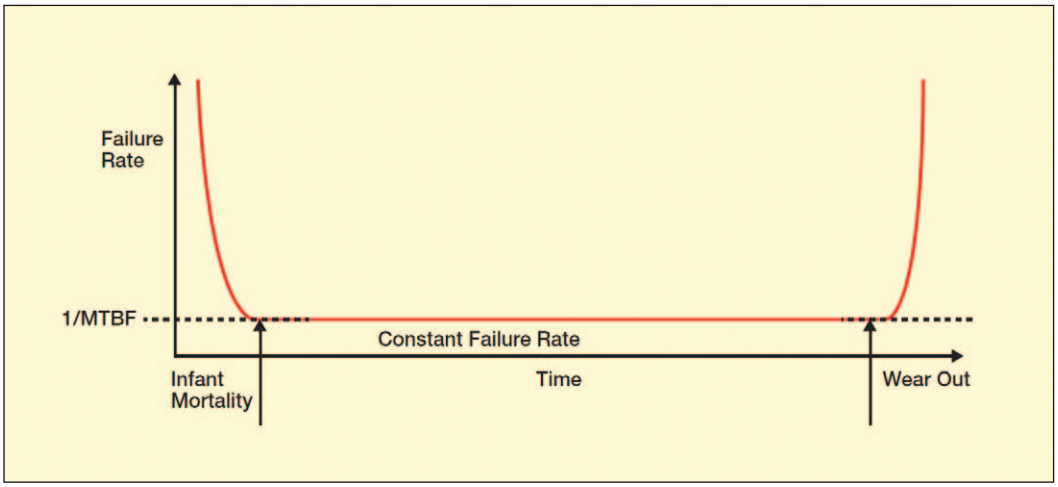

Bild 1: Die Badewannenkurve veranschaulicht die Frühausfälle bei der Einführung eines Produkts, die Ausfälle während dessen Lebenszeit, sowie die Abnutzungsausfälle zum Ende der Lebenszeit.

Bestmögliche, quantitativ umrissene Zuverlässigkeit im Sinne der vorgesehenen Applikation ist eine der wichtigsten Kenngrößen erfolgreicher Systementwicklungen.

Adam P. Taylor
Xilinx
www.xilinx.com

Als zentrale Metrik zur Abschätzung der Zuverlässigkeit gilt gemeinhin der MTBF-Wert (mean time between failures) des Systems, der seine Ausfallwahrscheinlichkeit vorhersagt. Ein zweiter Faktor für den Nutzwert eines Produkts ist die ‚Erfolgswahrscheinlichkeit' (probability of success).

Im Aerospace- und Miltärbereich ist die Zuverlässigkeit eines Systems ganz selbstverständlich greifbar in Bezug auf die Sicherheit der Passagiere oder der vorgesehenen Mission. In der Telekommunikation gilt es Systemausfälle zu vermeiden oder zu minimieren. In industriellen Anwendungen sind die treibenden Kräfte das wirtschaftliche Ergebnis und die Reputation des Anbieters. Auch hier gelten als sekundäre Bedingungen der sichere Betrieb des Systems im Fehlerfall und die Abgabe einer Fehlermeldung, die das aktuelle Problem umreißt. Unter kommerziellen Gesichtspunkten müssen die Entwickler sicherstellen, dass die gefertigten Produkte ihre vorgeschriebenen Garantiebedingungen erfüllen.

Alles das fließt in die Zuverlässigkeitsbetrachtungen beim Systemdesign mit FPGAs ein. Der Einsatz von FPGAs erlaubt höher integrierte Systemlösungen. Das erhöht auch den MTBF-Wert, insbesondere, wenn der Hersteller der Bausteine dem Anwender regelmäßige vierteljährliche Zuverlässigkeits-Reports zur Verfügung stellt. Xilinx bietet dies unter der Bezeichnung UG116.

MTBF ist ein Maß für die Wahrscheinlichkeit, dass ein System über seine Lebensdauer gemäß den Spezifikationen operiert, oft veranschaulicht in der bekannten Charakteristik als „Badewannenkurve". Für eine zuverlässige Designlösung muss eine Entwicklungsumgebung die korrekten Vorgaben, Review-Gates, Designregeln und Richtlinien anbieten, zusammen mit unabhängigen Peer-Reviews zu den angemessenen Zeitpunkten im Lebenszyklus eines Produkts.

MTBF und Ausfallkurve

Die Definition des MTBF-Werts ist eine statistische Voraussage über die Zeit zwischen zwei Ausfällen während der Betriebszeit eines Systems. Die Hersteller berechnen den MTBF-Wert eines Systems als Reziprokwert der Summe der Ausfallraten seiner Komponenten. Diese Ausfallraten werden meist als FIT-Rate (failure in time) bezeichnet, in der Größenordung 1x 10^{-9} pro Stunde. Man erhält Angaben über die Ausfallraten vom Hersteller der Komponenten oder entnimmt sie einem Standardwerk wie dem US-Military Handbook MIL-HDBK-217F oder Bellcore/Telcordia SR332.

Die Beziehung zwischen MTBF und FIT-Rate lautet:

MTBF = 1 / FIT-Rate

Allerdings sind diese Ausfallraten nur gültig im Bereich des geradlinigen Verlaufs der Badewannenkurve nach Bild 1.

Diese Kurve setzt die Frühausfälle (‚infant mortality') bei der Einführung eines Produkts ins Verhältnis mit den Ausfällen während der normalen Lebensdauer (‚constant failure rate') und den Ausfällen zum Ende der vorgesehenen Lebenszeit. Dem trägt die Burn-in-Prozedur während der Herstellung Rechnung. Sie soll die Frühausfälle aus dem Kurvenverlauf ausschließen. Die dabei applizierten Temperaturzyklen beschleunigen die Ausfälle durch latente Defekte vor der Auslieferung und der Systemintegration.

An welcher Position auf der Badewannenkurve sich ein

Produkt oder System befindet, lässt sich durch eine Weibull- oder Lebensdatenanalyse in Excel einfach bestimmen. Der Formparameter ß zeigt an, ob die Ausfallrate stabil, ansteigend oder abfallend ist. Ein Formparameter β kleiner als 1,0 bezeichnet eine abfallende Ausfallrate während der Frühausfallperiode, während ein Wert größer als Eins auf eine steigende Ausfallrate deutet, etwa in der Phase der fortgeschrittenen Abnutzung eines Produkts.

Nach der Bestimmung des Ortes auf der Badewannenkurve könnte man geneigt sein, anzunehmen, dass das untersuchte System zumindest in der dem MTBF-Wert entsprechenden Zeitspanne erfolgreich arbeitet. Leider ist dies so nicht richtig, denn MTBF ist nur eine statistische Repräsentation der Ausfallrate, die man in der Nutzungsphase eines Produkts erwarten kann. Nochmals: MTBF repräsentiert nicht die vorhergesagte Lebenszeit des Produkts.

Um die vorhergesagte Lebensdauer zu ermitteln, muss man die „Erfolgswahrscheinlichkeit" (probability of success) P einer Entwicklung betrachten. In der folgenden Gleichung ist t die gewünschte Betriebszeit in Stunden.

$$P(s) = - t / e^{MTBF}$$

Wenn man die Erfolgswahrscheinlichkeit graphisch aufträgt, erkennt man, dass bei der Annäherung der gewünschten Betriebszeit an den MTBF-Wert die Erfolgswahrscheinlichkeit etwa 0,37 beträgt (Bild 2). Wenn man also in diesem Zusammenhang eine Serie von Produkten betrachtet, sind immer noch 37 Prozent von ihnen funktionstüchtig.

Um also eine akzeptable Erfolgswahrscheinlichkeit über die Lebensdauer des Produkts oder seiner Mission sicher zu stellen, erfordern viele Systeme und Produkte einen MTBF-Wert, der signifikant höher liegt als deren vorgesehene Lebensdauer. So muss bei einer angenommenen Lebensdauer von fünf Jahren und einer Erfolgswahrscheinlichkeit von 0,99 der MTBF-Wert 4.361.048 Stunden oder 497 Jahre betragen. Das ist um ein Vielfaches länger als die Betriebszeit. Dazu die folgende Gleichung:

$$MTBF = P(s) / - ln(t)$$

Berechnung der Zuverlässigkeit

Man kann die Zuverlässigkeit und den MTBF-Wert nach zwei Methoden ermitteln – entweder über eine Analyse der Komponentenzahl (parts-count analysis) oder über eine Belastungsanalyse der Komponenten (part stress analysis). Die Parts-count-Analyse ist das Einfachere der beiden Verfahren. Sie wird manchmal in einem frühen Entwicklungsstadium ausgeführt als Indikator, ob das zu entwickelnde Produkt seine Zuverlässigkeitsanforderungen erreichen wird. Diese Analyse berücksichtigt das Qualitätsniveau des eingesetzten Bauteils, die Anzahl der eingesetzten Bauteile und die Nutzungsbedingungen des Produkts. Eine Parts-count-Analyse ist schnell ausgeführt. Doch die Ergebnisse tendieren eher zur pessimistischen Sicht, also zu höheren Ausfallraten und niedrigerer MTBF.

Eine Stress-Analyse der Bauteile zieht eine weit größere Zahl von Parametern in Betracht. Deshalb nimmt sie entsprechend mehr Zeit in Anspruch, liefert dafür aber ein genaueres Ergebnis. Eine Stress-Analyse umfasst viele Faktoren, wie Temperatur, elektrische Belastung, Qualität, Aufbau, Betriebsumgebung und anderes mehr, je nach dem analysierten Komponententyp. Diese Analyse resultiert in einer sehr viel genaueren Ausfallrate für die vorgesehene Applikation.

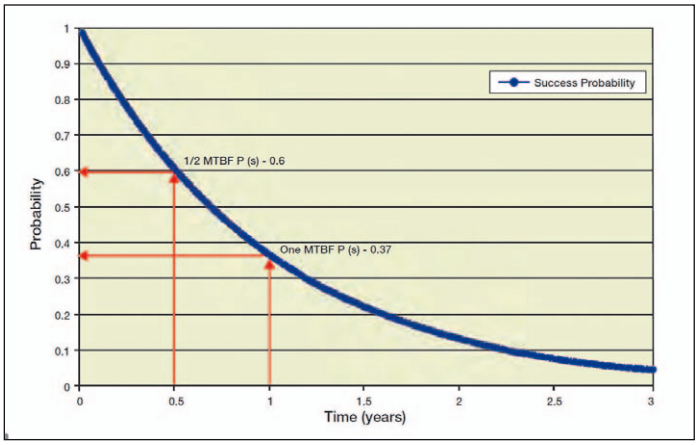

Bild 2: Wenn die gewünschte Betriebszeit die Größe von MTBF erreicht, ist die Erfolgswahrscheinlichkeit 0,37.

Erhöhung der Zuverlässigkeit

Zur Erhöhung des MTBF-Werts und der Erfolgswahrscheinlichkeit der Produkt- oder Systementwicklung gibt es eine ganze Reihe von Verfahren. Die am häufigsten eingesetzte Taktik ist das Derating der Komponenten in Bezug auf die elektrischen und thermischen Belastungen. Derating erlaubt die Einbeziehung der Belastungen des Bauteils bei der oben beschriebenen Stress-Analyse. Die Bauelementehersteller schreiben oft ihre eigenen Derating-Regeln vor. Doch man kann auch Industrie-Standard-Regeln nutzen, wenn keine In-house-Vorschriften verfügbar sind. Beispiele sind ECSS-Q-30-11A der ESA (European Space Agency) und NAVSEA TE000-AB-GTP-010 der US-Navy.

Die Durchführung einer Stress-Analyse der Bauteile erhöht die Fixkosten einer Entwicklung. Andere Analyseverfahren für Entwickler wirken sich auf die laufenden Kosten aus.

Die erste Option zur Verbesserung der Zuverlässigkeit sind Komponenten mit höherem Qualitätslevel, unter Beibehaltung derselben oder ähnlicher Derating-Ansätze. So kann man von

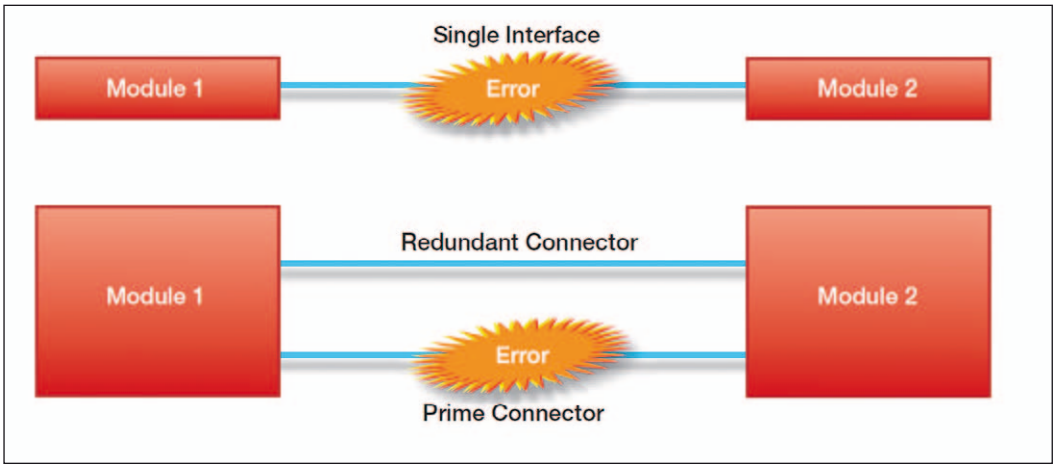

Bild 3: Beim Ausfall des regulären Steckverbinders übernimmt eine redundante Einheit – bei höherer Komplexität.

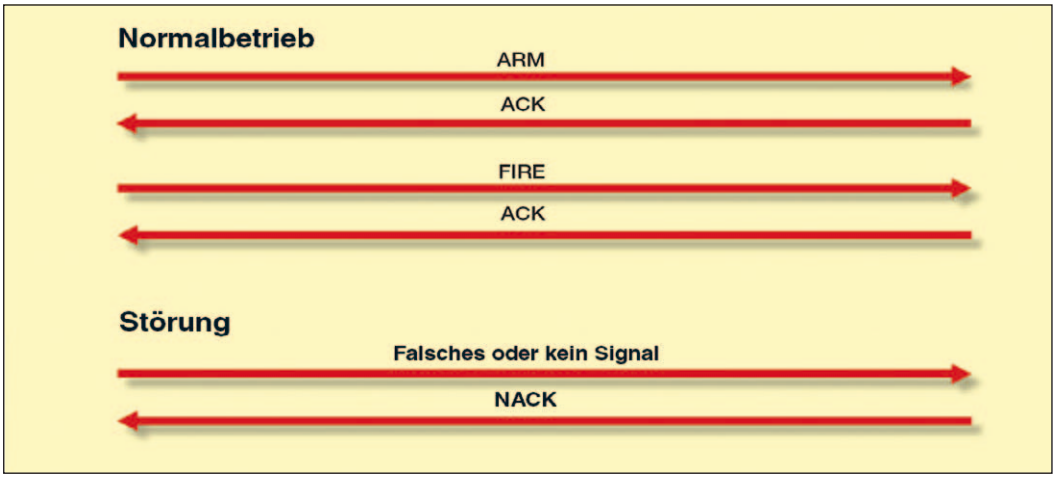

Bild 4: Eine „Arm and Fire"-Sequenz hilft in elektromagnetisch gestörten Umgebungen.

Type	Standard	Military	Space
Integrated Circuits	MIL-PRF-38535	QML Q (Class B)	QML V (Class S)
Hybirds	MIL-PRF-38536	Class H	Class K
Discrete	MIL-PRF-19500	JAN TXV	JAN S

Tabelle 1: Standard-, Militär- und Raumfahrtversionen von ICs, Hybriden und diskreten Komponenten.

Parameter	Comment
Temperature	Units and critical component
Current	Drawn from main supply
Voltages	The health of subregulated voltages within the system
Redundancy Switching	Reports position of any switches used to route prime/redundant signals
Processing Status	Results of CRC, over- and underflow of calculations, signals out of range, etc.

Tabelle 2: Aspekte der Überwachung des Systemstatus.

Code	Error Correction	Error Detection	Comment
Parity	X		Errors can be masked
N of M	X		Not suitable to multiple bit
CRC	X		Good for burst errors
BCH	X	X	Easy to Decode
Hamming	X	X	One of First EDC
Reed Solomon	X	X	Special case of BCH

Tabelle 3: EDAC-Codes, einfach bis komplex.

kommerziellen Standard-Bauteilen auf militärische (QML Q für ICs) oder sogar Raumfahrt-qualifizierte (QML V für ICs) Komponenten übergehen. Bei steigendem Qualitätslevel steigt natürlich auch der Preis. Tabelle 1 listet unterschiedliche Standards für ICs, Hybride und diskrete Komponenten.

Einführung von Redundanz

Die zweite Option ist die Einführung von Redundanz in oder zwischen den Systemeinheiten. Redundanz erhöht die Baugröße, das Gewicht und die Kosten der Lösung. Doch sie hat einen dramatischen Effekt auf die Zuverlässigkeit und die Verfügbarkeit des Systems. Am besten trifft man die Entscheidung über die nötige Redundanz auf der Systemebene, und fügt zusätzliche Komponenten in den Bereichen des Designs ein, in denen die Ausfallrate hoch ist. Dieses gezielte Vorgehen in Bezug auf die Redundanz liefert gut optimierte Lösungen.

Eine weitere Betrachtung in Bezug auf die Redundanz ist die Frage „hot" oder „cold". In einer heißen Redundanz-Lösung bleibt das redundante System ständig eingeschaltet und konfiguriert. Es lässt sich also sofort und unmittelbar zuschalten, um eine ausgefallene Einheit zu ersetzen, ohne Beeinträchtigung der System-Performance. Der Nachteil dieses Szenarios ist, dass auch das redundante Equipment ständig gewissen Belastungen ausgesetzt ist.

In einer kalten Redundanzanordnung ist das redundante System nicht eingeschaltet. Es wird nur dann hochgefahren, wenn die primäre Einheit ausgefallen ist. Das Gesamtsystem stoppt also seine Aktivität, bis das redundante Element so konfiguriert ist, dass es die Funktion der ausgefallenen Einheit übernehmen und fortsetzen kann. Das bewirkt eine Unterbrechung des Betriebs. Doch der Vorteil liegt darin, dass eine kalte Lösung nicht altert, weil sie im Aus-Zustand keiner elektrischen Belastung

unterliegt. Bei der Einführung von Redundanz muss man natürlich dafür sorgen, dass keine unerwünschte Ausbreitung von Störungen innerhalb des Systems auftritt, die beim Ausfall der primären Einheit auch die Funktion des redundanten Moduls nachteilig beeinflussen könnte.

Betrachtungen auf der Systemebene

Neben der Betrachtung der Bauteile-Qualität und der Redundanz mit ihrem signifikanten Einfluss auf die Zuverlässigkeit des Gesamtsystems gibt es eine Reihe weiterer Optionen, die man implementieren kann, um die korrekte Performance unter Fehlerbedingungen oder bei Ausfallereignissen zu sichern. Dazu zählen:

- Ausbreitung von gefährlichen Ausfallzuständen
- Eingebaute Test-, Telemetrie- und Event-Logs zur Überwachung und Aufzeichnung der Systemfunktion
- Equipment-Schnittstellen mit einzelnen Steckverbindern, oder mit primären und redundanten Einheiten
- Kritische Befehlssequenzen (z. B. Auftrennung der „Arm“- und „Fire“-Befehle des Systems)
- Akzeptable Fehlerraten (BER, ECC) in Speichern und auf Datenverbindungen

Im Rahmen von geltenden Regulierungen und Zertifikationen muss man oft eine Gefahrenanalyse durchführen, um potenzielle Gefahren zu erkennen und auszuschließen, die bei einem Ausfall der Einheit auftreten können. Es liegt in der Verantwortung des Entwicklers, das angemessene Verhalten eines Produkts auf der Systemebene sicherzustellen, etwa durch geeignete Sperrvorrichtungen und ähnliche Maßnahmen. Falls nötig, sollte man diese Schutz- und Korrekturfunktionen als genau definierte Anforderungen auf Subsysteme verlagern, um die Ausfall-Moden richtig zu adressieren.

Die genaue Kenntnis des regulären Betriebszustandes des Equipments mit Reports oder Aufzeichnungen über dessen korrekten Status kann man auch als Prognose-Tool nutzen. Damit ermöglicht man ausfallsicheren Betrieb und die Aufdeckung von Fehlerursachen zur schnelleren Reparatur. Komplexe Systeme sollten auch eine umfassende Selbsttest-Funktionalität einschließen, entweder beim Einschalten oder kontinuierlich während des Betriebsablaufs. Tabelle 2 listet die Aspekte empfehlenswerter On-demand-Testroutinen.

Die Ergebnisse solcher Tests lassen sich in Form von Zustandsberichten über eine Datenverbindung ausgeben oder in nichtflüchtigen Speichern (Flash oder FRAM) ablegen. Dies geschieht entweder mit Echtzeit-Erfassung oder einem Zähler, der diese Ereignisse mit einer Zeitlinie versieht, um ihre ursächliche Einordnung zu ermöglichen.

Besondere Beachtung beim Systembetrieb in rauen Umgebungen gilt den Steckverbindern. Sie sind eine häufige Ausfallursache, da einzelne Anschlüsse im Steckverbinder unterbrochen sein können oder die Kabel durch mechanische Schocks und Vibrationen abfallen können. Also erzielt man größere Zuverlässigkeit durch die Einführung redundanter Verbinder und Kabel. Beim Ausfall des primären Verbinders übernimmt die redundante Einheit (Bild 3). Auch hier entsteht wachsende Komplexität, wenn viele Module zu verbinden sind. Eine gängige Alternative ist die Nutzung von Steckverbindern, die speziell für harsche Umgebungen ausgelegt sind, etwa nach MIL-STD 38999.

Wenn das System oder Produkt für raue Umgebungen mit elektromagnetischen Feldstörungen vorgesehen ist, kann es angebracht sein, eine „Arm-and-Fire“-Methodik (Bereitstellen und Auslösen) einzusetzen, deren Befehle über interne Datenbusse übertragen werden. In der Anordnung nach Bild 4 wird zunächst ein solcher Befehl zum Empfänger geleitet, der ihn bestätigt und eine Auszeit (time-out) startet. Der Empfänger gibt ein NACK-(negative acknowledge character) Kommando aus, so lange er nicht das „Fire“-Kommando erhält. Andernfalls reagiert er mit einem ACK-Signal, bevor die Auszeit beginnt. Erhält der Empfänger irgendein anderes Signal, gibt er NACK aus, und der Vorgang startet von neuem. Somit können unvollständige Signale, etwa infolge elektromagnetischer Interferenzen (EMI), keine unbeabsichtigten kritischen Befehle auslösen.

Ähnlich dem „Arm-and-Fire“-Prinzip kann man auch sicherstellen, dass alle Datenverbindungen und Speicher geeignete Codes zur Fehlerkorrektur und -detektion haben, um zuverlässige Datenübertragung und Speicherung zu gewährleisten. Die Wahl zwischen reiner Fehlerdetektion und Detektion plus Korrektur ist durch die finale Applikation bedingt. Es gibt allerdings eine Reihe von einsetzbaren Codes, die man vom einfachsten bis zum kompliziertesten Fall skalieren kann (Tabelle 3). Deren Schutzumfang skaliert mit der Komplexität des Codes.

Autor:

Adam P. Taylor ist Head of Engineering Systems bei e2v.