Electronic Design

By JERRY TWOMEY, Engineering Consultant, Effective Electrons

The Do's and Don'ts of Designing Robust and Reliable Systems

Cost-effective strategies and best practices for designing robust and reliable electronics, ensuring longevity and performance without increasing product cost.

The crown jewels in the world of high-reliability embedded systems are the Voyager spacecraft. Voyager 1 and Voyager 2 remain in service after being launched close to 50 years ago, and they're expected to continue running until 2032. However, reliability and robustness in electronics can be achieved at a much lower cost than an interstellar satellite. The end goal for engineers is to build devices that can tolerate multiple forms of abuse without increasing product cost.

High-reliability electronics can be implemented with many levels of rigor. At one extreme, there are failsafe systems where reliability is the top priority and cost is less of a factor. This includes the avionics of military and commercial airplanes, which tend to have several redundant systems that run the same computations and check each other's results for issues.

When such systems don't concur, they're swapped out for a secondary system, while the primary computer pair executes a self-test and check assessment before being returned to service.

Many satellites use triplication and voting methods for digital processing. This technique looks at the results of three independent logic systems and uses the majority result. It improves reliability when radiation ions strike the logic ICs. Failsafe systems add redundancy but incur added costs to improve reliability.

A multitude of best practices can help designers add reliability and robustness to consumer electronics and other systems that aren't as mission-critical as military airplanes, satellites, or spacecraft. These include:

- Eliminating historically unreliable components.
- Designing circuits to reduce the risks to reliability.
- Reconfiguring the PCB and interconnect wiring to reduce failure mechanisms.
- Applying software/code techniques that improve the system's reliability and ability to recover.
- Rigorously testing the system to identify potential issues

and then fixing them ahead of production.

As it turns out, many of these best practices can be implemented with little or no added cost to the final product. Swapping out or removing unreliable components from the design is the obvious first step.

5 Tips for Robust and Reliable Component Selection

Component failures are dominated by two parts—power transistors and capacitors—so it makes sense to start there.

Eliminate electrolytic capacitors (ECs) wherever possible

While these capacitors are cheap and widely used, they're the most common source of component failure in many systems. It's worth noting that the EC has a limited life, which depends on the specific qualities of the device. Lifespan is also related to the temperatures that these parts are exposed to.

Using surface-mount (SMT) multilayer ceramic capacitors (MLCC) is a much more reliable alternative, and they're widely available up to 100 µF. Larger capacitance values are available that aren't SMT-MLCC, but all devices must be carefully qualified before use.

Include generous design margins on components

In general, power transistors operating close to their specified limits will result in a shorter lifespan. This includes excesses in current, temperature, and voltage. Capacitors should be kept well away from their maximum voltage rating. Power dissipation, maximum current, maximum voltage, and operating temperature range need to be examined for all components.

Mitigate hot components

Any component operating close to or outside thermal limits will have a higher failure occurrence. For switched power transistors, choosing parts with lower $R_{DS(on)}$ will keep heat under control. Voltage-regulator ICs with large $V_{IN} - V_{OUT}$ values will exhibit significant self-heating, especially as output currents rise. Design margin on the power rating of resistors needs to be checked as well. As a backup plan, you can add a heatsink to a hot device. Limiting heat creation is the preferred strategy.

Eliminate mechanical switches and relays

Mechanical switches used as inputs to a system can usually be replaced by more modern methods that avoid mechanical wear and tear. This includes capacitive touch sense, opto-interrupters, and Hall sensors. High current switching by relays can usually be replaced by an on/off control signal to the power supply, a solid-state relay, or other semiconductor power switches.

Carefully examine lifetime and reliability data in the AC-DC power supply

Many electronic designs use a standard product power supply. Beyond voltage and current capabilities, these devices can have starkly different standards for reliability. On top of that, some AC-DC converters lack safety shutdown features and many use short-life capacitors. The noise on the output power tends to vary between products.

High-reliability design is more than just choosing the right components, though. Next, a multitude of circuit features can affect circuit reliability, and omissions of others can leave your system vulnerable.

A Design Checklist for High-Reliability Circuit Design

Minimize the use of analog circuits

Analog signal processing is still required in certain places, but these are usually high-frequency scenarios or other special requirements. With modern data converters, digital signal processing costs less to implement and offers better long-term repeatability. Analog methods often require high-quality—and so, high-cost—components to maintain accurate response and linearity.

Include specific features necessary for signals over cables

Cabled data connections require several things to be reliable. This includes differential signals to improve noise immunity and dealing with the lack of common ground and error detection and correction to validate data and request re-transmission when needed.

Cable-friendly methods include USB, Ethernet, RS-485, and CAN bus. All use variants on low-voltage differential signaling (LVDS) signals and a protocol that checks data integrity and requests re-transmission upon detecting errors. Ground referenced data interfaces like I2C, SMB, and SPI are designed for use only on a single PCB and have no error detection. Non-differential data becomes error-prone due to noise and variance between the grounds at each end of the connection.

Furthermore, take care not to run analog signals over a lengthy cable. Instead, run the signal through an analog-to-digital converter (ADC) so that you can send data across the cable instead. This minimizes signal-integrity problems.

Protect external port connections

External ports are often subjected to electrostatic-discharge (ESD) events, accidental groundings, or forced input voltages. ESD protection can be implemented by current limiting the connection, giving you a port that can suffer abuse while avoiding permanent damage.

Include protective shutdown methods

Temperature sensing for motors and other high-power devices can tell the main controller that the device is approaching destructive temperatures. A fuse strategy for current overload may require both high- and low-current subsections. For instance, if a motor requires a 20-A fuse and the PCB needs 1 A, the PCB should be individually fused so that it can never burn up when faced with a 20-A overcurrent.

Use on-board voltage regulators for stable on-board power

Creating the final power supply off the PCB means that the voltage on the PCB will fluctuate due to surge currents and the inductance of the wire interconnect. Local, on-board voltage regulation allows for a low-impedance power grid with better stability.

Consider connector types and interconnect strategies

In general, interconnects that go to cables and plug-in cards are a frequent failure point, so it's worth considering whether they're necessary. Other connector issues to consider:

- Minimize plug-ins: A single PCB will be more reliable than a motherboard with multiple connections to other boards.
- Design an "error impossible" plug-in strategy: When practical, every connector on the PCB should be unique, stopping improper plugging in the wrong device/location. Plugs should be keyed in some manner to prevent improper insertion or designed to be compatible with any orientation plugging.
- Use multi-contacts for high-current connections: Parallel connected contacts add redundancy and reduce the overall resistance of the connection.
- Qualify connectors: Check connector specifications for insertion life, contact wear, contact materials, and contact plating thickness. Many miniature connectors are designed only for single insertion and fail upon multi-insertion use.

Monitor and control the application as well as the internal system

In addition to controlling the blinky lights, bells, and buzzers of the system, monitoring and controlling the internal electronics can be valuable. Some examples:

- Use power sequence control to selectively enable/power internal systems: This can be implemented with the MCU powered on at all times, and it can enable the rest of the system. This allows for a more orderly and predictable power-up sequence.
- Monitor currents and voltages of critical system parts: The average current for a motor tells a story. If the current rises over time, it could indicate a bad motor bearing. The common modern example here is the "check engine" light in a car. That's the result of many things being monitored in the system.

Of course, if any of the basic connections are faulty, all bets are off on the entire system. Getting the PCB interconnects and cabling right is the next step in high-reliability system design.

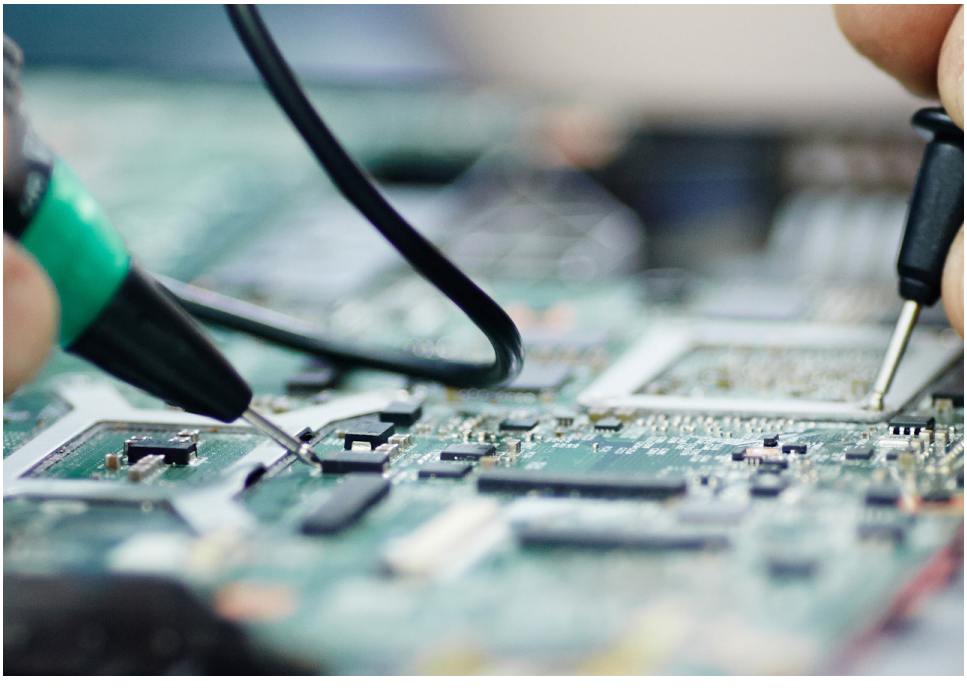
The Ins and Outs of PCB Interconnects and Wiring

No soldering of stranded wire

Stranded wire is used in situations where the wire must be able to flex without fear of failure. If the end of the wire is soldered, it creates a hard solder/wire region that tends to break with repetitive flexing or vibration. Stranded wires should be connected using crimped connections, not solder. Crimped connections are the preferred approach for NASA and aerospace and avionics in general.

Use highly flexible wires for cable connections

Not all stranded wire is created the same. The cables in industrial robotics or other systems that are constantly in motion require wire and cable structures that can withstand the physical demands of the application. Specialty vendors produce wire and cable bundles designated as "high flex" or "continuous flex" cabling. Vendors define flex radius limits and typical cycles of the cable flexing unique to their products.



Strain-relief cable bodies near PCB connector

Connecting cables securely to the device chassis or other mount near to the cable-PCB connector minimizes mechanical strain of the actual electrical connector. Doing so

reduces wear and tear induced by vibrations and bending, and it minimizes loosening of the electrical connector.

PCB mounting to mitigate vibration and shock

Depending on the situation, mounting may require more than corner mounting posts on the PCB. Longer distances between mounts can set up sections of the PCB to resonate when the device is subject to vibration or shock. The IPC, NASA, and even the U.S. aerospace and defense industry have all defined tests and guidelines to determine suitable mounting methods.

Use fatter traces and wider separations in PCB layout

The IPC specifies minimum trace separation down to 0.1 mm. Except for the highest-density layouts, most designs can use larger dimensions. Larger feature sizes typically yield better, are more resilient to physical abuse, and less susceptible to tin whiskers that can cause bridge shorting.

Minimize probability of tin whiskers

Problems stemming from tin whiskers became more common as RoHS efforts removed lead from PCBs. Tin whiskers can cause shorting between different circuit nodes, with the most common occurrence being from plated tin surfaces. Pure tin plating seems to be common to most tin whisker problems. While tin whiskers are still being researched, there are methods to reduce the risk:

- Avoid pure tin plating of components and use a small amount of lead in the plating alloy.
- Avoid minimum interconnect separation and maximize separation spacing.
- When possible, use nickel plating instead of tin.
- Investigate PCB conformal coatings, which can be effective.

Implement a comprehensive EMC strategy

All devices need to meet FCC requirements for radiated emissions. But rejecting the effects of both radiated and conducted EMI will help any product survive in demanding environments.

However, it's not all about the physical implementation. Addressing several software and coding issues can assist in improving system reliability.

Software: The Other Secret to High-Reliability Hardware

If implemented correctly, defensive coding methods can help you avoid the need to turn the power off-on to start a recovery. These tactics include:

Configure a watchdog timer

If the system gets hung up and doesn't respond as expected, a watchdog timer can help the system recover by initiating a restart routine.

Insert Figure 3

Set up background re-initialization

Most embedded systems do an initialization upon power up, and then never consider initialization settings during regular use. If something corrupts those settings, the system fails. Instead, include the capability to check the configuration status, or blindly reload configuration information periodically. This aids self-recovery without needing to "pull the plug" and force a restart routine.

Include device driver routines that protect the peripherals

At a minimum, device driver code includes those actions and responses necessary to control the peripheral. Beyond the basics, the capability to monitor the peripheral, and protectively react when things go "off the rails," can improve both reliability and safety. This is especially important for systems using motion control, motors, and other actuators.

Pre-process your data inputs

Data from sensors or HMIs should be examined to see if it makes sense within the system. If the data is outside the expected range, a re-measurement can be called for to determine validity. Similarly, keyboard entries should be checked for validity of the input and acceptable format. For noisy environments, averaging can be used to reduce

the effects of noise. Finally, switch inputs should be processed to eliminate contact bounce.

Testing: The Final Step Before Full Production

Depending on the situation, several other best practices should be considered before finishing up a product design, namely:

Perform comprehensive EMC testing

Most consumer products require radiated emissions testing to keep the FCC happy. Medical, military, and aerospace applications require more rigorous EMC testing for regulatory compliance. The standard medical-device test suite is readily available from regulatory compliance labs and will expose vulnerabilities, many of which can be easily mitigated.

Avoid a product recall by getting these tests done before the product moves to production. This is a one-time expense that will pay for itself.

Burn-in testing

Extended testing of the final product with an elevated temperature and high levels of circuit and mechanical activity, called burn-in testing, will often yield information about unexpected weaknesses.

Thermal imaging

A thermal image of the PCB tells a quick story about any components that are running hot. Make sure thermal images are done in all possible modes of operation, and that all circuits are active.

Vibration, shock, and acceleration tests

Mechanical vibration and shock testing is a must-have for high-reliability systems, specifically in the U.S. defense industry, which has to meet the MIL-STD-810 standard. Unless required, full compliance with regulatory testing doesn't need to be the goal, but these tests will point out potential problems. The test results should be examined to determine if corrective actions are needed.

Determine a protection strategy against corrosion and moisture

The need for corrosion protection depends on the environmental conditions to which the system is exposed. Potential solutions to the problem include sealed enclosures, the use of corrosion-resistant metal plating on electrical contacts, sealing the PCB with conformal coating, anticorrosive lubricants in electrical connectors, use of stainless-steel mounting hardware, and humidity control of the environment.

High-Reliability Hardware isn't Out of Reach

Most consumer electronics never address all of the issues outlined above. But while many of the fixes may require more investment in engineering, they can be implemented without additional cost at a product or system level. To go deeper, check out, *Applied Embedded Electronics – Design Essentials for Robust Systems*. The book presents in-depth illustrations and more detailed explanations, and it outlines a nuts-and-bolts design approach to highly reliable and robust embedded systems.

Jerry Twomey is an engineering consultant with Effective Electrons. He has extensive experience designing electronics, medical devices, electromechanical systems, and transistor-level integrated circuits. He is also the author of the book Applied Embedded Electronics – Design Essentials for Robust Systems. This is an in-depth reference that covers the design process from initial concept to final PCB, for all embedded-system electronics.

References

Jerry Twomey, *Applied Embedded Electronics – Design Essentials for Robust Systems*, 2023, O'Reilly Media, ISBN-13: 978-10981447911.

S. Yang, A. Bryant, P. Mawby, D. Xiang, R. Li, and P. Tavner, "An Industry-Based Survey of Reliability in Power Electronic Converters," *IEEE Transactions on Industry Applications*, vol. 47, pp. 1441-1451, 2011.