Powering Up the Protection for Medical Device Batteries

Counterfeit products are a problem for many original equipment manufacturers across all market sectors. However, in the medical device area, it can have a significant, life-threatening impact that has the potential to not only harm patients, but also cause irreparable damage to the OEM's reputation and brand. This article examines the dangers of counterfeit batteries and how designers can help protect their products from their usage.

By Robin Tichy
Robin Tichy is the technical marketing manager at Micro Power. She is responsible for technology investment to enable new portable markets. Tichy can be reached at 503-530-4901 or rtichy@micro-power.com.

The ownership period of an individual portable device often exceeds the cycle life of the original battery. This is especially true in the medical industry where product lifecycles are commonly more than ten years. In addition, portable medical devices are becoming more commonplace and models of these devices are becoming more truly mobile as healthcare providers recognize the advantages that portability offers. Intense use shortens the number of years of viability of the original battery. The high price points of medical devices in combination with the increasing volumes of portable devices opens this market for third party replacement batteries. Aftermarket vendors may resort to activities that compromise the end user experience or safety to make the battery packs inexpensive and attractive to those placing purchase orders for replacements. Both the medical original equipment manufacturer (OEM) and end user pay a price when counterfeit battery replacements are chosen. The quantifiable impact of imitation battery packs to the original equipment manufacturer includes increased safety risks for their customers, greater product returns due to non-performing batteries, reduced customer satisfaction, and reduced revenue for batteries supplied by the original manufacturer. Seemingly random battery fires are often attributed aftermarket or "fake" batteries.

When overstressed, almost any Li-ion technology can be hazardous to a degree. Extra caution must be exercised during the design process to ensure that the cells are being utilized in a manner appropriate to the technology.

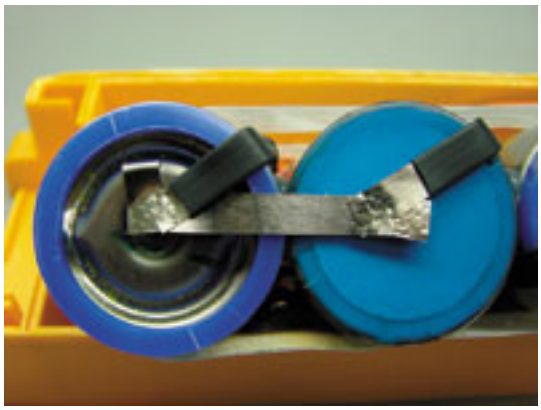
Counterfeit products can be found easily on the web for most portable products, including medical devices. In an analysis of aftermarket battery packs, compared with their counterparts from the original manufacturer, many quality issues were observed in the aftermarket medical battery packs. There is a large potential for safety hazards due to the manufacturing and design issues found. It is both surprising and troubling that more safety and performance issues were observed in

the medical products analyzed by Micro Power than any consumer battery products. This goes against intuition, but it is easily explained because these products are produced in lower volume, there is less automation, and the products are more complicated.

Battery packs are no longer a simple configuration of cells. They are carefully engineered products with many safety features. The main components of a battery pack include the cells, which are the primary energy source; the printed circuit board, which provides the intelligence for the system with features such as the fuel gauge and protection circuitry; the plastic enclosure; external contacts; and insulation. In an analysis of many aftermarket battery packs, the following issues have been identified:

- Use of substandard or unqualified cells
- Mismatched components on circuit boards that may not provide adequate performance
- Lack of a current/voltage or thermal protection circuit
- Lack of accommodation for normal cell swelling over time
- Nonexistent or obstructed gas vents
- Bad welds or solder joints

Bad welds are, by far, the most commonly observed problem and they can serve as a warning signal. Welds such as those illustrated in the image should be caught in a next step inspection process, but if they are present in a battery pack that goes out to the market, it is a strong indication that the manufacturer's quality processes are not sufficient.



The poor welds shown here are a first warning sign that the manufacturer of this battery pack does not have adequate quality controls

One way to protect the end user and to give him the best performance is to authenticate battery packs and other accessories. As healthcare consumers, it is important for designers to protect themselves against the dangers of knock-off battery packs and, as electronic design engineers, it is their responsibility to protect their company from the aftermarket packs as well. Fortunately, there are many options available to design in protection against aftermarket batteries. The most obvious is the form of the packaging and connectors, but this approach can be circumvented by simple measurements, and once a counterfeit or clone is available, the original manufacturer would have to change the form factor-a non-trivial task.

Labeling-such as stickers, certification markings, and holograms-is another possibility, but high quality, inexpensive scanners and color copiers make these methods easy to reproduce. Web-based registration is another idea, but it creates an inconvenience for the user. The design engineer's objective is to increase the pain level of an unauthorized manufacturer so that they choose not to manufacture a clone of the battery pack. An electronic challenge and response or electronic identification (ID) may be warranted for the protection of the OEM's product; the added cost of an ID-based solution may be sufficient to achieve the goal of increasing the time and expense to create counterfeits.

A simple ID approach should not be considered secure because an occiloscope measurement will give all the information needed to reproduce a static ID. If an unauthorized manufacturer is willing to add the cost to reproduce the ID, then this system fails to protect the end user or the OEM. A changing challenge and response between the battery and the device is a more secure approach. It requires a secret that is shared between the host and the battery, random input, and an algorithm for generating an output that is difficult to predict. Selection of the correct authentication technique is about understanding the tradeoffs to be made.

One strategy that an engineer could employ is the cyclical redundancy check (CRC). In this system, the challenger, which is the host, sends a command to read the ID from the responder, which is the battery or peripheral. The data returned from the device includes the product family code, ID, and CRC value. The CRC value is used to ensure that the data is transmitted completely and correctly. The host checks the validity of the data and determines how the system should react based on that validity. A more secure version of the Challenge/Response technique requires four components missing from the CRC approach:

- A secret that is shared between the host and the peripheral
- A good random input
- An algorithm for generating an output that is difficult to predict based on the input and the secret
- The algorithm should not be easily analyzed such that the secret can be determined.

The algorithm itself does not need to be a secret. In fact, a public domain algorithm, such as an SHA-1/HMAC, is preferred because it has been reviewed by a large group of people who have determined that the secret cannot be deduced from the output.

Peripherals become significantly harder to counterfeit or clone by adding randomness, secrets, and computation. However, there is a price to implement these systems correctly. They require that the host medical device have a secure memory to store a secret that is not easily accessible by external means and a good random number generator. Without a good random number challenge, the security can be defeated in much the same way as done for the simple static ID technique. Also, code must be added to perform the computation for the expected answer. It is possible to have intermediate solutions, something between an ID and a fully secure solution. Creation of unauthorized products may be discouraged by adding a

little computation complexity.

It is important that the design community not neglect the danger of counterfeit batteries. Imitation or aftermarket batteries have resulted in public relation issues for portable equipment manufacturers because these counterfeits are usually of lower quality than the original battery. While protection of business is a side effect of adding authentication, the main benefit to OEMs comes from the protection of their corporate names and reputations. The intangible qualitative impact negative effect on the device manufacturer's brand name equity cannot be underestimated.

Online

For additional information on the technologies and products discussed in this article, see *MDT* online at www.mdtmag.com or Micro Power at www.micro-power.com.

Source URL (retrieved on *07/28/2014 - 3:02am*):
http://www.mdtmag.com/articles/2008/08/powering-protection-medical-device-batteries