ELECTROCHEM
CREATING TOMORROW

The Dangers of Aftermarket Counterfeit Battery Packs

Introduction

The continuing growth of portable handheld devices has spawned a healthy selection of aftermarket battery pack suppliers. The ownership period of an individual portable device often exceeds the cycle life of the original battery. This is especially true for medical, industrial and military original equipment manufacturers (OEMs) where product life cycles can be as long as ten years or more. Both the OEM and end user pay a price when counterfeit battery replacements are chosen. The quantifiable impact of imitation battery packs to the OEM 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. The field failures of individual batteries have the potential to result in serious injuries, and we mustn't forget the importance of protecting ourselves and our customers from these failures.

In an analysis of several counterfeit batteries, Electrochem Solutions, Inc. engineers found safety violations ranging from insufficient safety circuitry to poor manufacturing quality. This paper details some of the safety issues observed in counterfeit battery packs and presents options to implement a prevention program to control the aftermarket ecosystem.

Battery Pack Components

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 were selected specifically for the particular requirements of the product, the printed circuit board, which provides the intelligence of the system with features such as the fuel gauge and protection circuitry - again designed explicitly for that product's power needs, the plastic enclosure and insulation robust enough to withstand the product's drop requirements, and external contacts designed to meet insertion needs of the product.

Safety Features

The safety features of a battery pack are outlined in great detail in standards from several sources. The most notable are the IEEE 1625 and 1725 standards for laptop and cell phone batteries, respectively. Some of the guidelines for battery systems include using:

- Quality cells from a top tier cell manufacturer
- A protection or safety circuit that provides safe electrical operation
- Quality manufacturing and good mechanical design
- Isolation of the printed circuit assembly from the cells
- Support for the release of vented gasses
- Electrical tests should be applied to every pack design including continuous charge, over-discharge, overcharge, and short-circuit tests
- Mechanical tests should be applied to every pack design include shock, vibration, thermal shock, altitude, thermal exposure, and mold stress

All packs should be designed to withstand a moderate amount of shock and vibration, but the requirements can be much greater for equipment used in the field instead of a home office. Seemingly random battery fires are often attributed to aftermarket or "fake" batteries. When overstressed, almost any Li-ion technology can be hazardous to a degree. Careful consideration must be exercised during the design process to ensure that the cells are being utilized in a manner appropriate to the intended technology.

Many packs today are certified to UL2054. It is a non-mandatory certification but is useful when the host product is required to get any of the UL certifications. Its primary focus is for the battery to fail safe even after some of its internal safety components are disarmed. This requires redundant safety features designed the pack. A counterfeit pack with an insufficient design will fail this testing. Tests include short circuit, abusive overcharge, vibration, drop/impact, forced discharge, and temperature cycle testing. A pack that passes UL2054 gives the consumer a high confidence level of the battery.

Aftermarket Ecosystem

The product life cycle of a portable device in the medical, commercial military and industrial equipment markets often exceeds the cycle life of the product's battery. In addition, portable devices are becoming more commonplace and the use models for these devices are becoming increasingly truly mobile and intense as users adjust to the advantages that portability offers. Intense use shortens the number of years of viability of the original battery. The high price points of medical, military and industrial devices, in combination with the increasing volumes of portable devices, opens these markets 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. Counterfeit products are found easily on the Internet for most portable products.

Counterfeit Battery Pack Analysis

There is a high potential for safety hazards due to the manufacturing and design issues found in the aftermarket batteries analyzed by Electrochem. It is surprising and troubling that more safety and performance issues were observed in the medical and industrial products than any consumer battery products. This goes against intuition, but is easily explained; because these products are produced in lower volume, there is less automation and the products are more complicated. In our analysis of many aftermarket battery packs, Electrochem has most often found the following issues:

- 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
- 4 bad welds or solder joints

The following images illustrate some of the poor manufacturing quality issues observed in a selection of counterfeit battery packs:

Bad welds are by far the most commonly observed problem, and they can serve as a warning signal.

Insufficient welds that are not fully on the tabs

Half-moon shape of the welds indicate that the weld process used for this battery is not optimal

Welds such as these above should be caught in a next-step inspection process. 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.

Connector design is another place where insufficient quality is often observed; this image below shows the battery terminals standing out from the enclosure.

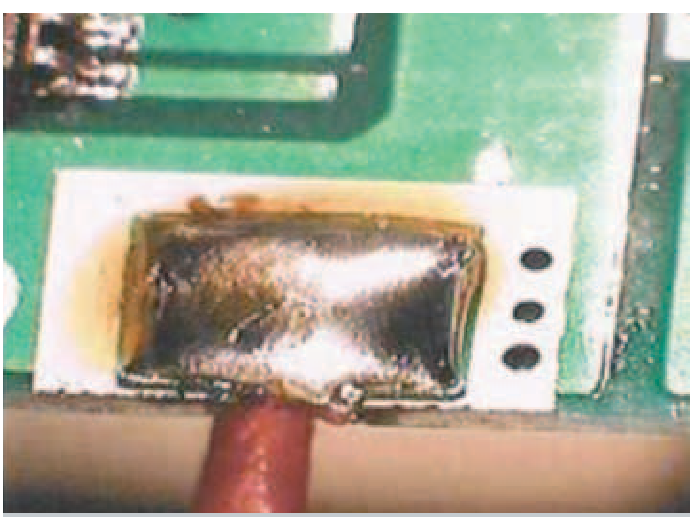
Terminals standing out from the enclosure

The contacts could also be misaligned in the enclosure housing. This could be an extremely dangerous condition as the pack could short out if placed against a conductive surface, for example a metal work top, or intermittent contact with the host device could lead to interrupted device operation.

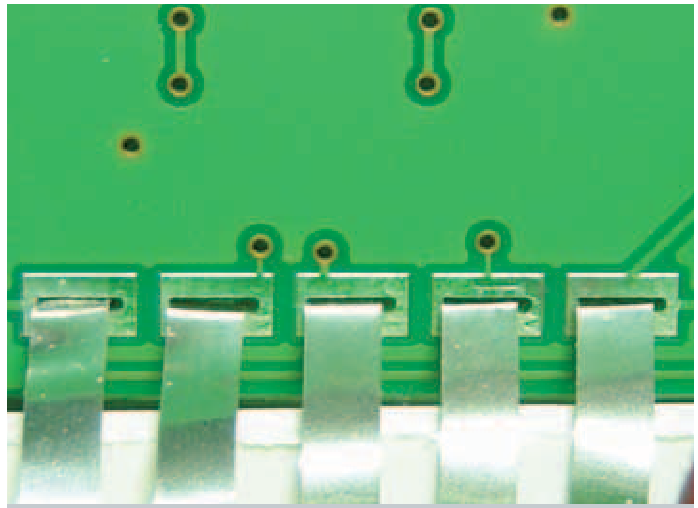
A small amount of separation should be included in the form of a polymeric shock wrap. Insulation around the cells can be damaged and expose the cells to an increased likelihood of shorting or mechanical damage. This photo below shows an aftermarket battery where the cells are not separated at all.

No insulation was used between these cells

Solder quality is another area where low quality is often observed in counterfeit battery packs. The following pictures show aftermarket batteries in which too much or too little solder was found.



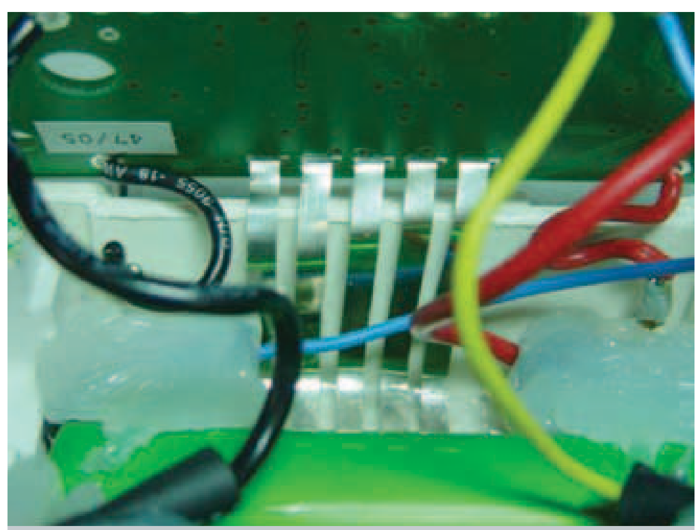
Excess flux may cause components to short



Less than 50 % solder fill

IPC requires 75% fill or better for solder. Adequate fill is especially important for lead-free solder, which has become common with ROHS legislation. It is hard to get a good connection with lead-free solder.

Any bare or loose conductor is a potential hazard, and a sharp bare piece of metal is especially troublesome. In a properly manufactured battery, the Nickel strips should be separated and insulated to prevent shorts between strips and prevent cutting the insulation on the nearby wires. In this image below, the strips in a counterfeit pack are completely bare. These strips are long and wrap around the cells, so the concern is increased that they could touch one another or cut into other insulation.



These metal strips should be insulated

Finally, this image below illustrates a very serious manufacturing issue for this rechargeable Li-ion battery pack. It is important to use silicone insulation sparingly if at all. Excess silicone can block cell vents- one of the primary safety features provided by the cell manufacturer. Trapped gas increases explosive risks. If one of the cells goes into thermal runaway, the gases could be trapped and build up pressure, creating a very serious safety issue for the user. Frame holders or foam are much better alternatives to silicone because they are more easily managed during manufacturing and will not block vent holes in the pack or cells.

Excess silicone insulation can block safety vents

Protecting Your Products

It is important to protect yourself as a consumer against the dangers of knock-off battery packs. As an electronic design engineer, it is your responsibility to protect your company from aftermarket packs, as well. One way to protect the end user and to give him or her the best performance is to authenticate battery packs and other accessories. 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 are other possibilities, but good 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. However, a simple ID approach should not be considered secure because an oscilloscope 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 trade-offs 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 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 things 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
- An 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 a SHA-1/HMAC, is preferred because it has been reviewed by a large group of people that have determined that the secret cannot be deduced from the output. This authentication strategy is the method of choice in the battery industry; it can be implemented in the fuel gauge or in a separate IC.

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 device have a secure memory to store a secret which 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 fully secure solution. Creation of unauthorized products may be discouraged by adding a little computation complexity. Fortunately, many of the latest gas gauges have SHA-1 based authentication as one of their features, so simply planning for the implementation of this feature with appropriate design on the host side is all that is necessary to implement a secure ID solution.

Conclusion

It is important that the design community does not neglect the danger of counterfeit batteries. Imitation or aftermarket batteries have resulted in public relations nightmares for portable equipment manufacturers because these counterfeits are usually of poor design standards 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 and negative effect on the device manufacturer's brand name equity cannot be underestimated since safety and performance are both compromised in the production of aftermarket battery packs.

About Electrochem Solutions, Inc.

Electrochem, founded in 1979, is a world leader in the design and manufacture of customized total power solutions. A subsidiary of Greatbatch, Inc., Electrochem was born from the lithium battery invented for the implantable pacemaker by founder, Wilson Greatbatch. Today, Electrochem is known for providing safe and reliable products which are used across a range of critical applications in the portable medical, energy, military, and environmental markets.

For additional information on Electrochem, visit **www.electrochemsolutions.com.**

About Greatbatch, Inc.

Greatbatch, Inc. (NYSE: GB) provides top-quality technologies to industries that depend on reliable, long-lasting performance through its brands - Greatbatch Medical, Electrochem and QiG Group. Greatbatch Medical develops and manufactures critical medical device technologies for the cardiac, neurology, vascular and orthopaedic markets. Electrochem designs and manufactures custom battery technologies for high-end niche applications in the portable medical, energy, military and other markets. The QiG Group empowers the design and development of new medical devices for the company's core markets.

For additional information on Greatbatch, visit **www.greatbatch.com.**