Safety First: Required Industry Practices to Enable the Widespread Adoption of Energy Storage

Greg Tremelling
Senior Manager of Electrical Design and Test Engineering
NEC Energy Solutions

Mass energy storage must be respected

As the technology of energy storage advances, it is imperative to understand primary drivers of energy storage safety. Over the years society has become accustomed to using energy storage of all kinds. Fuels for all types of transportation like gasoline or jet fuel are forms of condensed energy storage which are used only as they are needed. A hydroelectric dam is another form of energy storage. Usage of any type of concentrated energy storage must follow proper safety precautions. Battery energy storage must be respected in the same way as these other technologies, and has the potential to find its way into everyday life in the same way that gasoline, jet fuel, and hydroelectric dams have.

The handling of electrical energy storage should be as straight forward as pumping gas. Anyone of legal age can go to a gas station and fill up a car with a highly volatile and flammable liquid. By following basic and well understood safety precautions people are able to pump gas with confidence. To realize the benefits of electrical energy storage and enable successful adoption of new technologies, the industry must achieve the same level of well understood safety precautions and level of confidence.

Human Error

Despite the precautions and mechanisms which have been put in place human error will always be present and have the ability to cause damage. When used improperly, even lead acid batteries which have been around for over 100 years can cause fires, explosions, and personal injury including death. A quick search online will yield a number of photos of cars that have driven away from the gas pump with the pump nozzle still plugged into the vehicle. In most cases, the “break away” hose does its job, prevents a fire or explosion, and sometimes the drivers don’t realize what they have done until they park the car and exit the vehicle. The vehicle is not severely damaged if damaged at all and the hose repair is simple. To enable the widespread adoption of high performance energy storage, the battery energy storage industry needs to demonstrate the same type of safety and use ability features. People will make mistakes using battery energy storage and when they do, the result shall not be catastrophic.

Human error, when working with both large and small scale energy storage, must be mitigated by product, process, and system design. The battery management system (BMS) design is the key to having a safe energy storage system. Operations such as system start up, system installation, and service create opportunities for human error to cause a problem. It is for this reason that battery management systems must be designed with robust protections and redundant safety mechanisms. Not to mention that it is much more damaging and expensive to fix problems after significant failures occur[6].

Energy Storage Safety

The two primary drivers for safety in energy storage systems are the cell/module construction and the BMS system design. Overvoltage, over-discharge, thermal and short circuit conditions can lead to catastrophic failures. Understanding how these failures occur and what actions can be taken to mitigate their effects will lessen the severity of the outcome. To help identify these risks, organizations such as UL and IEC have developed standards that can be used to evaluate the cell as well as all other components of the storage system. Well defined standards such as UL1642 and IEC 62133 are used to evaluate the safety of cells. UL1973 with UL991 evaluates batteries or groups of batteries as well as their electronic controls. If the controls are trusted for primary safety protection, these controls must be evaluated to UL991 (Tests for Safety-Related Controls Employing solid-State Devices) which among other things requires a Failure Mode Effects Analysis (FMEA) of the Device Under Test (DUT) and single fault redundancy. In other words, UL must be convinced by analysis that all possible battery faults have been accounted for and the battery will not fail catastrophically when any one single component in it fails, even if the battery is suffering abusive conditions.

Battery Management Systems

The term Battery Management System (BMS) means different things to different people. In this paper BMS contains all required functions to enable the use of the energy storage while preventing damage to both the energy storage and its management system. A BMS can also provide data logging and telemetry functions as well as higher level features such as providing a user interface. At a minimum, the BMS is responsible for mitigating any conditions which may cause a battery system failure. There are a number of off the shelf components available to perform some BMS functionality; however, designing a BMS that performs all these functions well is not straightforward. The challenge in the design process is to perform the protection functions mentioned previously while creating a useable battery system. The design cannot be considered robust until it is tested to pass regulatory standards and verified in actual use case testing. The best quality BMS will perform its safety functions with a level of redundancy while offering availability, and serviceability.

Abuse tolerance of the battery cells

Within a given energy storage chemistry the differences in construction and assembly process can create vast differences in response to abusive conditions. Most oxide based chemistries evolve free oxygen as they rise in temperature which can result in a self-heating effect called “Thermal runaway”. Once thermal runaway starts, the battery cell can self-generate temperatures in excess of 300°C. Lithium Ion Phosphate (LFP) has historically garnered the reputation of being a “safer” chemistry than oxide based chemistries (such as Lithium Ion Cobalt Oxide) because the LFP types generate significantly lower temperatures in response to abuses like crush, accelerating rate calorimetry (ARC), short circuit, and heat testing[3].

It is interesting to note that through testing we now know that not all LFP cells have a benign response to these types of tests, and not all oxide based chemistries fail catastrophically. After testing multiple LFP samples, it has been observed that some will fail benignly, and others will not[4]. Data shown below in Figure 1 shows a 3.75V nominal oxide chemistry subjected to a 33A constant-current (CC) charge (a one-hour charge rate) with a constant-voltage (CV) limit of 10V[4]. The cell skin temperature peaked at less than 110°C and the failure mode was benign.

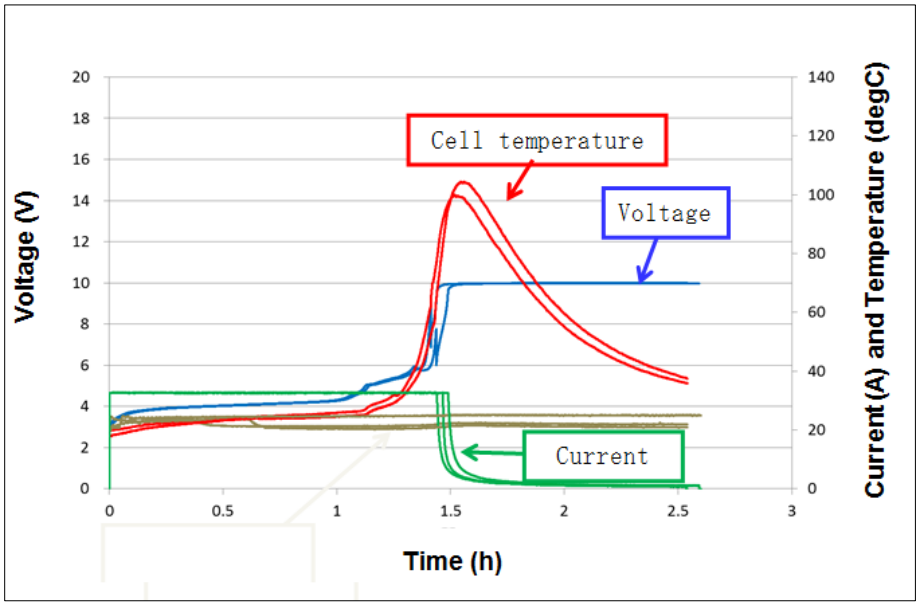

Figure 1. Overcharge testing of a select manganese oxide prismatic cell to 10V

The chart shown below in Figure 2 illustrates that an LFP battery pack when overcharged, had a more dramatic failure mode than the previously mentioned oxide chemistry. The cells underwent a minor self-disassembly process as they reached 5.25V.

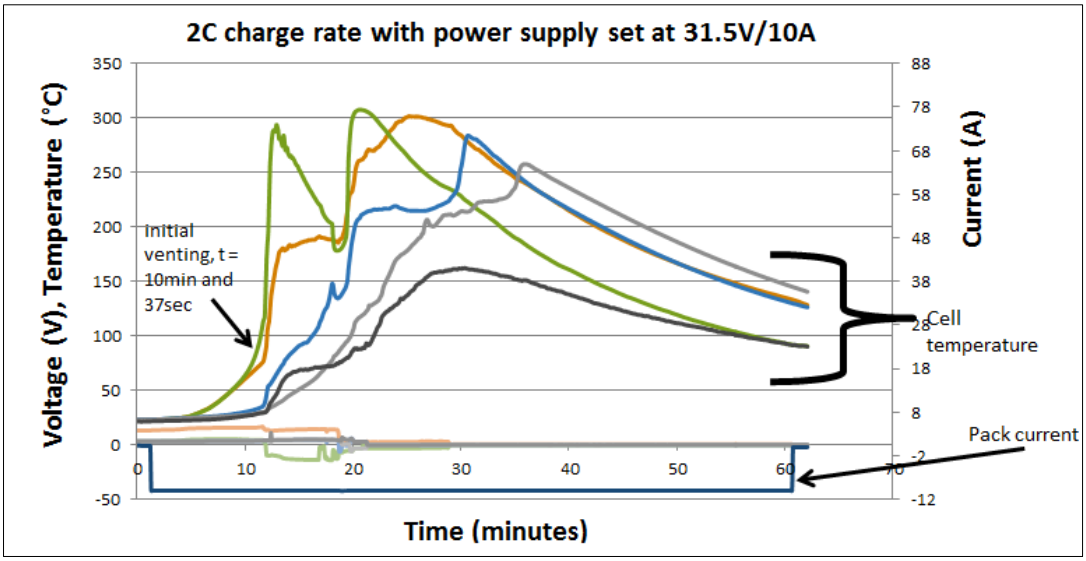

Figure 2. Iron Phosphate pack charged at 2C

These examples tend to be more of the exception and not the rule, but the points are clear. The fault characteristics of a given battery cell/module must be understood, tested, and characterized prior to designing a system around them. It is not enough to assume that just because a battery cell uses a specific chemistry that the cell is somehow more or less safe than other competing chemistries. Referencing test data at the cell level is one way to compare different cell constructions. UL certifications are public information and can inform the engineer of all the safety characteristics of the cells under consideration.

The data from these tests illustrates that the cell chemistry type alone does not make a battery cell or system "safe", and so it would be the responsibility of the BMS to prevent abusive conditions from reaching the cells or mitigating the effects of a cell failure. Cells which fail benignly are a good starting point for a safe system; however, gasses and chemicals which are typically released during overcharge events are highly undesirable. To ensure that the safety mechanisms designed into the system are both sufficient and appropriate, data from these abusive tests which validate the cell construction and design must be the starting point for any BMS design.

Battery Management Safety

Knowing how variable battery cell failure modes can be when damaged, it is no wonder UL1973 requires overcharge, short circuit, forced discharge, crush, and impact testing at the product level[1]. Because the BMS is responsible for safety critical functions it is also evaluated to UL991 where the battery or system is expected to pass these tests after a single fault has been applied anywhere in the system. Redundancy is likely required in both large scale grid systems as well as smaller commercial systems to pass this type of testing. It is all too common for suppliers of battery systems to only perform these tests on a single cell or battery if that single cell or battery is intended to be used in series and parallel. The UL file will state whether a product has been tested as a standalone "battery" or if testing has been done at a "system" level. Conditions of Acceptability (CofA) are often used by some integrators as an easy way out or a crutch to avoid the cost of thorough design and testing. Conditions of Acceptability have the potential to undermine the value of a given UL standard by subtly listing exceptions where the product design and testing may be incomplete. In addition, failure to comply with the stated conditions of acceptability invalidates the UL certification of the product.

Redundancy must not be considered optional as it will end up being the deciding factor between a returned product (RMA) and a highlight on the 5 o'clock news. Despite having a solid design, the reality of manufacturing products is that there will be some level of component failure. Even if the failure rate is low, in the .05% or less range, shipping 10K pieces means that 5 pieces are going to fail, and when they do, it shall not be catastrophic. UL has recognized this need and with UL1973/UL991 requires products to be "fail safe" in the presence of component faults. During the test process, UL generates a test plan which includes single fault conditions to components which perform critical safety functions. These critical safety functions and components are identified using an FMEA process. Components which are typically faulted include the main protection switches as well as the drives which control them. After the fault has been applied, over charge, over current and over temperature tests are performed. A product will pass if it fails safe. This means that systems which bear the UL1973 mark will be designed and tested to tolerate a single fault event anywhere in the system and maintain a "fail safe" response.

Understanding Redundancy

There is a difference between perceived redundancy and true redundancy. One example of perceived redundancy would be to have a battery management chip which claims that it has secondary over voltage protection. The lure of having this secondary protection integrated onto the same chip sounds enticing however if this chip has only one voltage sense input to serve both primary and secondary functions it may not be as redundant as we would like it to be.

Other battery management IC's can have safety gaps as well. For example a number of IC's available for battery management contain internal voltage dividers to create the hardware protection trip points. After review it will become obvious why a dedicated set of redundant sense lines may be required. If there is a bad connection (open circuit) between the battery cells and the IC, a voltage divider inside the chip may be created. In one particular example, the chip will see the average of two cells between which the midpoint sense line has been lost. One cell could be 2V and the other at 4V, and the IC would think that both cells are in the acceptable range at 3.0V. Figure 3 shows a diagram of cells connected to an exemplary battery management IC and the internal voltages which are created.

One way to mitigate this gap is to ensure that another layer of protection would not fail to recognize this situation. Having a redundant voltage sensing connection connected to an independent battery management function prevents a single bad connection from undermining the integrity of the BMS.

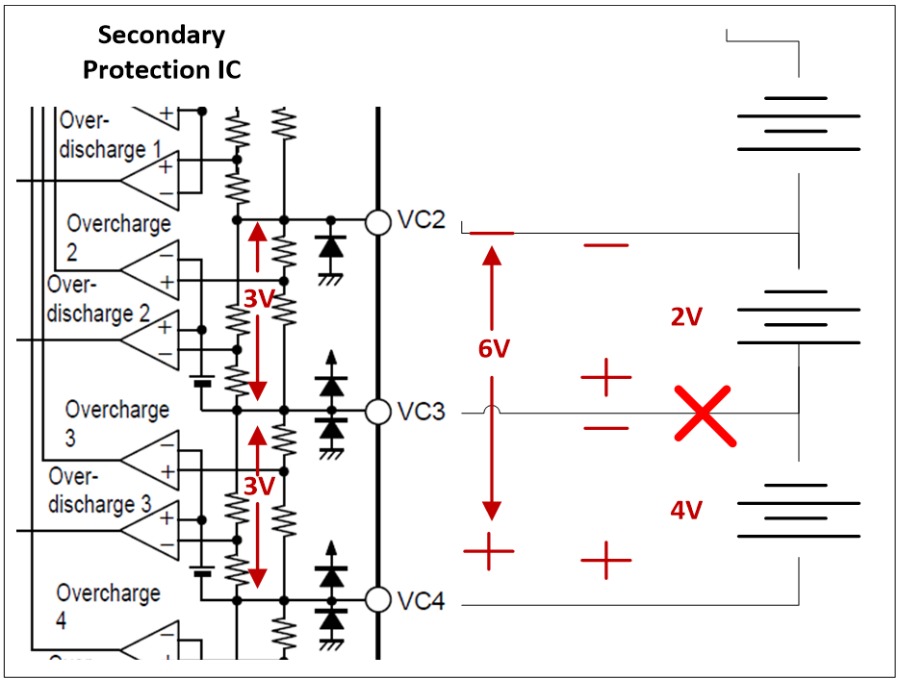

Figure 3. Broken wire/ bad connection fault case for secondary protection IC's

Large Energy Storage Systems

Safety for grid level energy storage systems requires a layered approach. Each layer of the system needs to provide an appropriate level of protection in it. Protection starts at the cell level and progresses to the battery/module, string, and container or building level and involves all aspects of design, including electrochemical, electrical, mechanical, thermodynamic and controls.

The development and design of a large system which includes an enclosure (container/building) must be able to meet a variety of requirements which are driven by safety. Specific subsystems which must be reviewed include but are not limited to heating and cooling systems, fire detection systems, electrical service equipment, emergency lighting, and electrical disconnects. Enclosures must be evaluated for load, force and tolerance needed to sustain earthquake and hurricane proof capability. As with smaller battery systems, these types of requirements drive the need to meet a variety of standards from organizations such as UL, IEC, NFPA, ASME, NEMA and others.

Mechanical integrity of battery pack design

Equally important as the electrical aspects of the management system are the mechanical interconnections of battery pack assemblies. This includes proper wire routing, cell interconnections, mechanical supports, and chassis features. A quick industry survey shows that not all battery pack integrators understand the importance of a robust mechanical design. One might find a lack of strain relief for weld straps, pinched wires between chassis parts, and overall lack of cooling considerations. Passing drop and vibration testing per the relevant safety and compliance standards may be required to manufacture and sell energy storage products and also proves that a design is mechanically robust. When procuring energy storage it is important to obtain or verify the test data which shows that a product has undergone this testing and certification.

Safe Transportation of Energy Storage

In addition to safety compliance within product design, one area that seems to be either overlooked or not well understood is that lithium ion cells and systems are considered Dangerous Goods (Hazardous Material) and must abide by international shipping and testing requirements. This class of product is required to meet certain criteria in order for them to be legally transported domestically or internationally. These requirements are based on the UN recommendations on the transport of dangerous goods model regulations. Transport of dangerous goods is regulated internationally by the International Civil Aviation Organization (ICAO) Technical Instructions, International Air Transport Association (IATA) Dangerous Goods Regulations, and the International Maritime Dangerous Goods (IMDG) Code.

In the United States, transportation of hazardous material is regulated by Title (part) 49 of the Code of Federal Regulations or CFR's. Title 49 CFR Sections 100-185 of the U.S. Hazardous Materials Regulations (HMR) contains the requirements for transporting cells and batteries. Before transportation can take place the battery cell, or battery assemblies must meet the criteria contained in the UN Recommendations on the Transport of Dangerous Goods – Manual of tests and Criteria part III subsection 38.3. Consumers must also know that in addition to being certified to ship hazardous materials, they must also ensure that the product meets the criteria of UN38.3 to legally ship product between facilities or return product for RMA

UN38.3 also requires short circuit and overcharge testing after the product has gone through altitude, thermal, vibration, and shock testing[5]. It is important to note the significance of the order of the testing. Battery packs which have insufficient mechanical support will start to come apart and fail mechanically during the vibration and shock testing. When the test sequence gets to the electrical section containing the BMS functions it will likely fail if the mechanical part of the design is insufficient. Designs with taller electrical components on the PCB with no mechanical support or poorly designed cell interconnections will not pass this testing.

Not only is UN38.3 a great test to run to demonstrate the robustness of the design, it is also required by law to ship lithium ion battery products. There are many suppliers out there who are selling and shipping products without passing these tests; and these are the products which will wind up on the news when they fall apart and fail catastrophically while in transit. The energy storage industry has to be diligent in eliminating this irresponsible behavior because it creates a bad reputation for safe high performing battery technologies. Just this week (3/3/15), there was more negative press on ABC news associated with a general description of "lithium ion batteries" due to technologies which fail poorly when tested[7].

System safety as it relates to reliable operation

Systems that are designed to be reliable will also achieve a higher level of safety. Failures like welded contactors or blown fuses are not just reliability issues because they can create opportunities for unsafe conditions. For example, welded contactors could leave high voltage present on a DC bus when it is supposedly off, and fuses that open prematurely require frequent service events which can introduce an opportunity for human error.

The impedance of the energy storage plays a direct role in how a system should be designed to prevent damage to protection components like contactors and fuses. It is not uncommon to have a high voltage (960V) string of lithium ion batteries which has an impedance of around 100milliOhms. When battery strings are first connected together a difference in voltage of as little as 15V between a battery string and the rest of the DC bus may be enough to generate a significant inrush current. On such a high voltage bus, 15V represents a mere 1.5% of the total string voltage which starts to approach the measurement error of common control electronics. If this inrush current is not controlled or accounted for, system damage may occur. Figure 4 shows how the low impedance of an exemplary lithium ion battery causes 125A to flow in response to a 28V difference between two strings. Using only two strings is not a worst case scenario because it maximizes the total impedance for a given difference in voltage. In this case the string impedance calculates to be 112 miliOhm. ($V/I=R_{total}$ and R_{total} =String 1+ String 2) Connecting a string with a 28V difference into a DC bus containing 19 strings in parallel would result in a current flow of 237A. Current = 28V/ ((112milliOhm/19 strings)+(112milliOhm)) =237A

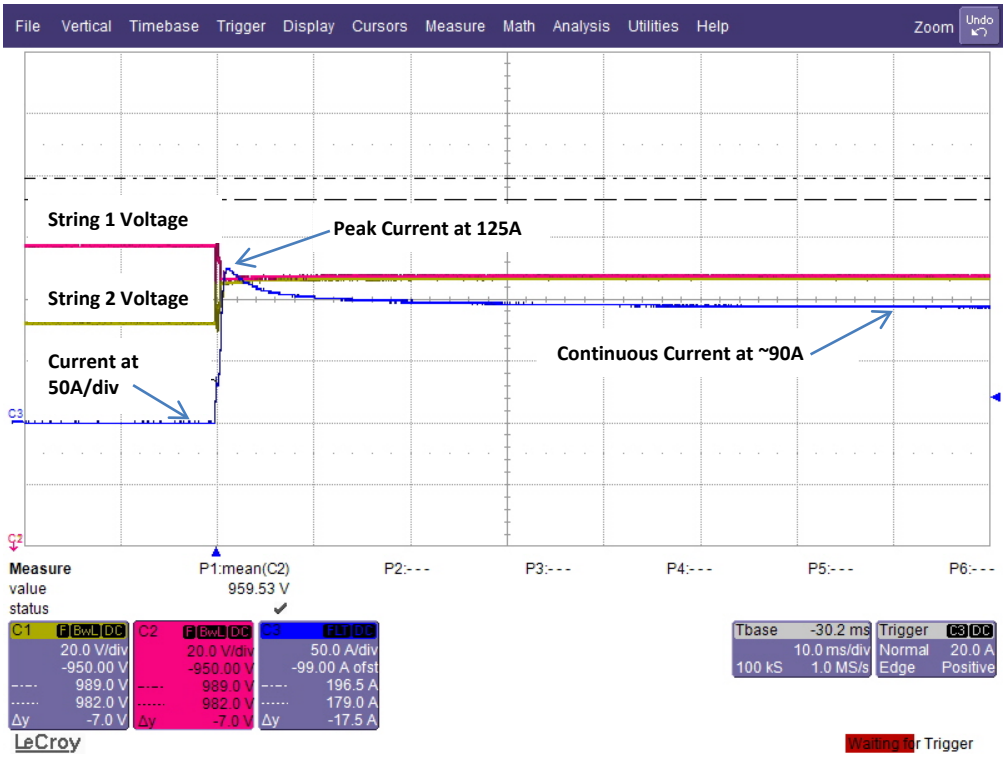

Figure 4. Change in voltage vs current for a high voltage lithium ion battery string

Equalizer Technology

Looking more closely at a system comprised of multiple battery strings in parallel, which connect through contactors to the main DC bus, will illustrate the need for a safe and reliable approach to high voltage parallel interconnection.

In such systems it is possible to isolate or remove individual strings for service or during fault conditions. If a single parallel string is taken offline it makes sense that the rest of the system would continue to operate. Taking a single parallel string offline is straightforward even under full load conditions. Here's why.

When all strings are connected to the bus (contactors closed) the difference in voltage that the contactors will see when they open is limited to the difference between the open circuit voltage (OCV) of the cells and voltage drop experienced by the string while under load (string current multiplied by the string impedance). Even if the individual string currents are 150A, opening 150A with a difference in voltage of 10-15V contains very little energy and is not a stressful event for a properly rated contactor or disconnect device.

However, reconnecting a string of batteries which has been taken offline has the potential to damage components. Assuming the system continues to operate while a parallel string has been taken offline, the DC bus voltage will transition to other levels proportional to the SOC of the system. As mentioned previously, very small differences in DC voltage can cause large inrush currents to flow. Closing the contactors with any appreciable amount of voltage across them will likely damage the system. If this is done, the system may continue to "work" for some period of time, but components will fail eventually. For example, the inrush current may exceed the rating of the string's fuses or contactors. Even brief over-current events can cause latent damage to these components, and they may fail after a limited number of these events.

One option to reconnect a string which is offline would be to require that the customer take the entire system offline, and then manually charge or discharge the system until it matches the offline string voltage. Such a manual process creates an opportunity for human error. A second option would be to leave the offline string disconnected until the DC bus happened to charge or discharge to the same level as the offline string, and then have the string opportunistically connect to the DC bus, which could take days or weeks depending on the application. Such a process could hurt the availability of the system. A third (and preferred) option would be to use an automatic equalizer design which can safely connect the string to the DC bus even while the main DC bus continues to operate. In such a system, the string level or system level control system automatically charges or discharges the offline string until it matches the DC bus, and then allows the offline string to automatically connect. This approach removes the human error element and maximizes availability.

Examples of inrush currents can be seen in lower voltage (e.g., 48V) applications as well. As stated in one exemplary battery manufacturer's operating manual, connecting parallel strings which are more than 2V different is not recommended. It also states that pressing the "on" button on the battery with the load connected could damage the fuse or the power board if an inrush occurs. Such a system allows human error to damage the product or create an unsafe condition. It would behoove the designers of these systems to implement safety features that could prevent damage from occurring from such basic product operations.

Comparing this case to the gas pump analogy could read something like this; "Failure to swipe your credit card before removing the nozzle from the pump will cause permanent irreversible damage to the pumping equipment". There is no question that it makes sense to swipe your card prior to removing the nozzle, however, it is not reasonable to accept that reversing this order of operations may cause damage to the pump. These are the types of barriers that the battery industry will need to overcome before higher performing batteries will experience widespread adoption.

Validation through testing

Once a safe design has been conceived and documented, it must be tested under as many worse-case conditions as possible. This brief paper is not the right forum to communicate a complete validation plan; however it will cover one transient over voltage case as an example. Figure 5 shows a single string disconnecting from the main DC bus while under full power charging conditions. This test case is equivalent to pressing the emergency stop button while a system is being used at full power. As shown below properly designed systems will prevent peak voltages from climbing to unacceptable levels and also prevent unwanted oscillations from occurring. In this case there was very little initial voltage spike across the main contactors because the DC bus had sufficient bus capacitance to counteract any series inductance. Because there was the only one string on the main DC bus, the picture shows that the inverter then drove the DC bus voltage to 1200V hitting its upper fault limit of the inverter which causes the inverter to clamp and shut down. All control circuits and components responded appropriately, and none were used beyond their operational limits.

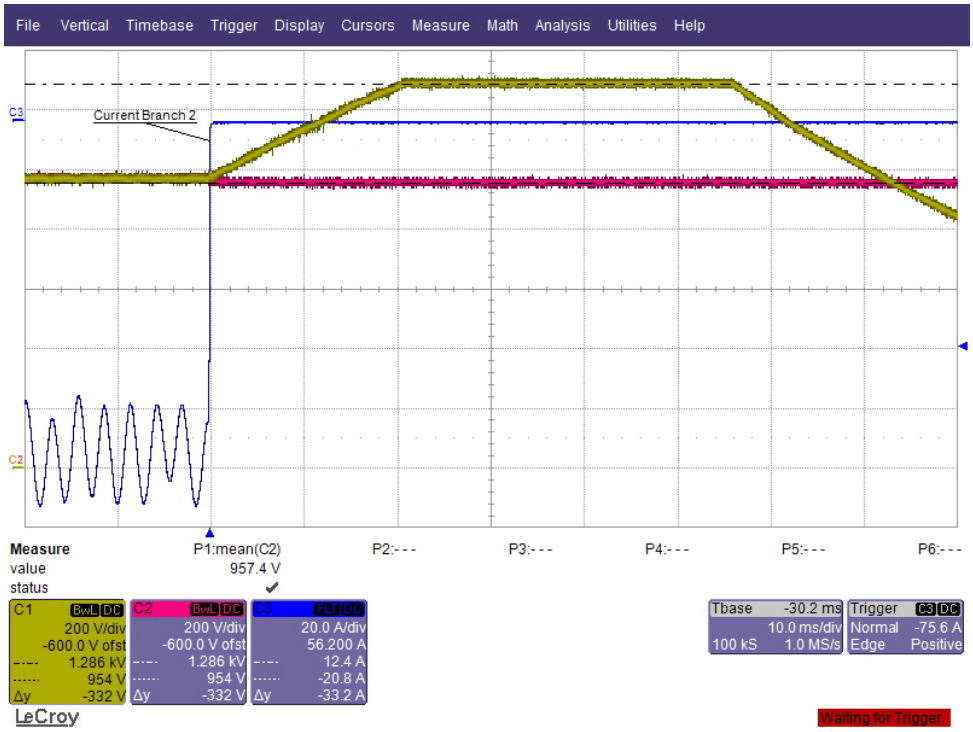

Figure 5. Voltage and Current of a high voltage rack disconnecting from the bus while under full charge power

Product design must account for the characteristics of the implementation

Unexpected damage to the BMS protections or its components cannot compromise the safety of the design. One factor which presents significant challenges to low voltage lithium ion BMS designs is the unavoidable inductance which can be found in the cables between the battery strings and the load (or inside the load itself). Inductance values vary with the types of cables used. A good rule of thumb would be to use 0.5µH per foot of cable. From $E_j=\frac{1}{2}Li^2$, an installation with a total length of 15 ft (7.5ft on the positive terminal and 7.5ft on the negative terminal) which is rated to trip an overload protection at 250A will generate a voltage surge containing 0.287 Joules of energy. This figure assumes an active clamp is in place which limits the voltage spike to 65V. The BMS design needs a method to absorb this energy safely, preferably without damaging its components and rendering the product useless.

A 12v battery placed in series with three other batteries withstanding the same 250A overload event will cause the surge energy to be much larger at 0.893 Joules. This is more than 3 times more energy for the same inductance and current value. If this energy is not absorbed it could cause the main protection switches and other components to fail. The failure mode for exceeding max die temperatures during avalanche (caused by overvoltage) events is typically observed as a “fail short” condition. Power MOSFET’s which fail short in BMS designs result in a loss of the charge or discharge protection. A safe design with short circuit protection is able to withstand over current and short circuit events when used in series and multiple parallel situations.

Not one size fits all

Similar to cell technology, there is no “one size fits all” battery management solution even within the same class of products. Comparing the optimal safety features for a central office battery bank to battery backup for communications equipment on a telephone pole illustrates an interesting contrast.

In a pole mount application, a feature called the “E-fuse” protects the battery, the connected equipment, and the user by dealing with short circuit currents so quickly that an otherwise catastrophic event becomes a non-event. A typical response time from an E-fuse protection circuit may be as little as 15 microseconds. This has many advantages including self-resetting output voltage in the presence of a fault on the output terminals.

Taking the same E-fuse feature and then applying it to the central office application has an undesirable effect. The central office wiring has many branch level circuits which are all fed by a central battery array. The branch level breakers isolate the downstream circuits in the event of a fault. This ensures that a single fault within one of the branches does not take down the entire system. If the fault current in the central office branch circuit exceeds the total short circuit capability of the battery array containing the E-fuse function, the E-fuse ends up responding much faster than the branch level breakers. If the E-fuse protection responds first, it means that the fault will now take out the entire system instead of just the branch level circuit.

In some applications this may be an acceptable trade off to gain the safety that the E-fuse offers. However in the central office application this result would be considered highly undesirable. The solution here requires that either the total E-fuse fault current is high enough to trip the branch level breaker or a more traditional fuse or breaker over current protection must be used in the central office battery system. This is just one example where the requirements of different applications have the potential to create different implementations of the same safety functions even within products which have the same capacity and voltage.

In Closing

Deploying high performance energy storage solutions which are safe is the only way the energy storage industry will be trusted enough to scale into the applications of the future. Through experience we know that safe energy storage designs start with a detailed understanding of the cell level energy storage technology, mature through product level testing, and end with 3rd party validation and certification. This testing includes the certifications required by law to transport and sell the product or system. Energy storage providers who are able to follow a robust product development process including the proper 3rd party testing will be able to avoid the costs associated with deploying systems which are unreliable or unsafe.

References

1. UL1973; Batteries for Use in Light Electric Rail (LER) Applications and Stationary Applications issue number 1 October 6 2010

2. UL991; Tests for Safety-Related Controls Employing Solid-State Devices

3. Noah Budiansky, Ph.D., Quinn Horn, Ph.D., Xiaoyun Hu, Kevin White, Ph.D., “BN64159 Comparison of Selected Lithium-Ion Battery Chemistries Testing Report” July 11, 2007

4. NEC Energy Solutions internal research. 2014

5. UN Recommendations on the Transport of Dangerous Goods – Manuel of Test and Criteria 5th revised edition. Lithium battery testing requirements – 38.3

6. Robert Swaim, Thomas Chapin, “787 Battery Investigation”

7. http://abcnews.go.com/Politics/wireStory/airlines-stop-accepting-rechargeable-battery-shipments-29345804

8. Sam Abuelsamid; “Lithium Ion Use in Transportation Markets”, February 10 2014