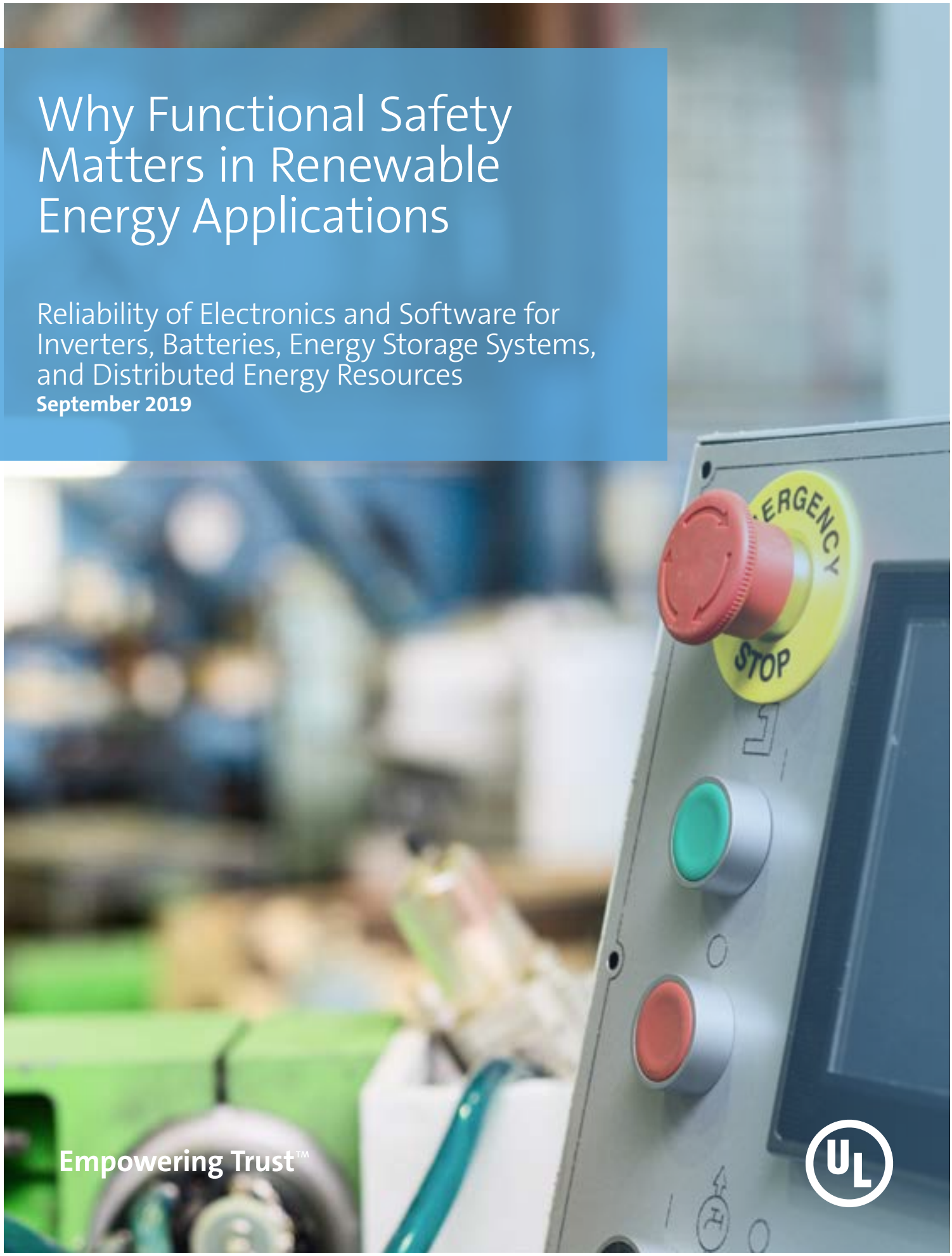
Why Functional Safety Matters in Renewable Energy Applications

Reliability of Electronics and Software for Inverters, Batteries, Energy Storage Systems, and Distributed Energy Resources

September 2019



Empowering Trust™

Authors

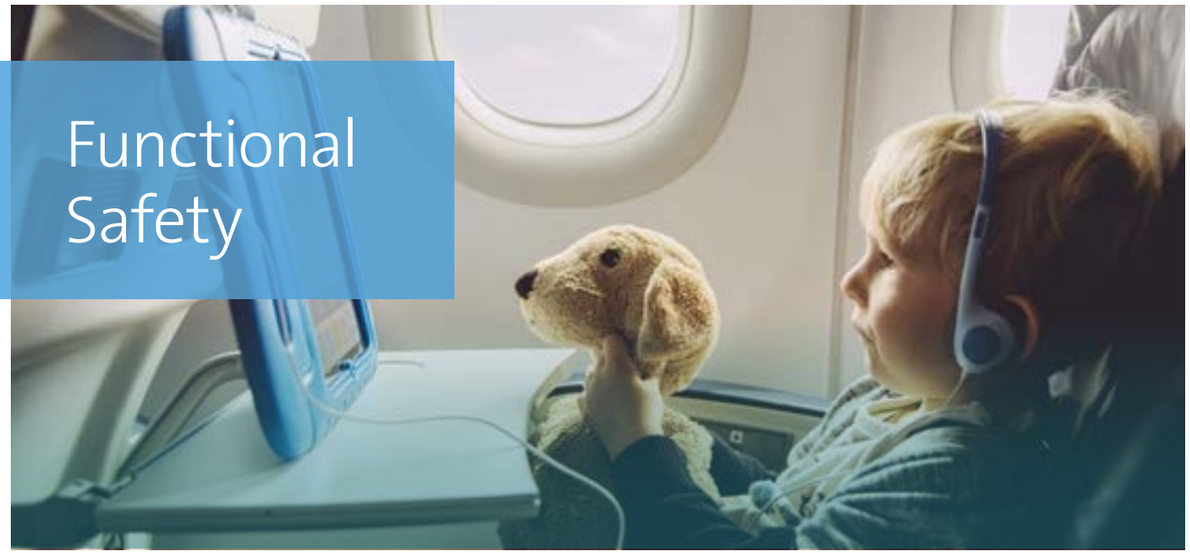
Jason Smith, Principal Engineer, UL LLC
Northbrook, IL USA

Laurie Florence, Principal Engineer, UL LLC
Northbrook, IL USA

Tim Zgonena, Principal Engineer, UL LLC
Northbrook, IL USA

Scott Picco, Business Development Manager,
Energy Systems and eMobility, UL LLC
Northbrook, IL USA

Functional Safety



We've all been there

You've purchased a children's toy with embedded electronics and it suddenly stops working. No matter what you try – turn it off and on again, replace the battery – that product won't come back to life. It's broken. "They don't make them like they used to," you might utter in disgust.

Or, you're working on an important document on your laptop computer and your computer crashes, perhaps due to a fault in the computer's hard drive or memory. You've now lost the contents of your document and also the time it took to create that document.

Now, imagine that the product with embedded electronics that suddenly stopped working was a hoverboard with a lithium-ion battery or the computer that crashed was controlling the acceleration of your automobile. The ramifications of the electronics failing in these products could be far more severe than inconvenience; your safety could be at risk.

Thankfully, these types of failures do not manifest themselves as often as a broken children's toy or a laptop crashing. One of the main reasons why is because manufacturers generally take greater care to ensure reliable, functional performance of the electronics and software in these products when there are risks relevant to safety. They do still happen, however [1] [2].

What is functional safety?

Functional safety refers to part(s) of a system that must function correctly to maintain safe operation of that overall system. Examples of functional safety include a battery management system (BMS) that monitors voltage, current, and temperature inside a lithium-ion battery, solar photovoltaic (PV) rapid shutdown devices used to ensure a PV / solar installation is off when placed into a rapid shutdown mode, and electronic throttle control (ETC) in a passenger vehicle.

Functional safety can be provided by electronics, software and other technologies, including hydraulic or mechanical. While not usually thought of as such, overcurrent and overtemperature protection devices such as fuses, thermal cut-offs (TCOs), and circuit breakers are actually functional safety devices as they ensure the safety of their overall system.

That being said, functional safety has become closely associated with electronics and software, because they are now often replacing safety devices that were based on mechanical or other technologies. With that, more attention is being paid to functional safety, since electronics and software have a reputation of sometimes failing to do what they are supposed to do.

Concerns with electronics and software

Everything will fail, eventually; it is just a matter of when and how. Even a perfectly designed product, at some point in time, will fail due to one or more parts of the product wearing out from physical stresses. The average time to failure can be estimated, and manufacturers will often plan their warranty and service periods for a product based on this estimation.

Electronic components are getting smaller, getting placed closer together, and executing tasks faster than ever, allowing manufacturers to incorporate more powerful technologies into smaller packages. This also potentially reduces the margin for error and shortens the estimated time to failure of these products.

In addition, products usually have at least one systematic flaw; an inherent part of the design of a system that does not perform or execute exactly as intended. Systematic flaws can cause every one of the same product to fail in the same way, given the same initial conditions, so manufacturers obviously want to avoid this type of flaw as much as possible.

Systematic flaws tend not to reveal themselves when initial conditions are normal. It may take a combination of conditions, such as a product getting hit by another object, getting struck by lightning, operating in hot, cold or humid conditions, operating next to a radio tower, or suddenly losing power, before a systematic flaw will cause a product to fail.

In addition, managing systematic flaws in software is challenging. Just eight bytes of a program – not kilobytes, megabytes, or gigabytes, but eight bytes; not even enough to display “Hello World!” on your computer screen – has 18,446,744,073,709,551,616 (18 quintillion) possible combinations, and a change of just one bit could completely alter the behavior of the program.

Because of this complexity, if there are software bugs, software can seem to execute erratically in a random way. The software may work correctly most of the time but may not work correctly the next time. This isn’t in fact random, but it appears so because there is virtually an infinite number of possible initial conditions (inputs, timing, environment, etc.) to consider with software.

All of this needs to be considered when designing safety-related electronics and software. Random faults, due to wear out, are inevitable and products need to be designed to help ensure that when the product does fail, it does so safely. Systematic flaws additionally need to be avoided as much as practicable to help ensure that there is no adverse impact to safety.

Mitigating random faults

As mentioned previously, everything will eventually fail due to wear out. One of the most important things to consider when designing a system for functional safety is how that system will fail when it does. The three typical manners in which a functional safety system will fail are fail-dangerous, fail-safe (shut down), and fail-operational (fault-tolerant).

Failing “dangerous,” as the name implies, is generally the situation to avoid as it increases the probability of harm. To avoid a fail-dangerous situation, additional diagnostic measures to detect faults are needed at a minimum, or sometimes a second (or even third or more) redundant way to maintain safe operation of the system is necessary.

Failing “safe,” which will turn off or shut down the system when a fault is detected, is sufficient for many basic safety-related applications. Failing safe requires additional diagnostic measures implemented in the system to detect faults. An example of a diagnostic measure would be a separate thread in software to check Flash memory in a processor for faults.

But sometimes just shutting down isn’t appropriate. In automotive or avionics applications, for example, suddenly turning off the method of propulsion if a fault is detected could cause more harm than good. In these cases, a fail-operational system may be needed, which will keep the system running safely, at least on a

temporary basis, even in the case of one or more faults.

A fail-operational system requires at least one if not more redundant backup systems in place in case the primary system fails. Because it effectively doubles (or more) the number of components in the system, designing fail-operational systems tends to be more expensive, but the amount of risk to safety in these types of applications warrants the additional expense.

Avoiding systematic flaws

Because of the aforementioned complexity of electronics and software, systematic flaws are nearly impossible to avoid. In fact, some of the most significant failures of electronics and software in history have been systematic in nature. To reduce the likelihood of a systematic flaw, care needs to be taken in the planning, implementing, and testing of a functional safety system.

Following a defined and documented process to develop a functional safety system is essential to avoid systematic flaws. Some may see it as nothing more than red tape, but it forces the developer to think out and put their design down on paper, giving others the opportunity to review and approve the design before it is actually implemented.

Documenting a design makes clear the objectives of each unit in a system, which allows the system to be thoroughly tested. This is particularly important for software, which must be tested at the smallest unit levels to help ensure that all code branches, even those (and especially those) less likely to be taken, execute as intended.

In addition, functional safety systems need to be tested under abnormal conditions to help ensure they will react safely. Testing for immunity to electromagnetic interference – voltage surges or dips, electrostatic discharge, radio frequencies, etc. – and variations in environmental conditions – temperature, humidity, etc. – are essential in proving a system has been designed correctly and will continue to operate safely in the presence of these abnormal conditions and environmental stresses.

This well thought-out approach is especially needed when designing a system to deal with inevitable failures. Functional safety systems that should have been designed to be either or both fail-safe and/or fail-operational sometimes turn out to be neither. The ramifications of this, as in the Boeing 737 MAX MCAS example, could unfortunately lead to significant harm [3].

Safety certification

UL certifies thousands and thousands of different kinds of products for safety, including those that incorporate electronics and software. Each kind of product has its own standard that describes that product's essential safety requirements (fire hazards, electrical hazards, mechanical hazards, etc.) and required testing needed to certify the product and therefore bear the UL Mark. The product standard may additionally reference other standards as well where the same process and requirements are applicable to that end product.

When a component of a product is relied upon for safety, that part or component has to meet additional requirements and tests in its component standard before it is incorporated into a product. Depending on the specific component and end-product application, it isn't good enough to just test that component in the end-product standard, as the end-product

standard does not cover all concerns particular to all its components.

Fuses evaluated to the UL 248 series of standards for Safety Low-Voltage Fuses, for example, undergo an evaluation of the fuse construction and a test program that verifies the fuse performs its function correctly and reliably according to its type and rating. Fuses, however, are relatively simple components; applying the same requirements to electronics and software would be inappropriate.

Functional safety standards, such as UL 991, the standard for Safety-Related Controls Employing Solid-State Devices and UL 1998, the standard for Software in Programmable Components, contain requirements to help ensure that electronics and software have appropriate diagnostic measures and/or redundancies in place, have an appropriate level of immunity to electromagnetic interference and environmental conditions, and have been developed using robust design, implementation and testing processes.

In some limited cases, it is permissible to evaluate electronics and software as a black box – that is, only taking end-product standard requirements into consideration and ignoring any functional safety requirements. This provides little to no assurance that the product will operate safely after that product leaves the production line or when it fails. Further, in the case of software, the revision cycle is often quite frequent, if not continuous, and as such this black box approach has extremely limited longevity due to the pace of software changes and updates. Unfortunately, it has been observed that several National Recognized Testing Labs (NRTLs) have inappropriately expanded the black box approach to functional safety in general for all devices. This is not permitted across the board, and if allowed is clearly marked in the specific end-product standard where the black box approach is allowed.

Functional safety concerns with smart grid support and utility interactive inverters, PV/ solar system equipment, and distributive energy resources (DER) devices

Modern utility interactive inverters embody and orchestrate power conversion, high-speed computing, real-time power metering and analysis, communications, and input and output circuit control while simultaneously acting as a PV system safety watchdog preventing a variety of shock, fire and energy related hazards. Having microprocessors and electronic monitoring, DER devices and inverters used in distributed generation (DG) applications have always been relied upon to perform system protection functions, which have increased system reliability and reduced cost. The PV and DER industries are excellent examples of a growing dependency on inverter functionality over the years and so has the list of responsibilities performed by PV inverters. The inverter has become the brain of the PV/DER system and software has become its most critical component.

Inverters are being relied upon for an ever-increasing list of protection and performance functions for the entire PV and microgrid system. The National Electrical Code (NEC) requires that equipment shall be listed to the applicable safety standard for the functions they perform. The recent changes to the NEC as well as product safety standards and grid codes for grid interactive and support functionality will directly impact inverter certifications. Understanding these standards and codes is critical to using proper equipment designed, built, certified, and installed correctly for the application.

Areas where functional safety is applicable in this industry include but are not limited to:

- Overcurrent protection and Power Control System (PCS) current monitoring and limiting functionality (2020 NEC)
- PV system protection: Ground Faults, Arc faults, PV Rapid Shutdown equipment and systems including PV Hazard Control in the future UL 3741 Standard
- AC modules, AC module systems and PV module mounted electronics for smart junction box applications.
- Use in energy storage systems (ESS) and in coordination with battery management systems (BMS) equipment.

Standards in this area that require functional safety are:

UL Standard	UL Standard Title
UL 1741	Standard for Inverters, Converters, Controllers and Interconnection System Equipment for Use With Distributed Energy Resources
UL 62109	Standard for Safety of power converters for use in photovoltaic power systems
UL 3741	Standard for Safety Photovoltaic Hazard Control
UL 1699B	Standard for Photovoltaic (PV) DC Arc-Fault Circuit Protection
UL 2231 (via UL 2202 references)	Standard for Safety for Personnel Protection Systems for Electric Vehicle (EV) Supply Circuits: Particular Requirements for Protection Devices for Use in Charging Systems
UL 2200	Standard for Stationary Engine Generator Assemblies

Inverters will be key participants in micro grids and multimode (utility interactive + standalone) applications. Hardware, firmware and software reliability including, internet connectivity, communications, remote revisions and cybersecurity will be a key consideration in maintaining safe and reliable DER systems

Programmable electronics have become a common foundation for power generation, control and protection electronics for distributed generation and renewable energy sources. The growth and expansion of programable electronics continue to replace individual discrete electronic control and protection components. The transition to programmable electronics is also allowing for a combination and consolidation of overall functionality. This consolidation and reduction of discrete protection devices drastically increases the importance of the programable electronics reliability and further illustrates the importance of a functional safety investigation.

Luckily this industry was able to take advantage of existing published functional safety standards that clearly define a path to evaluate the functionality and reliability of electronic controls and programmable electronics. The predominant functional safety standards used in this industry are:

UL Standard	UL Standard Title
UL 60730	Standard for Safety of Automatic Electrical Controls
UL 1998	Standard for Software in Programmable Components
UL 991	Standard for Safety Tests for Safety-Related Controls Employing Solid-State Devices

All U.S./UL renewable energy and distributed generation safety Standards specifically require that safety critical electronic controls, software, and/or programable electronic features and functions be evaluated and found compliant with these functional safety Standards. It is crucial that these renewable energy and DER products and systems are evaluated thoroughly and completely using all of the applicable requirements in the applicable standards.

Severity of a failure mode (electric shock, energy hazard and/or fire) resulting from the loss of a protection circuit is the primary driver of the functional safety based requirements published in these renewable energy and distributed generation standards. The environmental stress and electrical reliability testing to "stress test" these critical software/hardware functions is imperative to maintaining reliability and safety. Failure Mode Effect Analysis (FMEA) help ensure that in addition to the stress tests, these circuits are single fault tolerant safe. Without the functional safety investigation the reliability of the device and/or systems to function safely can be compromised.

Functional safety concerns in battery storage and energy storage systems: small and large scale

Energy storage systems relying on battery storage use electronics and software for safety monitoring and critical safety controls within the system. For example lithium-ion batteries need to be operated within their safe operating regions for charge and discharge. The parameters of current, voltage and temperature during operation should not fall outside of the battery's operating region for charging and discharging as defined by the lithium-ion battery manufacturer, or the batteries can potentially pose serious safety hazards.

This is especially true for the charging voltage limits, which are temperature dependent and must be strictly controlled. This level of control cannot be accomplished without the battery management system (BMS), which is essentially a programmable electronic control board(s) that monitors and controls the battery system's operation. Since the BMS is critical to the battery energy storage system's safe operation, it is imperative that it be evaluated for reliability via a functional safety investigation to a level critical for safety as determined by a thorough analysis of the BMS and battery. The BMS should operate to protect the battery as intended over the life of the battery, and be able to reliably operate within the anticipated environmental stresses it will be exposed to. There should be sufficient redundancy built into the BMS to ensure reliability of its operation to maintain the system in a safe state.

To help ensure that the battery energy storage system controls function as intended and have a level of reliability over the life of the system, it is critical that the BMS undergoes a functional safety investigation. This investigation should be based upon a thorough safety analysis such as a Failure Modes and Effects Analysis (FMEA) where electronic components and software critical to safety are identified for evaluation in accordance with appropriate functional safety standards. This evaluation should include redundancy of critical safety functions, consideration of environmental impact including electromagnetic compatibility EMC stresses, temperature exposure and others that could impact the operation of the battery system and its safety controls.

Standards in this area that require functional safety are:

UL Standard	UL Standard Title
UL 1973	Standard for Batteries for Use in Stationary, Vehicle Auxiliary Power and Light Electric Rail (LER) Applications
UL 9540	Standard for Energy Storage Systems and Equipment
UL 2271	Standard for Batteries for Use In Light Electric Vehicle (LEV) Applications
UL 2580	Batteries for Use In Electric Vehicles
UL 2849	Standard for Electric Bicycles, Electrically Power Assisted Cycles (EPAC Bicycles), Electric Scooters, and Electric Motorcycles
UL 2272	UL 2272 Standard for Electrical Systems for Personal E-Mobility Devices

There can be no shortcuts taken when conducting a safety analysis of the system and a sufficient understanding of the safety needs of the system along with the capability of those controls responsible for maintaining that safety is critical to preventing hazardous events in the field. Insufficient safety controls in a battery energy storage system can lead to hazardous events occurring including fires and potential explosions from lithium-ion cells driven into thermal runaway and cascading throughout the battery system. In short there is not black box approach allowed in the case of functional safety of batteries.

For example, charging a lithium-ion battery cell as little as a volt over its charging voltage limit can result in overheating of the cell and a potential for a thermal runaway event. The BMS, continuously monitoring cell parameters such as temperature and voltage can react when these values are reaching limits to lower or stop charging and discharging of the battery to prevent hazards. A functional safety evaluation of the BMS is an important step in helping ensure that the BMS, a critical safety component of the battery energy storage system, is operating as intended to maintain the system in a safe state.

In more complex battery energy storage systems where there may be an additional energy management system (EMS) controlling multiple battery systems and BMSs and other components affecting the overall safety of the system, this same safety analysis conducted on the BMS extends to the EMS. Similar to the BMS, an EMS consists of programmable electronic control board(s) to help ensure that all parts of the battery energy storage system work together to avoid out of specification conditions that could lead to a hazardous outcome. The amount of energy contained within a large battery energy storage system with multiple battery systems can be considerable. Fires within one battery system can cascade throughout the battery energy storage systems resulting in a significant fire event. The initial fire event can further spread resulting in hazardous off gassing of flammable

gases and potential explosions presenting a real threat of fire and explosion hazards to buildings and surrounding areas.

The EMS analysis needs to consider any components and software impacting safety and needs to take into consideration the reliability of communication systems that may be relied upon as part of the system safety scheme. Without these controls reliably monitoring and helping ensure safe operation of the battery energy storage system, the system cannot react in a reliable manner to stresses that can occur during operation. A safety analysis and a functional safety investigation of the battery energy storage system safety controls is a critical step in helping ensure that even a large complex battery energy storage system will operate safely throughout its intended life.

Functional safety is critical to the safe operation of a battery energy storage system. Not conducting a rigorous safety analysis followed with an appropriate level of functional safety evaluation and testing on a battery energy storage system results in a significant increase in substantial fire and electric shock risks of the equipment and to service persons, users, and people located in the vicinity of the battery or ESS, e.g., buildings where these devices are located. This can result in serious damage to property and injury to those unfortunate to be in the area of a battery energy storage system when it goes into failure as a result of out of control conditions.

To connect with an expert about functional safety in renewable energy applications contact ***renewableenergyquote@ul.com***.

References

[1] https://www.cpsc.gov/Safety-Education/Safety-Education-Centers/hoverboards

[2] https://www.eetimes.com/document.asp?doc_id=1323061

[3] https://www.seattletimes.com/business/boeing-aerospace/a-lack-of-redundancies-on-737-max-system-has-baffled-even-those-who-worked-on-the-jet/

UL.com

210.01.1019.EN.EPT