TECHNIQUE FOR DATA RETENTION AND RESTORATION FOR SYSTEMS MONITORING BATTERIES AT REMOTE SITES

Chris Belcher
Technical Solutions Leader
NDSL, Inc.
Raleigh, NC

Duncan Brown
Senior Software Developer
NDSL, Inc.
Raleigh, NC

Abstract

Monitoring systems are widely deployed as a maintenance practice by many industries today including, but not limited to, data centers, telecommunications, rail, and power utilities. Maintaining and managing the data collected by each of these automated monitoring systems can be challenging, especially as operators deploy hundreds of monitoring systems across widely dispersed locations. While there are various practices for data sampling frequency and reporting intervals, it is critical to not overlook the backup and data restoration elements for their monitoring systems. Without proper backup of critical information, such as baselining records, system configuration, reports, historical records, and fault history, it would be extremely difficult to restore a system back to its original state following a product failure of the monitoring system or a catastrophic event. This paper will explore which records need to be maintained and propose a best practice for record keeping and restoration management in support of electronic monitoring of battery systems. While the practices can be applied across multiple industries, this paper will highlight the best practices for remotely distributed systems such as those found in power utilities. Where it is beneficial, application will be made for co-located large deployments such as data center environments.

Introduction

The authors support the position that the only 100% reliable way to determine if a battery will properly perform is to conduct a capacity test. However, this is not only challenging to perform, but also unadvisable to perform frequently and can be costly. Based on over 25 years of working with customers who monitor their batteries using affixed electronic monitoring systems, the authors strongly believe that valuable information can be collected from the battery system which can reduce the risk of dropping the load. Also, the use of a battery monitoring system can capture discharge events which if recent and of sufficient duration, can safely extend the time between capacity tests.

Battery Monitoring Systems collect information on a regular basis for analysis. Often this information can be used for historical trending and in some cases identification of an impending issue within the battery system and operating parameters. Information such as individual cell/container float voltage, discharge voltage, ohmic value, temperature, string voltage, current, ambient temperature, ac ripple, and other measurement points are collected at regular intervals. Some data points may be updated continuously, while others may be recorded as infrequently as once per day or less. Data is often used for analyzing performance information of the overall battery and each string. The availability of historical data is largely dependent upon the monitoring system selected and its capabilities. Some systems can simply provide real-time information, leaving all historical analysis to another device or system, such as a data historian, while others may maintain detailed logs and historic data for the entire life of the battery system.

By engaging in hundreds of battery deployments per year, the authors have aided many customers in post-mortem failure analysis of their batteries. These failures are often a result of neglecting the data reported from the monitoring systems (Belcher 2015). Unfortunately, a common occurrence is the lack of data backup procedures or processes to maintain useful information about battery history. Often this oversight is not identified by the user until after a power loss event. It is only then that the user realizes their battery data has been lost and they have no contingency plan in place for a failure. This paper will highlight the importance of maintaining up-to-date backups of the historical information from the automated monitoring system, what data to protect, and the importance of having a system restoration process for your battery monitoring system. Some recommended practices for backing up the data will be proposed, as well as options for how to maintain the data, the format for backups, and the type of information that should be maintained. Backup methods may vary depending on the criticality of the site and the nature of any regulations that may be enforced. Data retention requirements may not be the same for all industries, however an adequate backup practice should be utilized for all industries.

The criticality of the system data will depend on the application and how much of the data is maintained long-term within the system. To best determine the criticality of the data, we encourage users to ask several questions. For example:

- What happens if the historical data is compromised?
- What are the impacts to the business if historical data is lost?
- Is there a paper trail or sufficient data backup in place to make decisions should the system be compromised?
- Are there potential fines or financial implications for not maintaining that information?

The reliance on monitoring systems is increasing as the value of the assets they are protecting continue to increase in importance. It is also recognized that these systems reduce the need for periodic site visits, as many manually measured parameters can now be automatically measured and documented, as well as the "invasive testing of components by on-site technicians" (NERC (Sup. Ref) 2015, p26). As previously mentioned, these systems actively and automatically collect information about environment, performance, and stresses/stimulus applied to the battery. Even if only used to monitor real-time conditions for immediate alarm notification, a battery monitoring system can provide significant value to any team responsible for UPS battery assets or distributed network of DC battery systems. Immediate alarm notification holds only a fraction of the value attainable from the system when fully utilized. By capturing the complete recorded history of metrics and alarms created by the system, performance and state of health data is available for analysis, regulatory compliance reports can be generated, and data driven planning for battery asset management and replacements can be implemented.

By examining battery measurement data, often performance issues can be identified before failures become substantial. This analysis can be conducted using software routines or by visually examining the measurements for alarming variations in readings. Graphical representations aide in quickly distinguishing outliers and determining trends in data. Areas of particular interest include ohmic value trending, voltage variation, and discharge performance. By examining data, the engineering team can assess which battery strings are most vulnerable and therefore can prioritize the battery replacement budget to address the most at risk batteries with the highest priority. Lastly, some operators are subject to either internal performance assessments or regulatory review. Where applicable, the battery data can be used to demonstrate battery performance and performance oversight at whatever cadence has been established. However, this analysis is available only when historical data is properly maintained and stored.

Local Versus Centralized Data Retention

There are differing implementation strategies regarding local information storage, or information stored at the on-site battery monitoring system. One option is to have no local data retention, just real-time measurements. This option requires the SCADA or similar network-based historian to poll information continuously. Should the network connection or communications fail, information during the outage is lost and can never be recovered. Another challenge is the network bandwidth utilization can be stressed. Usually polling techniques are required and a round-robin scheme of similar method is often used to avoid network conflicts.

Some systems provide the option to locally store data for a short timeframe, for instance up to 48 hours, which is largely limited by the size of the system storage and the number of data points. This allows for momentary loss of communications between the device and the historian controller. However, any analysis conducted at the local site requires access to the centralized database. This means the user at the local site must have authorization to access the centralized database through the network.

A third option is to retain all information locally in addition to making the data available to the historian. This ensures any communications loss can be managed, since the database can be mirrored or synchronized, and provides other benefits for local data analysis, especially for isolated systems.

Risk of data loss exists for all systems, though some are more vulnerable than others. Systems that do not retain information locally or that only retain information for short periods are prone to a risk of important data loss largely due to factors beyond the reliability of the monitoring system. Statistically, this might not appear to be a significant risk. However, systems that do not retain the information locally are vulnerable to all network outages, which will create gaps in data. These outages could occur due to natural disasters, faulty communications connections, failing electronics, and equipment taken offline for maintenance. Cisco states in their product training literature that even in networks that have dual redundancy for major components, the network reliability could be as low as 99.5% ((Network Reliability Series: Introduction to Network Redundancy 2014)). While there is often redundancy in sections of the network, there is often less protection in wide area networks, especially in rural areas. Total network downtime in areas like the United States on average is generally quite low. Downtime could be as short as a couple of seconds to several days depending on the availability of the replacement equipment. However, in remote locations or in less developed countries, outages may be more frequent due to unavailability of the power grid. While downtimes may be quite low for individual sites, when managing widely dispersed networks the downtime costs per outage can be quite large. If a piece of network equipment fails on the remote end of the network, it can sometimes take days to recover.

Synchronization and Security

When systems retain data locally, it is important to date and time stamp the data, since data synchronization relies heavily on proper data date and time identification. Often this involves having a master time controller that all devices use to synchronize the system clock. This is similar to the National Time Servers IT networks and other devices used to synchronize their system clocks. With standardized time stamps, if communications are lost, any information that has been recorded locally can be resynchronized with the centralized backup system. Only by having a substantially large local history storage can a network operator be assured that all information is retained locally and can be fully synchronized into a centralized database. The authors are aware of sites that were down for more than a week due to network failures, i.e. outages or simple communication failures due to changes to local network settings. With the proper combination of adequate storage and effective data synchronization, all information recorded during a communications outage, such as those described, can still be retrieved.

In addition to maintaining continuity of data, local data storage is also helpful for on-site evaluation, troubleshooting, or maintenance operations. If the data is available locally there is no need to connect to remote servers during on-site analysis. Therefore, a servicing technician can analyze any alarm conditions and fully assess the health of the battery even if the technician is unable to connect to the network.

Security must also be considered for remote data backup. Some backup methods require uninhibited network communications between devices, such as what may be found on internal networks. Other systems may require communication through outside, unsecure, servers using internet connections, firewalls, and port mapping. In many cases this can be overcome by utilizing secure communications between devices (HTTPS protocols) or secure VPN connections. In addition to monitoring inbound traffic, some network operators have significant concerns about external communications from their network. In situations where no inbound communications are allowed, we suggest a solution using only egress or outbound-only communications. With this solution data is pushed out to the corresponding secure centralized database by way of their internally approved servers and network scanners.

It should be noted that the more critical the data the more important a handling and protection system becomes. As a best practice all data should be protected at least as frequently the analytical record period. This is the minimum measurement frequency required to detect failures and to understand trends.

Local Data Backup and System Restoration

If local data is retained on the battery monitoring system, it is important to consider a backup and restoration process. A comma-separated file (csv) is a common export format for some data stores that could be considered for basic backups. While the data will likely be stored on the centralized historian, even if in a simple csv file, the data is not likely to be in a format that would allow for a restoration should the system need to be rebuilt.

The restoration process can be valuable even if there is no local data storage. In those instances, the system configuration and alarm setting can be quickly reestablished, minimizing system downtime. This can be important for regulatory requirements that require in some instances a response and initiation of corrective action time within 24 hours. Systems do not typically need to be restored often, but when they do, having the following settings makes the process much faster and more accurate:

- System configuration
- Baseline information
- Alarm settings
- The data history (if available)
- The alarm history (if available)

Ideally, a centralized system would also support automated software backups, thus allowing for remote site software updates with little to no user interaction.

Mirroring of Local and Centralized Data

As noted previously, there is a great deal of value in having a local record store at the remote site where the battery and monitoring system is located. Keeping the centralized master backup record up to date and accurate in the past has been challenging. However, with the development of modern software tools, database synchronization is prolific and can be achieved without any human interaction. One common method for synchronization is “master-master”, where data from either the local site or the centralized site is propagated to

the other database. This often requires both read and write capabilities for the database stores but ensures very little to no downtime should one system go down.
Secondly, a method called "master-subordinate" can be used, which is ideal for the remote battery application since all records from the local site need to be mirrored in a central location. In this solution data is replicated from the master location (remote site) and pushed to the subordinate location (centralized server) regularly, often at a set time during low-activity hours. A high-performance solution is capable of synchronizing hundreds or even thousands of remote battery systems into an integrated database. Rather than attempting to synchronize the databases on a schedule-timed interval, the authors promote a solution based on the following criteria:

- Events (alarms or conditions) as soon as they occur
- Updates to historic data (measured parameters) once per day
- Updates occur based on a random schedule such as system start time

The start times of the system are not totally random since most systems are started during the daytime. However, there is enough variability in the starting of systems across a network that it is likely only a few systems may update at the same time. Randomization between the synchronization schedule of the systems reduces network load and system load on the centralized database. A good design should allow for queuing and synchronization retries just in case the network is slow or potentially unavailable.

What Data Should Be Maintained in a Centralized Backup?

To fully understand the battery's performance, the following parameters should be retained for the life of the battery.

- Historic measurements for all parameters
- Full alarm history
- Configuration including alarm setting record

Historic Measurements

Utilizing measurement data allows an analyst to evaluate battery performance, generate reports, and determine battery health. Daily data is preferable, at a minimum, to allow the analyst to evaluate changes in battery performance. This level of resolution is even more critical as batteries age and their risk of failure increases.

Alarms

By reporting alarms immediately, any severe failures can be reported, and action can be initiated. NERC PRC 005-6 Table 2 requires this information be reported within 24 hours of the occurrence, so the data cannot be delayed and needs to be reported promptly after the event occurs.

Configuration

The configuration information is not necessary for most analysis situations but can be valuable if the system needs to be restored in the future. Therefore, this information only needs to be updated when the configuration or alarm settings change.

Data History

History of all reported parameters will be valuable but does not need to be reported or stored any more frequently than daily. For long-term trending and battery analysis daily information is more than adequate to provide the precision required. Often, this historical data will be analyzed once an alarm event is detected.

Alarm History

Alarm history should be retained when each alarm is reported, as this allows analysts to review events that may have occurred since the last maintenance visit or report period. By having local alarm storage, all alarms that occur will be recorded and are not lost, even if there are communications issues. Some monitoring systems do not maintain historical records of alarm history, such as start and stop times. If the long-term alarm history is not recorded locally and stored for future analysis, the historian could retrieve this information daily.

Data Retention

There are many drivers influencing the extent to which a user should maintain their data. These drivers include: analysis requirements, reporting intervals, and retention of evidence for regulators. In addition, since historical baseline data is one of the most important measurements that should be recorded for any battery system, that needs to be considered. At a minimum, the Evidence Retention (Section C1.2) of NERC PRC-005-6 states:

> "…Provider shall keep its current dated Protection System Maintenance Program, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System…" (NERC 2015).

Further discussion on the retention policy outlined in the Supplementary Reference (Section 8.2.1) indicated that the suggested data retention period would include:

> "All activities since previous audit (assuming a 6-year audit cycle) or most recent performance (assuming 3 year audit cycle), whichever is longer" (NERC (Sup. Ref) 2015).

Based on the authors' understanding and the stated intent of the Supplementary Reference, the intent of the retention period is for the operator's protection and to help demonstrate compliance. The automated monitoring system provides information regarding the condition of the DC Station Battery, and since the device is continuously monitored, an extended time interval of maintenance for certain battery parameters is permissible. Since Vented Lead Acid (VLA) batteries often have a life of 10 to 20 years, the authors believe it is important to consider battery data retention for the entire life of the battery and not simply based on what is mandated in the regulation. Comparison of current readings to baseline references are often a key indicator of battery state of health and easy access to this information can make analysis and decision-making much easier. Additionally, NERC PRC 005-6 standard references analyzing measurements against their baseline values, thus retention of a commissioning report can be valuable in this regard. Without a solid baseline reference ohmic value, measurements have little meaning. Therefore, having a system configuration backup is also extremely helpful in the restoration of a site should the system need to be replaced or repaired.

It is necessary to maintain a record of both historic data and alarm reporting data associated with each battery system. Additionally, companies often have their own historian databases. While these databases can be valuable for audit purposes, they should only be used if they are comprehensive and there are no major gaps in the data. The authors promote a local data retention mechanism and a high-quality synchronization process to ensure all critical data is captured and reported to the historian.

Customer Scenarios

Here we will show two practical applications for maintaining data backups. The following scenarios are based on feedback customers have given the authors. These scenarios will highlight the suggested retention scheme and restoration process.

Case 1

A customer has a natural disaster where significant damage occurs in their substation. Once the building is repaired new switchgear, RTU and charger have all be installed. Some of the battery monitoring components were damaged but a portion of the system was not affected. The battery however was tested and is intended to be recommissioned.

In this scenario, there is a battery asset that is salvageable and a portion of the battery monitoring system that can be utilized going forward. What is needed is a full data recovery for the battery monitoring system. Steps to recovery:

- First the necessary new hardware would be installed.
- Second, the system configuration would be either rebuilt or downloaded from a backup.
- Next the local alarms would either be regenerated or would be downloaded from a backup. This might require mining the historian for the initial baseline and calculating the alarms based on initial readings.
- Now is when restoration would be challenging for many existing systems deployed today. At this point the system is expected to begin generating new records but unless the history is restored only limited local analysis can be performed. By downloading the entire history into the local database, the maintenance team can work on a system with full visibility regardless of their local network access capability.

Case 2

A 20-year battery has failed in just 2 years. Many of the cells will not hold a charge. The warranty is still valid; however, the supplier has questioned the battery charging voltage and environmental conditions for the site since they don't have other customers reporting similar problems. The company ran a battery monitoring system since the battery was deployed. The operator wishes to provide evidence of the following to the battery manufacturer:

- Proper charging
- History of discharge activity
- Ohmic value baseline and trending to present state
- Cell voltage history
- Ripple activity on the battery
- Proper electrolyte maintenance

Much of this data is stored by the historian. Therefore, the operator can pull records from the historian and produce a report. Most historians would record at regular intervals the voltage and ohmic value data required. One could also expect that the float voltage and cell temperatures would be readily available from the stored records. What could be more challenging is the more detailed data like evidence of discharge activity or in some cases the ripple measurements captured by the battery monitoring system. For flooded cells many battery monitoring systems can provide detailed about the proper electrolyte level measurements, another important factor to be considered in battery maintenance. By having a comprehensive backup of all data sampled by the battery monitoring system there is ample evidence that the battery was well maintained. The case to be made here is that all information captured by the battery monitoring system should be maintained and in a format that makes reporting simple for the operator.

Understanding the Criticality of the Application and Impacts on Backup Process

In the above examples, it is possible that some locations have batteries that are not deemed critical. Typically, the loss of battery performance information for these systems isn't vastly important. Some examples of batteries in this type of configuration may include small rechargeable applications, such as single-phase desk UPS batteries, and rechargeable alarm system batteries, or non-critical system and station batteries. In these applications, it could be argued that most individuals simply care if the battery will perform for a short duration and not about any performance characteristics of the battery. Most users don't monitor these batteries simply due to their size and relative ease to replace.

Some users have small deployments (~120 cells/containers) deployed across a vast region and geography, such as a utilities operator. A utility will often have keen interest in the current state of their isolated substation batteries because of regulatory compliances that they will be held to. Here, the criticality of the network component is a larger driving factor than size or location. In these deployments, regulatory compliance and potential fines and penalties may be enforced if data can't be furnished to prove systems were functioning as intended. Due to the remote nature of the deployments, frequent manual backups are likely hard to perform, and users may rely on automated backups over a secure network connection.

Others may have large populations of cells/containers in concentrated locations such as a data-center. Simply due to the sheer size of the application, sites could have deployments of greater than 1,000 containers/cells. The battery information made available here could provide insight into current performance of the battery system and show possible areas within their facility where the battery may be showing signs of degradation. Business drivers, to ensure the Service Level Agreements (SLA) with their customers, will motivate these users to be pro-active in mitigating the risk rather than be reactive following a failure after an outage event. In these deployments, a process may be in place to manually backup the battery monitoring data during a normal maintenance visit or system walk-through.

Best Practices

What can users do to implement best practices for their battery monitoring system data?

First, perform backups frequently. As noted above, frequency will depend on a variety of accessibility variables. For simplicity we propose breaking this down into two categories: Network Accessible Sites and Non-Network Accessible Sites.

For Network Accessible Sites daily backups are recommended. These often involve either remotely accessing a snapshot of the system, configuration and other important system files for backup, or the remote system automatically pushing these files to a centralized location.

For Non-Network Accessible Sites backups are most likely to be performed manually. These typically require an individual to be on-site to perform the backup. Best practices in these situations would be once every preventative maintenance visit.

Have a Restoration Plan

Should a system fail for whatever reason, a contingency plan should be in place. This will often require maintaining at least one spare monitoring system (or individual components) at the maintenance office. Speak with the battery monitoring system manufacturer about the necessary files or steps that would be required to migrate all data, configurations, and settings to a new replacement system. Steps will vary depending on the manufacturer, however users should be able to upload a few files to a system to restore operation.

Equally important to having a restoration plan is to test the restoration plan. Unless you can verify that the data is stored properly, you simply won't know and can't guarantee that the restoration process will function.

Much like our personal computers, a backup procedure must be established to maintain continuity of information. The amount of information lost is largely dependent on when the last backup of the system data occurred. Not only should that information be backed up, but there should be a reliable and tested method to restore system data or restore sufficient information to continue operating and collecting pertinent information.

Much can be learned about each individual battery by having an affixed monitoring system. Battery Monitoring Systems provide additional information that may not be found in the traditional preventative maintenance. This information can be used to determine if the battery is performing as anticipated during a discharge event, if the battery is healthy enough to withstand a discharge event, and if the individual containers are operating as intended within the given battery string. However, this information is compromised if the system fails, and without any data the ability to make informed decisions decreases substantially.

Works Cited

1. Belcher, Chris. *A Comprehensive Study of Battery Monitoring Failure and How they can be Avoided.* Battcon, 2015.
2. NERC (Sup. Ref). "Supplementary Reference and FAQ PRC-005-6 Protection System, Automatic Recolsing, and Sudden Pressure Relaying Maintenance and Testing." October 2015.
3. NERC. "Standard PRC-005-6 - Protection System, Automatic Recoling, and Sudden Pressure Relaying Maintenance." NERC, 2015.
4. *Network Reliability Series: Introduction to Network Redundancy.* Mar 7, 2014. http://resources.intenseschool.com/network-reliability-series-introduction-to-network-redundancy/ (accessed Feb 13, 2018).