Electrical Energy Storage Data Submission Guidelines, Version 3

Sandia National Laboratories
Waylon Clark
Yuliya Preger
Rodrigo D. Trevizan
Valerio De Angelis
David Rosewater

Electric Power Research Institute
Steve Willard
Caleb Cooper
Peggy Ip
Joe Thompson
Lakshmi Srinivasan
Morgan Smith

Electrical Energy Storage Data Submission Guidelines, Version 3

3002025977

SAND2023-12079

Technical Update, February 2023

EPRI Project Manager
S. Willard

SANDIA NATIONAL LABORATORIES
Albuquerque, New Mexico 87185 and Livermore, California 94550

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia LLC and Electric Power Research Institute.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

EPRI and Sandia National Laboratories prepared this report. The authors would like to acknowledge the Electric Power Research Institute Energy Storage Integration Council (EPRI ESIC) participants who provided technical guidance, insight, and review during the development of this report. Sandia National Laboratories (SNL) and EPRI would like to acknowledge specifically the following personnel:

Frances Cleveland – Xanthus Consulting

Jim McDowall, FIEEE – McDowall Advisors LLC

Donna Pratt and Ryan Quint – North American Electric Reliability Corporation (NERC)

Charlie Vartanian and Jaime Kolln – Pacific Northwest National Laboratory (PNNL)

This report describes research cosponsored by EPRI and SNL. SNL was supported by the Department of Energy Office of Electricity Energy Storage Program, under the direction of Dr. Imre Gyuk.

SNL and EPRI acknowledge that portions of this report might have been previously published by the Government and are now believed to be in the public domain.

This publication is a corporate document that should be cited in the literature in the following manner:

Electrical Energy Storage Data Submission Guidelines, Version 3. Electric Power Research Institute (EPRI) and Sandia National Laboratories (SNL): 2023. 3002025977.

ABSTRACT

The knowledge of long-term health and reliability of energy storage systems is still unknown, yet these systems are proliferating and are expected increasingly to assist in the maintenance of grid reliability. Understanding long-term reliability and performance characteristics to the degree of knowledge similar to that of traditional utility assets requires operational data. Numerous entities, including EPRI, the U.S. Department of Energy, the North American Electric Reliability Corporation, and the Federal Energy Regulatory Commission, have pointed out the lack of uniformity in data presented by a legacy system and recently installed storage systems. Access to relevant data has also been disparate, with some systems providing robust amounts of data from both AC and DC sides of the systems, with others providing only sparse AC meter data. Uniform and in-depth data acquisition specifications are needed to ensure placement of data systems that allow for efficient and reliable operation, improved safety, accurate modeling and planning for storage placement, and diligent monitoring of storage impacts to grid reliability as storage systems age.

This guideline is intended to inform numerous stakeholders on what data are needed for given functions, how to prescribe access to those data and the considerations impacting data architecture design, as well as provide these stakeholders insight into the data and data systems necessary to ensure storage can meet growing expectations in a safe and cost-efficient manner. Understanding data needs, the systems required, relevant standards, and user needs early in a project conception aids greatly in ensuring that a project ultimately performs to expectations.

Keywords
Energy storage data
Grid reliability
Storage controls
Storage performance

ACRONYMS

The following is a list of acronyms used in the report:

ANSI	American National Standards Institute
BESS	Battery Energy Storage System
BMS	Battery Management System
BOP	Balance of Plant
BTM	Behind the Meter
CIP	Critical Infrastructure Protection
DER	Distributed Energy Resource
DMZ	Demilitarized Zone
DOE	U.S. Department of Energy
EMS	Energy Management System
EPRI	Electric Power Research Institute
ES	Energy Storage
ESIC	Energy Storage Integration Council
ESMS	Energy Storage Management System
ESS	Energy Storage System
FTM	Front of the Meter
GADS	Generator Availability Data System
HVAC	Heating Ventilation and Air Conditioning
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
kV	Kilovolt
kW	Kilowatts
LVRT/HVRT	Low/High Voltage Ride-Through

MESA	Modular Energy System Architecture
ms	Milliseconds
MVA	Megavolt Amperes
MWh	Megawatt-hour(s)
NAS	Network Attached Storage
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OMC	Outside Management Control
OT	Operational Technology
PCS	Power Conversion System
PNNL	Pacific Northwest National Laboratory
PV	Photovoltaic
RMP	Risk Management Process
ROVI	Rapid Operational Validation Initiative
SCADA	Supervisory Control and Data Acquisition
SNL	Sandia National Laboratories
SOC	State of Charge
SOH	State of Health
V	Voltage

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
OVERVIEW

As energy storage technologies promulgate, the need to understand their reliability and performance has become paramount. In 2022 alone, over 13 GW has been installed, with strong growth expected to continue in future years as storage assumes a prominent grid resource role.[1, 2] The increased focus on how these systems perform has exposed gaps in data uniformity and the magnitude of data access needed for proper operation, robust analysis, and system health monitoring. Operational experience to date has revealed numerous instances where insufficient data access has led to costly project delays and required modifications to align performance with maturing expectations. Further guidance is needed to inform numerous stakeholders on what data are needed for given functions, how to prescribe access to those data, and the considerations impacting data architecture design.

This guide strives to accommodate data needs for various stakeholders as they have different needs for data:

- Researchers need as much data as possible with high granularity to develop tools for independent assessment of past performance and predictions of storage life and future performance.
- Operators of storage need a clear understanding of current and short-term storage capabilities and awareness of any conditions that may prevent required performance.
- Owners and off-takers of storage need knowledge on adherence to warranties and performance guarantees.
- Planners and modelers need to build the real-world characteristics of storage, based on field experience, into models and plans for future growth.
- Information Technology (IT) personnel responsible for communication infrastructure need inputs from system designers to prescribe the architecture to convey data to appropriate personnel, accounting for all data needs and cyber security restrictions.

Complete and accurate data are necessary for all stakeholders to truly evaluate the energy storage system; however, data also need to be extracted efficiently. The number of sensors and meters associated with even smaller storage systems and the associated data potentially available can be very large; a 20-MW battery can easily present over 20,000 data points for concurrent

[1] Energy storage news, https://www.energy-storage.news/us-deployed-record-2-6gwh-of-grid-scale-storage-in-q2-wood-mackenzie-says.

[2] S&P Capital IQ, https://www.capitaliq.spglobal.com/web/client?auth=inherit#news/article?id=71827357&KeyProductLinkType=14&utm_campaign=top_news_4&utm_medium=top_news&utm_source=news_home.

monitoring. This amount of data can be redundant for the requirement. This guide explores the Data Optimization topic, whereby a stakeholder can assess what data are needed and the associated bandwidth and architecture for use in analysis or monitoring. It also highlights associated topics to help guide the delivery of data.

This guide presents information in the following sequence:

1. Who needs what data, including impacts of recent standards and draft requirements from regulatory bodies
2. Overview of typical data architectures with examples of bandwidth required and data paths that may be used for typical systems
3. Description of a new Excel-based tool, published separately through the EPRI Energy Storage Integration Council (ESIC) Library (using Product ID 3002025961), for individual projects to demonstrate high-level data bandwidth requirements for given selections of sensor inputs
4. Case studies that highlight specific data requirements for different stakeholders in the Operations and Maintenance phases of a project, including Asset Management and Safety and Health Monitoring
5. Explanation of how data needs can be incorporated into IT Requirements and Project Solicitations
6. Influence of cyber security requirements on the design of the data architecture and data access by various stakeholders

Previous versions of this guide can be accessed for content not included in this version. These previously covered topics include[3]:

- Interoperability, standards, and guidelines
- Sensor and computational accuracy
- Alarm management
- DC power quality

The intent of the current guide is to give stakeholders insight into the data and data systems necessary to ensure storage can meet growing expectations in a safe and cost-efficient manner. Understanding data needs, the systems required, relevant standards, and user needs early in project conception aids greatly in ensuring that a project ultimately performs to expectations.

[3] https://www.epri.com/research/products/3002022119.

2
WHO NEEDS WHAT DATA

Storage systems are relatively new entrants into utility resource compositions and customer-side solutions. The essential roles these systems are tasked with require thorough knowledge on their status and ability to perform those roles safely and efficiently. This knowledge requires accurate data, and the need for data spans across many stakeholders. It is necessary to understand the amount of data required by different stakeholders early in project formation to avoid data oversupply, confusion, and inaccurate assessments. This section provides guidance for determining who needs what data, and why they would need it.

2.1 Tiers of Data Needs

For every installed energy storage system (ESS), there are varying levels of interest and need for operational, performance, and reliability data. Field experience with deployed ESSs (predominantly Li-ion battery energy storage systems: battery energy storage systems [BESSs]), has shown that entities that use ESS data can be categorized into five distinct groups. The amount of data required by each is indicated by the tier number and location, as shown in Figure 2-1. Those that use the least amount of ESS data are denoted as Tier 1 entities, with Tier 5 entities requiring the most data.

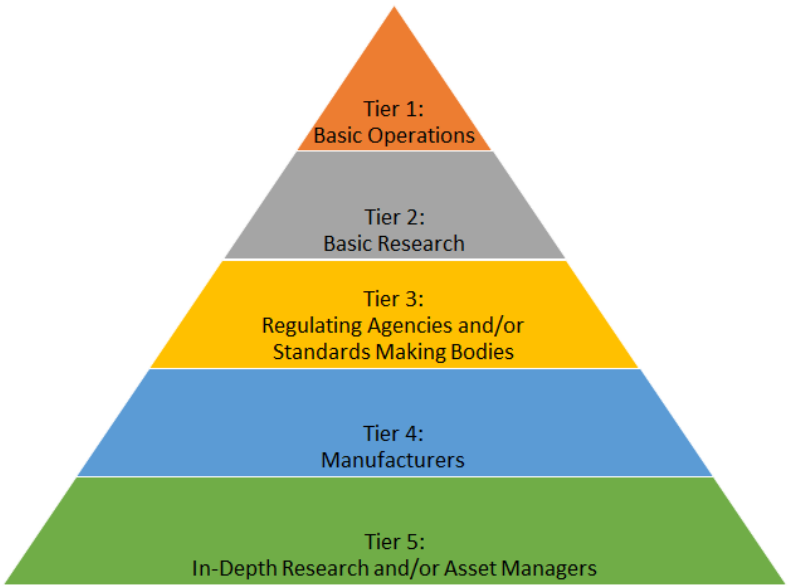

Figure 2-1
ESS data needs for different stakeholders (Data are from a single installation.)

Tier 1 – Basic Operations include entities that are relying on storage to perform given functions in their daily duties (for example, photovoltaic [PV] firming, frequency, and voltage regulation). They require knowledge of system status and short-term capability. Key indicators include state of charge (SOC), power output, and key faults and alarms (for example, grid faults, storage system faults, temperature warnings). Indication of the storage system's ability to perform short-term future functions is also key, and these operators need to be able to assess this capability to schedule storage as a viable resource. They also need to know how to operate the storage system to allow for rest periods to attain forecasted storage functions.

Tier 2 – Basic Research consists of entities that track the storage performance over time and project future capabilities. This includes asset managers who monitor storage system health and potential safety indicators, as well as respond to external signals driving storage functions. These external inputs could include output from a renewable resource, site electric meter demand readings, or market signals. Data needed could include historical output, achieved ramp rates, accuracy of response to external signals, and state of health (SOH). Analysis with this group informs basic operations on scheduling and warranty adherence.

Tier 3 – Regulating Agencies and/or Standards Making Bodies are entities with the authority to require reporting of specific data from components of a BESS. These entities can include, but are not limited to, NERC (North American Electric Reliability Corporation, IEEE (Institute of Electrical and Electronics Engineers), and IEC (International Electrotechnical Commission). Requirements may specify data points, frequency, and resolution. Specific data needs related to emerging standards and policies are provided later in this section, with full details in Appendix A.

Tier 4 – Manufacturers are entities that have supplied one or more of the base components of an ESS. For example, in a BESS this could be the DC block alone or the DC block and the enclosure. Manufacturers may also package together all components that comprise a complete ESS system (DC block, power conversion system, balance of plant [BOP]). These entities require data to provide diagnostics support to the BESS owner if a given component fails. Many of these entities have built-in methods to collect and store data from each of their supplied components.

Tier 5 – In-depth Research and/or Asset Managers is an entity that typically does not own and operate the BESS but has an interest in BESS-generated data. In-depth research is typically conducted by institutions such as U.S. National Laboratories or EPRI. The amount of data required for in-depth research is typically significant but will vary by the type of research being performed and the ability of the system owner to provide the amount of data requested. Asset Managers are responsible for management of warranty, daily operational, and economic performance of the ESS. Asset Managers can be the system owner or a third-party contractor, and require all data available to perform functions such as maintenance of the ESS, market dispatch, responding to events such as component failures or emergencies, warranty testing (capacity fade), and daily system monitoring.

In some cases, an entity can belong to more than one Tier class of data user based on ownership of the ESS. For example, a utility-owned system in which the utility is not only the system owner/operator but also self-performs the ESS maintenance will have the data needs of a Tier 5 entity.

BESS-generated data can be broken down into three major categories that correspond to the major system components of a BESS. These three categories are:

- DC block
- Power conversion system (PCS)
- BOP

The tiered system creates a structure for optimizing the amount of data that any given entity needs to ingest into their own system in terms of transmission bandwidth, data storage, and analysis.

Table 2-1 depicts an actual deployed BESS with the data generating categories. Within each category are non-exhaustive examples of common data available at the subcomponent level. The Tier columns designate the quantity of BESS-generated data points monitored and collected in this deployed system by Tier 1 (utility that owns the BESS) and Tier 5 (research institution/ asset manager) entities. Tier 4 entities may monitor and store data specific to the component of the ESS they supplied. Tier 2 data requirements would be dependent on the type of research being conducted. Even for Tier 5, the number of points available is limited by the number of points the manufacturer is willing to provide; some manufacturers do not provide access to all data being generated.

Table 2-1
Data points typically available to each user tier

Category	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
DC Block (Battery Management System Data) Rack, module, cell level battery data: • DC voltages, currents, temperatures, status, faults • Calculated values: • SOC, SOH, aggregate cell values (min, max cell voltages and temps)	~ 60	Research-dependent	Per regulation requirement or compliance with a specific Standard	Specific to manufacturer or component supplier	~ 70
Power Conversion System (PCS) Inverter data (individual and aggregate): • DC voltage, current • AC voltage, current, frequency, power factor • Aggregated/calculated values	~ 65	Research-dependent	Per regulation requirement or compliance with a specific Standard	Specific to manufacturer or component supplier	~ 90

Table 2-1 (continued)
Data points typically available to each user tier

Category	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
Balance of Plant (BOP) Enclosure and thermal management: • Temperature, humidity Fire detection and suppression: • Water/dry chemical system status • Smoke/heat sensors Alarms: • Faults, e-stops Local data: • Weather	~ 20	Research-dependent	Per regulation requirement or compliance with a specific Standard	Specific to manufacturer or component supplier	~ 20
Actual Monitored Data Points	~ 150	Research-dependent	Per regulation requirement or compliance with a specific Standard	Specific to manufacturer or component supplier	~ 200

The example given in Table 2-1 represents a single lineup BESS with the following characteristics: a single container housing the DC block with module-level and rack-level battery management systems (BMSs), a separate cabinet for each of the two power conversion systems (PCSs), and an energy storage management system (ESMS). For larger systems with multiple lineups, the amount of data available scales correspondingly. The numbers for each Tier indicate the points monitored and collected in each category for this deployed BESS. There are a total of approximately 1000 system data points. In this case, due to costs associated with data collection, only about 200 data points were collected for analysis by the Tier 5 entity. Typically, a Tier 5 entity will collect all available data points, but there are practical limitations, as discussed below.

The first practical consideration is how many data points each of the ESS component manufacturers will make available for collection and monitoring. As seen in practice, the data made available are often already aggregated and individual values are not accessible. This is especially true in the DC block component category where, for example, in a BESS, the cell level data are often aggregated and made available only at the module or even rack level. In other cases, the gateway to the ESS data is via the system integrator, and even less visibility, to lower-level data is possible.

The second practical consideration is the economics of the data acquisition infrastructure. There is a capital cost investment in the hardware, software, labor, and expertise in developing or expanding a data acquisition system. There are also ongoing maintenance, licensing, and other perpetual costs associated with monitoring and storing ESS data. Section 3 describes different data architectures.

A further consideration that can greatly impact the volume of data relates to assigning needed time granularity to each sensor and binary register to further define the *total* amount of data that can be acquired. Section 4 presents a tool to determine data volumes.

2.2 U.S. Department of Energy Data Standardization Efforts

The U.S. Department of Energy (DOE), under the Energy Storage Grand Challenge program,[4] has launched the Rapid Operational Validation Initiative (ROVI) to consolidate battery data across systems, stacks, and cells to predict field behavior when batteries are still being tested in the lab. ROVI also aims to provide ~ 15 years of life and performance predictions with commercially appropriate certainty, using less than one year of fielded system data. A key component of the initiative is to supply tools that standardize how data at different levels (cell to system) are collected and consolidated in repositories for further analysis. Figure 2-2 highlights the key elements of ROVI: data, analysis tools, and accelerated testing protocols for distinct energy storage use cases.

Figure 2-2
Key elements of ROVI (ROVI aims to use machine learning and systematic data acquisition tools to accelerate lab testing of battery technologies and prevent unexpected field failure.)

The first application of ROVI will be for the development of flow batteries, as detailed in the ROVI Lab funding opportunity announcement in 2022.[5] As part of the effort, the DOE will provide data specifications and tools to collect data at the cell (lab), stack (product development), and system (field deployments) levels. This data framework may be included as a requirement in future funding opportunities for energy storage demonstration projects supported by the DOE.

[4] https://www.energy.gov/energy-storage-grand-challenge/energy-storage-grand-challenge.

[5] https://www.energy.gov/oe/articles/us-department-energy-opportunity-rapid-operational-validation-initiative-flow-batteries.

2.3 Data Needs Related to Emerging Standards and Policies

The standards and policies that relate to energy storage systems, especially regarding monitoring and performance assessment, have lagged the actual implementation of these systems. Nevertheless, it is important to understand the development of these standards and policies as they become requirements and not options. The following section reviews draft reporting requirements from the NERC and data requirements stemming from IEEE standards.

2.3.1 NERC 1600 Draft GADS Reporting Requirements

Performance reporting has been traditionally mandated by NERC for the Generator Availability Data System (GADS) for fossil-based, NERC-registered entities. The NERC has since expanded reporting requirements to wind-based resources and recently has undertaken drafting of reporting requirements for Solar Generation systems, which include, in the case of PV Hybrid applications, requirements for energy storage reporting.

An extract of the storage-related requirements, derived from an October 2022 Board Review Draft, is presented in Appendix A.[6, 7] The draft structure is as follows:

1. Configuration data
2. Performance data
3. Event data
4. Outage reporting

Data fields in each section are labeled *Required*, *Conditionally Required*, or *Voluntary*. The majority of the fields are labeled *Required*.

The tables in Appendix A list the Draft Reporting Variable from the NERC and a longer description. This guide adds the Data Guidance and Data Source columns to those tables to illuminate how the data can be obtained and from where (some draft NERC requirements require manipulation of sensor data).

Table 2-2 is a sample of the tables in Appendix A and is used to demonstrate the application of the Data Guidance and Source Columns. In this case, the data field Charging Hours may require, per the Data Guidance column, modifications to meter logic. The Data Source column offers potential locations where logic to derive Charging Hours could be applied.

[6] https://www.nerc.com/pa/RAPA/PA/Section1600DataRequestsDL/GADS_Solar_DRI-Proposed_2024.pdf.

[7] This Section 1600 draft was specifically targeted to Hybrid PV systems and therefore included storage reporting. The NERC has indicated that GADS reporting for stand-alone storage will follow when the PV Hybrid requirements are defined.

Table 2-2
Draft energy storage reporting variables from the NERC

NERC Draft Reporting Variable	Description	Data Guidance	Data Source
Charging hours	Number of charging hours to the Energy Storage Group for the month being reported	Reporting system required to be able to count hours the meter moves in charging direction (This may not be a discreet point in standard control architecture and would need to be derived from applied logic to meter data.)	Site Meter or EMS or Historian if timing counter is built-in or via logic applied to a historian

Certain sensor-based data points would need to be reported with timestamps and assessed for inclusion. Additionally, some reporting requirements may necessitate added logic to the system assembling the report. Some of these points include:

- Meter data
- Alarms
- Alarm classifications
- ESMS reported condition
- Charging versus discharging hours and associated MWh

Manual inputs, distinct from sensor inputs, would be required to identify the following:

- Type of outage
  - Forced: outside management control (OMC) and non-OMC
  - Planned
  - Maintenance
- Duration of outage
- Cause of outage

These manual inputs would originate from either direct, manual reporting to the NERC, or via a field operations and maintenance (O&M) data collection or asset management tool.

While these reporting requirements are still in draft form, the content has remained relatively constant throughout the external review process. The initial draft was issued in July 2021 and went through numerous review cycles. The deadline for issuance and finalization of these requirements is currently listed as January 1, 2024. Projects in the planning stage could benefit from incorporating the logic and systems needed for NERC reporting. These requirements will also apply to NERC-registered entities.

2.3.2 Data Requirements Stemming from IEEE Standards

Recent updates to inverter-based standards have included reporting requirements that will impact storage systems. Two of these new standards (IEEE 2800-2022 and IEEE 1547.9) are discussed below.

IEEE 2800-2022 – Standard for Interconnection and Interoperability of Inverter-Based Resources Interconnecting with Associated Transmission Electric Power Systems

This standard was published in April 2022 and covers the technical requirements for "the interconnection, capability, and lifetime performance of inverter-based resources interconnecting with transmission and sub-transmission systems."[8] The measurement requirements for inverter-based resources (including storage) are differentiated by the type of recording system associated with the needed measurements. Note that some of these systems are very sophisticated, requiring high accuracy and ability to collect very large amounts of data.

Chapter 11 and specifically Table 19 of the standard describe specific measurement points and data collections systems that are required. Some of these points include:

- Plant supervisory control and data acquisition (SCADA) data, including, in part, interconnection voltage, frequency, active and reactive power, and external control signals. These are to be recorded on 1-s intervals in a CSV file and retained for one year.
- Plant equipment status, including, in part, breaker, transformer, and load tap changer statuses as well as status of medium voltage collector and individual inverter-based resources. These are to be collected on an as-changed basis with a timestamp and retained for one year.
- Unit functional setting collected on an as-changed basis, retained for one year.
- Sequence of events recording, including event type and associated timestamp. This requirement calls for very high accuracy of 1 millisecond or less and could include very large amounts of records, retained for 90 days.
- Digital fault recording, which focuses, in part, on transient events and associated data capture of phase-to-ground voltage, bus frequency, and phase currents. Data capture needs to be very fast (≥ 128 samples/s) and stored in a specific format for 90 days.
- Inverter fault codes to be recorded during ride-through events or inverter trips. This requirement calls for, in part, recording all fault codes, alarm descriptions, high and low voltage and frequency ride-through, *DC current and voltage,* AC phase current and voltage, and control system-associated parameters. This appears to imply the requirement to monitor DC voltage current.

[8] https://standards.ieee.org/ieee/2800/10453/.

IEEE 1547.9 – Guide for Using IEEE Std 1547 for Interconnection of Energy Storage Distributed Energy Resources with Electric Power Systems[9, 10]

This guide was published in 2022 in support of the base standard IEEE 1547 – 2018, recommending enhanced minimum requirements for ESS data. These recommendations are given in terms of data measurement accuracy/resolution and additional data points that would enhance the performance of an ESS. It is worth noting that some of these additional measurement and calculation recommendations are also found in other energy storage (ES) codes and standards such as NFPA 855 – 2020.

Chapter 4.4 [Measurement Accuracy], Table 1, of the standard provides resolution recommendations for the required reporting of the ES operational state of charge and operational capacity (operational capacity not required but recommended).

Chapter 4.4.3 [Operational Model Parameters], Table 2, lists additional parameters to supplement operational state of charge and capacity. Table 2 includes minimum resolution recommendations as well.

Chapter 10 [Interoperability, Information Exchange, Information Models, and Protocols] covers additional storage-specific example parameters that pertain to functionality already specified in IEEE 1547 – 2018 (that is, safety data and alarms) and new functionality not covered (that is, direct charge/discharge, scheduling, and so on).

The specific data points and associated resolutions that an ESS owner can expect will be equipment manufacturer-dependent as some may adopt as many recommendations as possible while others will not. A potential ESS owner will need to require vendors to provide a full mapping of the data exchange capabilities contained within the specified system.

2.3.3 FERC Notice of Proposed Rulemaking E-2-RM22-12-000

This Notice, issued in November 2022, directs the NERC to "develop new or modified Reliability Standards that address the following reliability gaps related to inverter-based resources (IBR): data sharing; model validation; planning and operational studies."[11(p. 1)] Of specific significance in this Notice is the language related to lack of data sharing.

FERC states: "The Reliability Standards do not ensure that planning coordinators, transmission planners, reliability coordinators, transmission operators, and balancing authorities receive accurate and complete data on the location, capacity, telemetry, steady-state, dynamic and short circuit modeling information, control settings, ramp rates, equipment status, disturbance analysis data, and other information about IBRs (collectively, IBR data). IBR data is necessary to properly plan, operate, and analyze performance on the Bulk-Power System. As evidenced by the Modeling and Studies Report, the Reliability Standards do not ensure that IBR generator owners and operators consistently share IBR data, as at least a portion of the information that is shared is inaccurate or incomplete."[11(p. 33)]

It should be noted that "reliability" in this context is referring to grid reliability. Elsewhere in this guide, reliability is focused on the storage system.

[9] https://standards.ieee.org/ieee/1547.9/10875/

[10] https://www.sandia.gov/ess-ssl/wp-content/uploads/2021/12/MicrogridsES_Session4_12-3-2021_CombinedSlides.pdf

[11] https://www.ferc.gov/media/e-2-rm22-12-000.

3
DATA ARCHITECTURES

The architecture used to extract, transport, and store data from a fielded ESS to various stakeholders impacts the rate and amount of data that can ultimately be accessed. Different architectures are suited to different application requirements and data needs. Key questions that arise in assessing architectures include: What is the typical streaming rate for a particular connection in Gb/s? What is the typical storage capability of a data historian (database) in Gb? How long should data persist in certain historians? This section conveys some typical architectures and parameters that can be accommodated, depending on how much data are needed. The subsequent section describes a tool to individually assess a project's data quantity and specific parameters.

3.1 Typical Data Categories

Data from energy storage systems fall into three primary categories: streaming, commands, and event. These data are reported at different rates and by different system components, as described below:

- **Streaming**. Real-time operational data including system and subsystem status, operating parameters, and health data. This group includes data from meters and various layers of BESS control down to the BMS, as illustrated in Figure 3-1 in the following section. Streaming data are recorded on a specified schedule, though the actual measurement sample rate can be much higher than what is recorded.[12]
- **Commands**. Real-time control commands sent to various controllers. It is useful to record commands so that they can be compared to the provided output to ensure the system is operating as expected.
- **Event**. Includes both synchronous and asynchronous data. For example, asynchronous security data such as user login events are captured in log files. Alarm and warning data (for example, if a PQ meter threshold is exceeded) may be captured as a time series or as part of log files.

The data architecture must account for all these types of data.

[12] The inverter and BMS must collect measurements much faster than what is feasible or required to record as streaming data. For example: in a specific system a BMS measures all cell voltages every 10 ms and communicates the maximum and minimum voltages over CANBUS to the site controller to prevent overcharge/over-discharge, whereas the average cell voltages are only recorded by the site historian once per second. When the minimum voltage cell nears its low voltage limit, the site controller commands the inverter to quickly change its discharge power limit, which is also only recorded by the site historian once per second. A specific cell exceeding its maximum voltage would be recorded asynchronously as an event and may not appear on the streaming data record.

3.2 Typical Data Architectures

Figure 3-1 shows the overall high-level control and data collection architecture typically used for medium to larger front-of-the-meter systems.

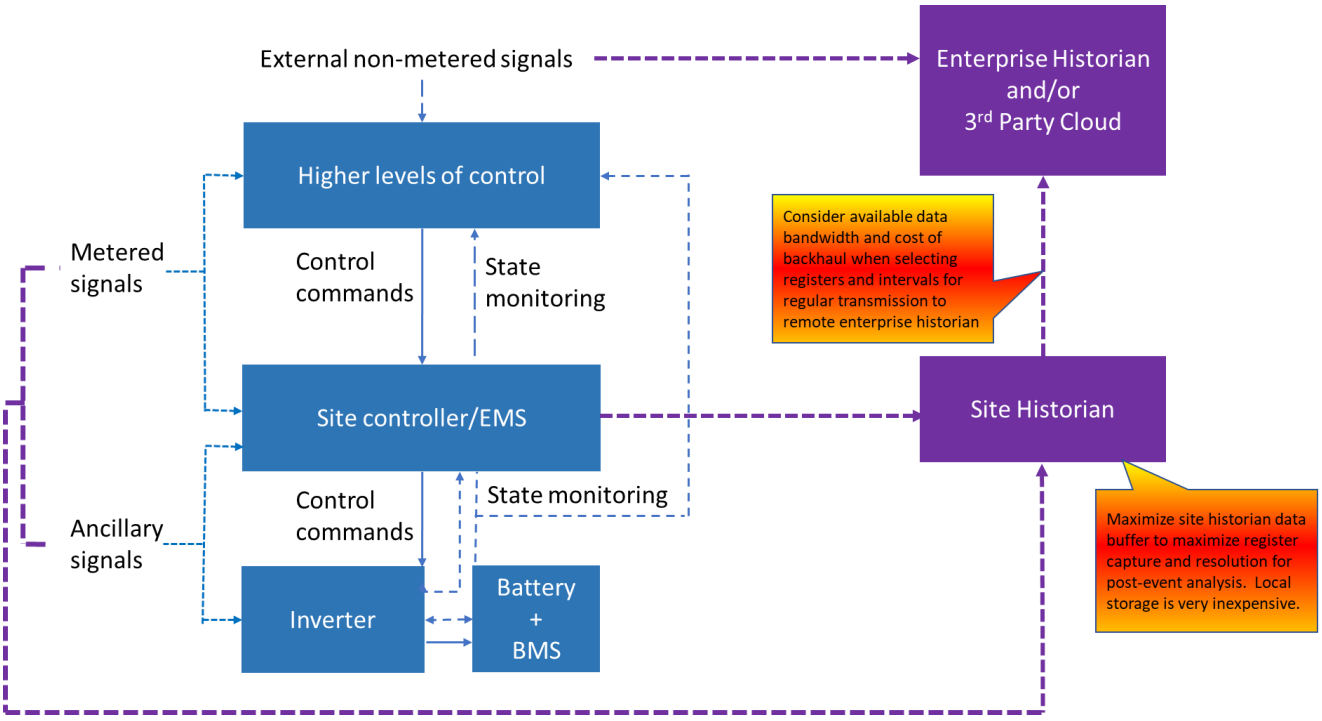

Figure 3-1
High-level ESS data and control architecture (Control architecture is blue, and data architecture is purple.)

In most cases, a sophisticated off-site data historian system (enterprise historian and/or third-party cloud) is preferred due to the capability of applying numerous tools that can be used for deep performance analysis, such as calculation of cell resistance trends and degradation estimation. A site historian can be used to compile data for transport via alternative means or on an as-needed basis. Note that event data, as prescribed by Standards such as IEEE 2800 (see Section 2), can produce voluminous amounts of data that are not suited for transport via typical communication methods. The architecture can be broken down into the following elements to allow an understanding of requirements:

- **Battery + BMS in the storage unit**. Includes all necessary points associated with the storage device(s), PCS, metrology, and all installed power meters.
- **Site controller** (the DNP3 or IEC 61850 based outstation). Data collection device must also have a backup connection to the primary with a speed of at least 10 Mbps, less than 200 ms of latency, and less than 5% packet loss.
- **Data transport.** Primary link for the data collection to and from devices (represented by purple dash lines in Figure 3-1) via high-speed wired or wireless connection with a speed of at least 10 Mbps for wired and 5 Mbps for wireless with less than 1% packet loss. Standard connections of this type include fiber-optic, Category 6 or 5e ethernet, RS485, and/or cellular.

It should be noted that higher upload speeds may be difficult to attain in certain cell coverage areas. Strategies for lower cellular transmission rates need to be further researched.[13]

- **Enterprise (or off-site) and site historian**.[14] Data collection software such as the historian, database, and operating system must be the latest version and kept up to date throughout the project to ensure data and cyber security policies are met. Data collection devices must have an onboard memory of at least 60 days with the same resolution of being collected. Note that there may be more than one historian. A site historian can collect and analyze data and report out, lessening the burden on data transport. The data transported from the site historian to an off-site historian may be a subset of the data recorded locally. Generally, data from the system stored in the enterprise historian pass first through the site historian. An off-site historian (also referred to as a *digital twin*) can be connected to numerous systems and used to analyze performance or issues without a direct, real-time communication link.
- **Higher levels of control, or off-site control systems**. These are the utility or market participant control systems that ingest external or grid signals and instruct downstream control systems. This could include grid operation controls adapted to accommodate storage as a grid resource.

Limitations on data transport and hence performance analysis capabilities hinge on the limitations of a given architecture. Consider the available bandwidth of locally available Internet connections, as well as the per-Gb cost of data backhaul. Many options for economically effective high-bandwidth connections are available such as cellular, satellite, cable, and fiber, as follows:

- The bandwidth for transporting data off-site does not need to be very high. Almost any network connection can handle a significant amount of data. Consider a very slow 9600 baud serial/dial-up connection; even this slowest of the slow connections can handle around 600 16-bit registers/data points per second. A modest 3G cell modem at 0.5 Mbps is 50 times faster than that of 9600 Baud modem, while modern cellular, broadband, fiber, and satellite are 100+ times faster than legacy 3G cellular.
- Data storage is very low cost in the context of energy storage or other renewables projects. Drives of 10-Tb NAS (Network Attached Storage) are about $200 each and can be run in a Redundant Array of Independent Disks configuration with multiple drives in a NAS to self-backup the data. If owning the hardware is not of interest, data storage vendors charge ~ $0.023/Gb/month to store data in the cloud (for example, Amazon Web Services).
- When a system is performing correctly, there is not much need for huge, high resolution data sets. However, during system commissioning and periods of non-specified performance, determining specific operational tendencies, root causes, and proper mitigations without robust data can be nearly impossible. It is possible to install a NAS on site that stores, for

[13] Lower cellular transmission rates can be achieved through use of an on-site historian. Typically, the on-site historian will contain complete, high-resolution data and event logs. It gets periodically overwritten but can be referred to after the fact if an event is noted in the relatively sparse cellular backhaul data.

[14] Digital twins are a type of off-site historian with special features for performance assessment, predictive maintenance, diagnostics, and troubleshooting.

example, a month's worth of data and overwrites the oldest data in perpetuity. This way, all data points can be recorded and stored for service use without the cost of data backhaul, but the data exist for analysis in case of an event. Additionally, certain standards like IEEE 2800 dictate event data holding periods (see Section 2).

- The cost of a single technician visiting a site for even simple remediation steps can exceed $1000. Thus, having data available in advance can be invaluable, to understand what issues the technician may need to solve and what parts may be needed, and can certainly pay for the data storage costs the first time an additional visit is avoided.

Regardless of the available bandwidth and cost of data transmission, limiting the total number of registers and the sampling interval for data routinely transmitted to the remote enterprise historian may be required. However, on-site storage can be very inexpensive. Storing the maximum available registers at the highest available resolution in the on-site historian data buffer can be advisable. Complete, high-resolution data sets can be integral to troubleshooting and/or determining the root cause of faults after events have transpired. These data will be continuously overwritten as the system operates, and the period for which the data persist in the local historian is dependent upon the size of the local storage and the rate of data evolution from the local systems.

The amount of data produced by a system can vary significantly, depending on the system size and collection strategy (sparse/minimal for operations versus robust for extensive analysis). The following ranges in Table 3-1 could be expected for a containerized lithium-ion system. These values were extrapolated from the new EPRI ESIC Data Calculator Tool discussed in Section 4.[15]

Table 3-1
Daily amount of data produced for different energy storage system sizes and collection strategies

System Size/Collection Strategy	Daily Amount of Data Produced (Gb/day)
1 MW/sparse	0.02
1 MW/robust	0.44
50 MW/sparse	0.70
50 MW/robust	21.76

[15] Numerous other assumptions underlie the numbers presented and are visible through use of the Data Calculator Tool.

Table 3-2 displays typical architectures, associated storage system size, and the paths data (and control signals) take, as well as the ultimate destination of the data.

Table 3-2
Common data architectures for different energy storage applications

Architecture; Location	Data Destination	Data Paths	Notes/Data Destinations
Single modem remote to vendor; BTM single use	Local interface, vendor cloud	Data to vendor, sometimes remote control enabled	Standard utility metering – may be remote
Single modem remote to Vendor + RTU to utility; BTM multiple units aggregated for utility resource needs	Local interface, vendor cloud Utility enterprise network (billing)	Data to vendor, sometimes remote control enabled – Utility accesses and controls via vendor cloud	Standard utility metering – may be remote – data collected by utility for verification
Utility RTU with meter and some storage data – vendor remote access via modem; FTM distribution	Local interface, vendor cloud Utility enterprise network (operations)	Shipped on utility SCADA	SCADA use DNP3 requiring Modbus translation and timestamping
RTU tied to remote utility historian via fiber with Vendor access via Utility fire wall; FTM larger and remote distribution and transmission (both off-taker and utility-owned systems)	Local interface Utility enterprise network (operations, asset management, and so forth)	Meters and EMS (including some BMS) data shipped to local and remote historian	Remote historian disperses to various business units Event capture via PQ or other metering stays on local historian

3.3 Data Routes to Users

There may be many different configurations of data flow, depending on the size, location, and contractual operating stance chosen for a given storage system. Figure 3-2 generically presents numerous routes for data to take from the originating BMS and/or EMS to local and remote historians. Not all paths may be used, and cyber security limitations may prevent some routes from implementation. Additionally, there are typically strong restrictions on access to utility revenue and system metering and, as noted above, high-volume event data may need to be extracted from the site via manual methods.

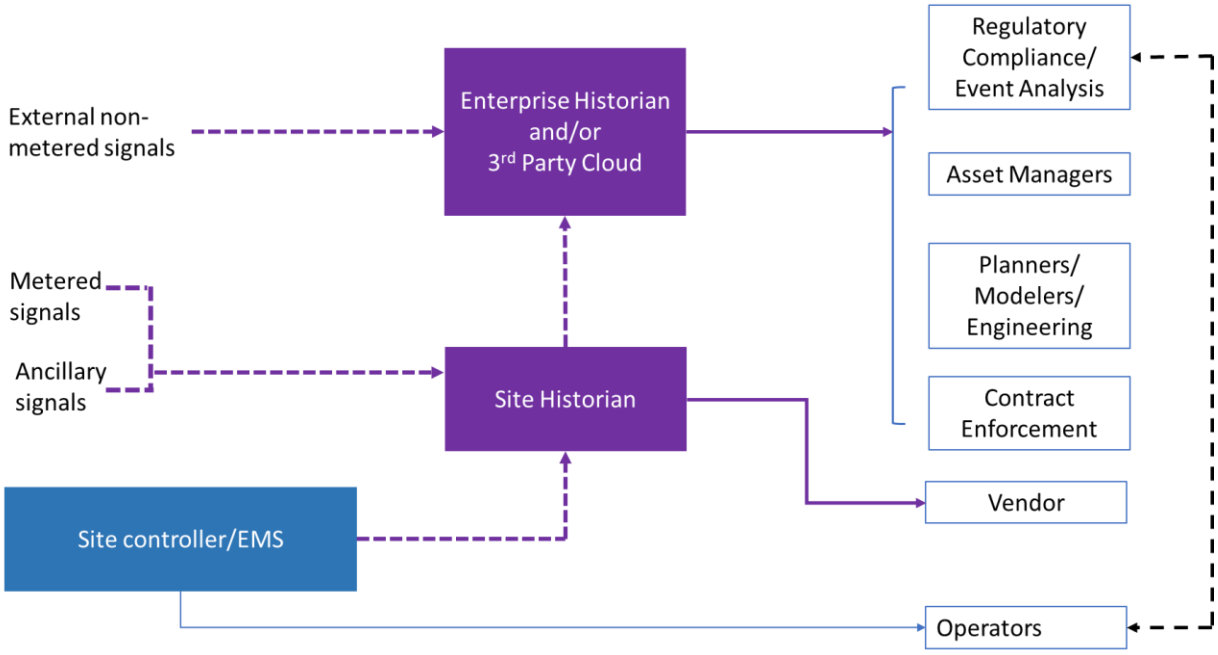

Figure 3-2
ESS data routes to different stakeholders

3.4 Use of Open-Source Software

Battery systems generate a large amount of data that need to be transmitted, stored, and analyzed. Commercial solutions for these tasks exist but can become expensive to manage, especially as the number of ESSs increases and their size decreases to meet the needs of distributed generation. Over the last two decades, large software companies, including Microsoft, IBM, Google, and Facebook, have adopted open-source software technologies. Most webservers run on top of Linux with databases like PostgreSQL and MySQL. The vast majority of smartphones use Android, an open-source version of Linux. Open-source software and systems foster innovation, freedom, integrity, continuity, security, and collaboration. As the energy storage market grows, it will inevitably adopt an open-source model for some of the software components. In this section, we discuss some of the open-source initiatives targeting battery and energy storage systems.

Open-source platforms have successfully been used to securely extract data from remote demonstration projects. For example, a data acquisition system developed by Sandia National Laboratories (SNL) uses Telegraf (an open-source server agent for collecting and reporting metrics) to collect data from the field and transmit them to InfluxDB (an open-source time-series database). Grafana (an open-source interactive visualization web application) is used to securely display the data in dashboards. When queried, InfluxDB generates data in JSON format that makes it easy for any web-based application to extract and analyze the data.

Figure 3-3 shows a practical implementation of an open-source software stack based on Telegraf-InfluxDB-Grafana. The plots on the left show data from an LFP battery pack and the plots on the right show the data from a lead-acid pack. The top plots, Battery A/B cell voltages, come from a BMS. The data in the other four plots come from the power electronics components.

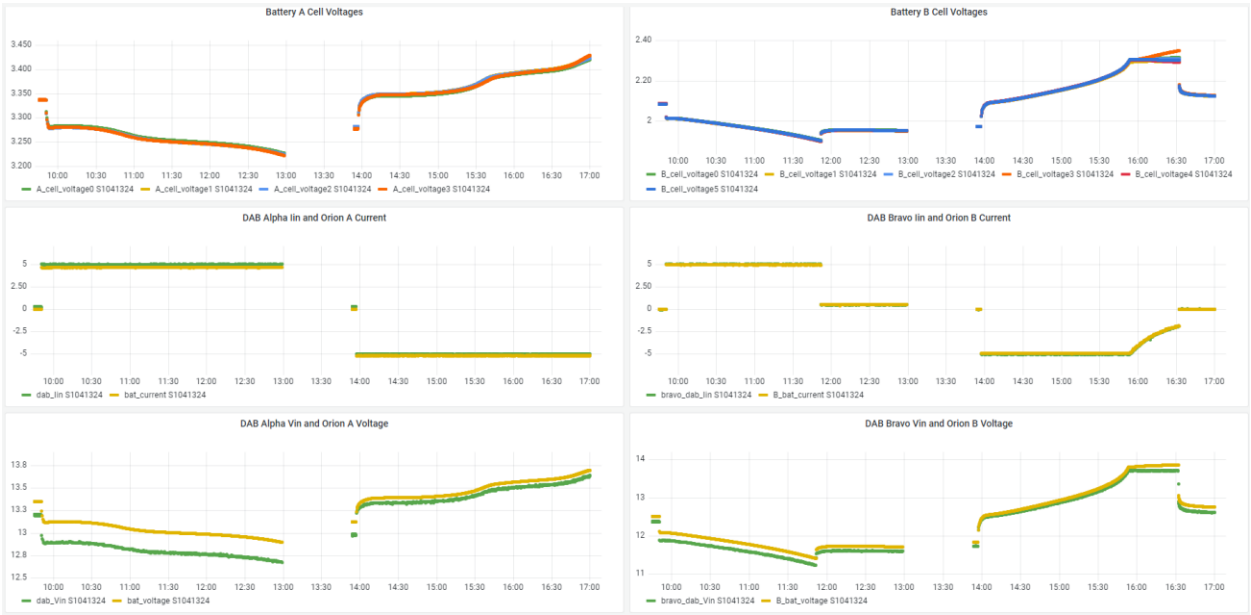

Figure 3-3
Application of an open-source software stack for energy storage data management (Data were collected from a system with Telegraf, imported into InfluxDB, and displayed in a Grafana dashboard.)

4
OPTIMIZATION OF DATA

As stated previously, different stakeholders have different data needs. A new data optimization tool, available through the EPRI ESIC library (Product ID 3002025961), allows users to define data points and sampling rates, then calculates the amount of data collected over a 24-hour period. Users can then align the amount of data they wish to collect with the limitations of the data architecture. This section outlines the general process of data point optimization and use of the tool.

4.1 Data Optimization Tool

This tool is centered on an extensive list of sensors typically available in a Li-ion battery system; however, it can be adapted to other storage technologies. The tool also denotes the time granularity typically associated with internal BMS register poll rates and the actual granularity that is needed. For example, cell voltages can vary quickly, on the order of seconds or less, but only need to be monitored on the minute level.

When a user selects the points desired and their associated sampling rate, the tool calculates the amount of data that would be collected over a 24-hour period. This allows the user to align the amount of data to known on-site data storage capabilities, outbound bandwidth for transporting the data to a remote historian, and the impact to the remote historian storage. Alternatively, if the above requirements are not yet defined, the selection of the data can be used to define formal IT requirements (see Section 7) to allow the selected data flow.

4.2 Instructions on Tool Access and Use

The user starts with the “System Configuration” sheet and defines system parameters for all input cells, highlighted in orange. There are example schematics showing the arrangement of containers on a site, battery racks within containers, and cells and modules within battery racks. These configurations are based on typical Li-ion battery system installations but can be adapted to a variety of battery technologies. When the system configuration data are entered, the user can move to the “Data Points” sheet to adjust the list of data points and the time granularity for each point. The suggested granularity for each data point is included in the tool and discussed below.

Returning to the main “System Configuration” sheet, the user can see the resulting data totals calculated by the tool. The user can adjust these values by changing the Data Sampling parameters on this sheet. To limit data infrastructure needs, the user can choose to only monitor a subset of equipment. Some selections have more impact than others on final data infrastructure. For example, changing the percentage of cell-level data that are sampled significantly impacts the total data collected per day, due to the number of cells in a system, whereas changing the sampling of container-level data has a relatively low impact.

4.3 Data Optimization Tool Application

The following section outlines the use of the data optimization tool for a utility in the design stage for a large storage system. Table 4-1 describes the configuration of the desired system: 10 MW/20 MWh Li-ion-based BESS with 1 MW per container.[16] The scenario assumes a 120 Ah cell; however, the cell count will vary with the cell capacity. The user provides all the information in Table 4-1. Table 4-2 provides the resulting calculated quantities of various components on the site. The "Data Points" sheet contains parameters recorded at different levels within the system, and Table 4-2 contains the multipliers for each data point. For example, for every parameter monitored at the cell level, 46,080 data points will be collected, assuming 100% of cells are sampled.

Table 4-1
System configuration inputs for a 10 MW/20 MWh Li-ion-based BESS with 1 MW/container

Number of site level meters	1
Number of auxiliary meters	1
Number of containers per site	10
Number of inverters per container	2
Number of BMSs per inverter	1
Number of battery racks per BMS	8
Number of HVAC systems per container	2
Number of modules per battery rack	12
Number of cells in series per module (S)	6
Number of cells in parallel per module (P)	4

Table 4-2
Calculated component quantities for a 10 MW/20 MWh Li-ion-based BESS

Number of cells per module (SxP)	24
Number of HVAC systems on site	20
Number of inverters on site	20
Number of BMSs on site	20
Number of battery racks on site	160
Number of modules on site	1,920
Number of cells on site	46,080

[16] Configuration assumptions (which can be altered in the Tool): 10 MW/20 MWh system, 1 MW per container, two inverters in each container, each inverter is 500 kW, one BMS behind each inverter, racks total 1 MWh, 120 Ah/cell at ~3.7 V is 444 Wh /cell, 6S4P arrangement, 24 cells per module, 12 modules per rack, 8 racks per BMS. System will be slightly oversized in terms of energy (1.02 MWh per BMS).

Beyond data points, the Data Calculator also considers the time granularity for the given sensors. The granularity can be modified to assess the impacts on data volumes. Table 4-3 shows the typical time granularity for common sensors.

Table 4-3
Typical time granularity for common sensors

Sensor	Needed Time Granularity	Reason for Granularity
Cell V, I	5 seconds or less	Allows for in-depth degradation analysis
Module temperature	1 minute	Thermal lag
Revenue meter MW	5 seconds or less	Allows ramp rate analysis
Ambient temperature, solar irradiance	15 minutes	Ambient swings minimized (Solar irradiance may need to be less for solar smoothing application.)
Inverter power data	5 seconds or less	Allows for in-depth power flow analysis (non-event oriented)
HVAC operating status	1 minute	Allows for visibility to events and outage causes
SOC	1 minute	Allows insight into how SOC is being calculated
SOH	1 day	Long term health indicator
Power quality meter (PQM)	Subcycle	Required for larger systems – allows for analysis of events[17]

When the data points list and time granularities are set, the tool provides the data totals for the scenario. The percentage of data that are sampled and time granularities can be adjusted to account for bandwidth or Site Historian data storage limitations.

The cell voltages and currents dominate the data count, and the daily file size is very sensitive to the percentage of cells sampled. The tool assumes each data point is 16 bits in size (based on the int16 data type). This is an approximation – some data points are Boolean and only require 1 bit, while others may require more than 16. Additionally, the choice of communication protocol will affect the overall data quantity (note the Tool does not account for specific protocol impacts on

[17] These are typically not polled by the same data acquisition system as the rest of the data. These meters present one-second data for logging; some of those data include values computed from subcycle data internal to the meter, like Total Harmonic Distortion (THD) or specific harmonics. Typically, the meter will provide a separate interface through another protocol like Telnet that will enable users to operate event logging, look at oscillography, and so on. A good baseline for a sampling rate might be 128 samples/cycle, but 512 is more common.

bandwidth requirements). Protocols such as SunSpec Modbus, DNP3, and IEEE 2030.5 differ in the size of message headers and data packets. Even different implementations of the same protocol can have different message sizes.[18, 19] Table 4-4 provides the data totals for the 10 MW/20 MWh system, assuming 100% of all the data a sampled.

Table 4-4
Data sampling, data totals, and file size for 10 MW/20 MWh Li-ion-based BESS

Data Sampling	
% Of container-level data sampled	100
% Of HVAC system-level data sampled	100
% Of inverter-level data sampled	100
% Of BMS-level data sampled	100
% Of battery rack-level data sampled	100
% Of module-level data sampled	100
% Of cell-level data sampled	100
Data Totals and File Size	
Total data points	25,201
Data points per second	22,424
Total bits per second (Assume each data point is int16.)	403,216
Total bytes per second	50,402
Gigabytes per day (24 h)	4.35

The final number in Table 4-4 is the total data collected over a 24-hour period for this configuration and sampling choice: 4.35 GB. This number will dictate the necessary on-site and off-site data storage, depending on where data will be stored and how frequently they will be transferred. The penultimate number in Table 4-4, "Total bytes per second," can be used to size the data bandwidth needed. It is important to note that typical implementations involve a local Site Historian, controller, or logger storing data temporarily, and then uploading the data in batches, instead of a steady flow of bytes/second. This is usually a cheaper method of retrieving data.

In the case of the 10-MW system, by adjusting the sampled percent of module and cell-level data, the bandwidth and storage requirements can be significantly reduced. The example presented in Table 4-5 limits the module-level data to 50% and samples 0.1% of the cell-level data. The resulting daily aggregated data is only 1.37 GB, compared to the 4.35 GB previously.

[18] EPRI 3002019357, *Communications Architecture Requirements for Near Term Smart Inverter Use Cases*.

[19] EPRI 3002016143, *Communication Requirements for Smart Inverter Use Cases*.

Table 4-5
Reduced data sampling and resulting data totals and file size for 10 MW/20 MWh Li-ion-based BESS

Data Sampling	
% Of container-level data sampled	100
% Of HVAC system-level data sampled	100
% Of inverter-level data sampled	100
% Of BMS-level data sampled	100
% Of battery rack-level data sampled	100
% Of module-level data sampled	50
% Of cell-level data sampled	0.1
Data Totals and File Size	
Total data points	7,933
Data points per second	6,100
Total bits per second (Assume each data point is int16.)	126,928
Total bytes per second	15,866
Gigabytes per day (24 h)	1.37

Both the SunSpec Modbus and MESA DNP3 for DER standards have built-in registers for minimum and maximum cell voltages. If, for whatever reason, bandwidth is limited such that cell voltage measurements must be limited, then these minimum and maximum cell voltage registers must be prioritized over random sampling. Understanding the difference between the highest and lowest cell voltages is informative with regard to non-uniform cell degradation, as well as for validating the balancing function of the BMS.

5
DATA POINT SELECTION FOR SPECIFIC USES

Expanding on earlier content on general data needs and data optimization, this section offers a detailed discussion of specific data point needs for operations, maintenance, and asset management. It also covers key data points for monitoring system health and safety.

5.1 Data for Operations, Maintenance, and Asset Management

Operations, maintenance, and asset management are distinct functions that align to different stakeholders and require different kinds of energy storage data. Operations data needs are driven by the operators of the storage. The focus is on understanding storage asset lifetimes as all are still relatively young.[20(ch.7.1)] Maintenance data needs are driven by service crews and overall asset managers who monitor trends. Asset Management focuses on how an overall fleet is managed and implemented, accommodating overall business objectives, risks, and stakeholder values.[20(ch.11.1)]

The following defines some specific data needs for a successful O&M program aimed at storage. As noted previously, regulators are focusing generally on utility equipment performance and reliability, including storage, and the reporting requirements from these regulators also help define the O&M data needed for storage.

5.1.1 Operations

Operators of storage systems are typically involved in dispatching storage, on a network basis, along with generation assets. While smaller storage systems may be operating in a more autonomous fashion, larger systems require real-time monitoring for near-term system balancing and resource needs along with longer-term monitoring of asset condition and predicted operational levels.

1. Scope—Operations can include visibility to current storage status, dispatch of storage, verification of proper response and forward-looking predictions of storage capacity requirements.
2. Assigned Personnel—Distribution, transmission, and generation desk operators. This also includes personnel operating from a remote vendor or integrator stance.
3. Data Needs for Operations
    a. Charging/discharging and SOC management—Operators need to be aware of short- and long-term needs and use SOC as an indicator of capabilities. SOC is not a physical measurement but rather a calculated indicator of current storage capacity. This calculation is typically proprietary and obfuscated. In some cases, SOC is not presented,

[20] EPRI TR 3002021342, *Power Transformer Guidebook, The Copper Book – 2021*.

rather State of Energy is used to indicate capacity. Operators need to be aware of the high and low limits of SOC and avoid situations where further action by the storage is prevented due to SOC status. An example would be when storage is requested to absorb energy from the grid but cannot due to a high SOC status.

i. SOC trending graph at least over the past 48 hours to allow visibility into actions taken, if any, by the storage system in short-term history and allow for identification of where the SOC is currently trending.

ii. Accuracy of the SOC needs to be established as there may be trends where erroneous SOC values are reported for short periods depending on the storage technology and vendor.

iii. In-depth data can potentially be used to independently calculate the SOC but this requires extensive data and algorithm tuning.

b. SOH management—SOH is a longer-term indicator of the amount of degradation a storage system experiences over time. As batteries age, they lose some capacity, and this is accounted for by the SOH. Operators need to be aware of the SOH in the longer term. A storage system with a given capacity for full charge/discharge when first installed will see this capacity diminish over time, thereby limiting storage capacity contributions.

i. SOH itself is a typical reported parameter and needs to be tracked continuously over time. Operators need to monitor SOH levels and check if the SOH is eroding per specifications. If not, warranty or augmentation to refresh capacity actions may need to be taken.

ii. SOH can be verified independently through staging of frequent Reference Performance Tests according to strict test protocols. Typically, full-cycle charge/discharge tests are conducted periodically to assess how much energy was absorbed and discharged. Relating results to past tests, conducted under the same protocol, identify erosion in storage capacity over time. This requires monitoring energy in and out as well as ambient temperatures to allow for correlation to HVAC load impacts.

5.1.2 Maintenance

A mature storage maintenance program, aimed at optimizing asset utilization and extending asset life, requires a well-developed plan and access to pertinent system data. Key data points for maintenance are presented in Table 5-1.

Table 5-1
Key data points needed for maintenance diagnostics

Subcomponent	Data Needed for Diagnostics
Battery modules	Module temperature Rack, module, cell voltage Rack current Balancing indication SOC, SOH history Alarms/warnings
Heating ventilation and air conditioning (HVAC)	HVAC status data Enclosure temperature humidity Ambient temperature, humidity Alarms/warnings
Computers and ancillary equipment (BMS, EMS, uninterruptible power supply [UPS])	Communication and processing related alarms/warnings
Inverter	Harmonics, frequency, voltage excursions
Utility transformer, protective, and switchgear	Dissolved Gas Analysis (DGA) and other traditional assessment data

1. Scope—Assess performance over time and incorporate performance indicators into ongoing maintenance activities as well as structure in-house maintenance activities or oversee outsourced activities.
2. Assigned Personnel—Asset Managers, Engineering groups assessing capital asset performance, planning personnel, standards committees, contracts (for outsourced).
3. Data Needs for Maintenance
    a. Corrective maintenance—Data to respond to the issue at hand
    b. Periodic assessments—Regularly scheduled check-ups
        i. Storage device—Any warnings or alarm on voltage deviations, indications of excessive cell balancing
        ii. HVAC—Internal temperature warnings or alarms and any unexpected deviation in internal temperature
        iii. Inverter—Any irregularities in voltage, current, or frequency
        iv. Safety systems—Alarms or warnings on sensors
    c. Predictive maintenance—Data to anticipate future issues

4. Data Needed to Assist Degradation Analysis
    a. Degradation will vary based on how the batteries are used, the specific chemistry involved, and how the enclosure environment is maintained. Close monitoring of SOH will provide an indication of how much degradation is occurring, but specific sensors and parameters may need to be accessed to indicate why degradation is occurring, especially if the erosion in capacity is greater than expected or warranted.
    b. Some relevant data points and approaches that can be accessed for high-level assessment of degradation include:
        i. Indication of cell balancing (digital register)
        ii. Temperature maps showing enclosure temperature distribution
        iii. Assessment of standby losses via metered energy in and out of the storage during idle periods, assessed over time
    c. For in-depth degradation analysis, the following data may be needed:
        i. Indication of cell balancing
        ii. Rack, module, and cell level voltages
        iii. Rack and module temperatures
        iv. Meter level power quality data
        v. Thermal imaging

5.1.3 Asset Management

Asset Management requires a broader and longer-term perspective on storage performance and reliability. It is also more focused on accounting for numerous systems and their combined impact on resource adequacy and utility system reliability.

1. Scope
    a. Assess current and predict impact of storage, as well as determine storage capacity requirements in total resource planning efforts
    b. Assess adherence to performance warranties and guarantees and impacts of deviation from specified performance
    c. Model storage in resource planning efforts
2. Assigned Personnel—Utility management, resource planners, system modelers, contract enforcement

3. Data Needs for Asset Management
    a. Condition assessment
        i. Related to Performance/Reliability assessment and associated data needs. Warranty enforcement may require in-depth access to battery subcomponent data if deviations are noted, including:
            – Maintenance and repair activities for components and associated dates
            – Field response time and repair time duration
            – Tracking of warranted SOH
            – Tracking of warranted system response times
    b. Model inputs
        i. Models require calibration on degradation experienced in the field to correctly model system life in various scenarios. This also may require access to in-depth data from battery subcomponents:
            – Data needed to independently assess SOC for model SOC tuning
            – Tracking of actual SOH related to different applications, for model SOH tuning
            – Tracking actual efficiency correlated to both applications being served and ambient conditions, for model efficiency tuning
    c. Fleet level management
        i. Comparisons between systems performing similar duties in different locations require higher level performance and ambient weather data for each location and the ability to correlate temperature data to ancillary cooling/heating equipment loads.
        ii. Comparisons between different storage technologies including different chemical variations of Li-ion batteries require similar data to location comparisons. If different technologies are compared (for example, flow vs. Li-ion battery), more in-depth data may be required, especially if ramp rates are being compared.
    d. Operational and maintenance data for organizational structure development
        i. Costs of maintenance including labor, travel, and materials
        ii. Impacts of outages including Mean Time to Repair (MTTR), Mean time Between Failure (MTBF)-type indices, and associated costs of substitute resources during outages
        iii. Assessment of non-specified performance of subcomponents
        iv. Assessment of failure rates for the storage system, in general, and subcomponents

5.2 Data for System Health and Safety

Continuous monitoring of alarms is central to a safety effort. The previous version of this guide discusses alarm management and methods to ensure the correct personnel are seeing the appropriate alarm and warning indicators. Other sensors can be monitored as well to discern aging effects and problematic conditions. Some of these data points and the reasons for monitoring include:

- **SOH**. Large downward trends can indicate significant erosion in performance. SOH trends depend on technology and application. As an example, for a typical Li-ion system cycled daily with a depth of discharge > 80%, an SOH drop of > 1% over one week is significant and merits investigation.
- **SOC**. Abrupt and unexpected changes in SOC could indicate issues with cell balancing, such as poor performing cells that have manufacturing defects. Over time, these defects can lead to cell failure and cascading events, impacting equipment and personnel safety.
- **Cell level voltages**. Overvoltage or undervoltage readings on cells may be an early warning for cell failure, which could lead to thermal runaway and propagation within the system. It is also useful to monitor minimum and maximum cell voltage trends. Significant or abrupt changes are other indications of imminent cell failure.
- **Cell balancing indication flags**. Increases in cell balancing activities (usually during idle or rest periods) could indicate poorly performing modules and cells.
- **Internal temperatures**. Variation in module temperature within a system can be an indicator of poor HVAC performance, which could also impact battery life.
- **Power quality**. Deviations from specified frequency levels and indications of unexpected harmonics can point to problems both internal to the battery system and from external issues with the connected grid.

5.2.1 Details of Assessing Cell Balancing Indication

This section provides an example of assessing cell balancing for a 1-MW Li-ion battery system. The system indicated high daily SOC losses after a long period of normal operation. On idle days with no power flow through the system DC meters, high daily SOC losses of 6.3% were observed. Normal losses incurred earlier in the operational life were measured at 0.78%/day. Investigation of the rack level indicators of cell balancing activity showed a relatively large amount of cell balancing occurring during these idle periods and correlation to large SOC standby losses. The cell balancing was performed by the rack level BMS to dissipate energy from higher charge cells to lower charge cells to correct charge imbalances between the cells. An increasing amount of cell balancing activity is an indicator of deteriorating performance at the cell level, warranting inspection and maintenance. Access to cell balancing indication is key to the level of performance analysis.

6
CYBER SECURITY

The acquisition, transmission, and storage of operational data from energy storage systems require interconnection between the industrial control systems (ICSs) and IT systems. In the past, the ICS network was separated from the IT environment, and this flow of data was very limited. This "air gap" was the main cyber defense feature of these systems and made some believe that this system architecture was immune to cyber attacks, a claim that was proven wrong several times. More recently, several companies have adopted technologies that provide networked connection between the ICS and IT environments. This new architecture provides cost reductions and improved productivity at the cost of exposing ICS to cyber threats from the IT environment.

This guide focuses on cyber security of devices that collect, transmit, store, and process energy storage systems' operational data. However, to be effective, cyber security must be an organization-wide effort with programs in place to cover organizational, business, and operational processes.

6.1 Examples of Attack Vectors and Attack Surface

ESSs have several vectors that could allow remote exploitation, as follows:

- **Service equipment**. It is often necessary to connect service equipment to ESSs. Service equipment could be compromised or used in an unauthorized manner.
- **Mobile media**. Insertion of mobile media into a system component can infect and compromise it, allowing an attacker to gain access to the system network.
- **Local networking**. While threats coming from outside of an organization are of great concern, local communications networks can also be used to access devices associated with ESSs. Some examples include local area networks (LAN), Wi-Fi, Bluetooth, and so on.
- **Vendor cloud service or server**. These require connection between the system and an external server or cloud over public networks. Third-party access through cloud services could be required for vendors to monitor or conduct maintenance on an ESS. If one of these external systems is compromised, cloud service or servers could act as a threat vector, potentially impacting the ICSs beyond the ESS.
- **Software and firmware upgrades**. Software downloads and program editing can be used to attack the ICS.
- **Public-facing infrastructure** (for example, web portals). Attacks on external web interfaces can be leveraged to pivot into the ICS historian that provides ICS data to the web server applications.
- **Phishing**. Phishing e-mail campaigns can be used to steal the credentials to establish a presence in business computers and later pivot deeper into the ICS network.

6.2 Relevant Cyber Security Regulations, Standards, and Guidelines

Cybersecurity standardization is an essential foundation in the highly interconnected and interoperable energy environment in which ESSs are operating. While standards cannot evolve at the same pace as cyber adversaries, a strong foundation of standards provides a common baseline for the industry and establishes fixed criteria to enter the market. Furthermore, requirements unique to each organization can be determined based on evaluated risks and mitigation strategies. The following sections discuss some cyber security regulations, standards, and guides in development that are potentially applicable to ESSs of interest. Regulations, such as those described below, could be legal requirements for bulk power system owners. Standards help owners and operators specify requirements as ESSs are designed and deployed, setting conformity and uniformity for ESS cyber security requirements. Guides are references and recommendations summarizing ongoing and developing efforts in ESS cyber security, such as applying a risk management framework.

6.2.1 Regulations

The NERC Critical Infrastructure Protection (CIP) plan covers mandatory standards applied to the power grid in North America. Standards 2 to 11 cover cyber security areas, including system categorization, security management controls, training, security perimeters, physical security, system security management, incident reporting and response planning, recovery plans, configuration change management and vulnerability assessment, information protection, communications between control centers, and supply chain risk management. NERC CIP standards apply to Bulk Electric Systems, which comprise transmission elements that are operated at 100 kV or higher, and might include generators, transformers, black start resources, dispersed generation resources, and devices dedicated to absorbing or injecting reactive power. Since the NERC CIP standards do not explicitly mention energy storage, it is not clear what standards should be applied to ESS. Under the interpretation that ESS might be analogous to NERC's definition of "generating resources" or "dispersed power producing resources," it is possible that CIP standards might apply to single systems larger than 20 MVA or aggregates of smaller systems that add up to more than 75 MVA. However, excluding systems connected at lower voltages or smaller sizes from compliance with CIP standards neglects the potential risk of coordinated cyber attacks on smaller DER.

6.2.2 Standards

Following is a list of standards that are potentially applicable to ESS cyber security:

- IEC 62351, "Cyber Security Series for the Smart Grid," is a series of standards that cover cyber security for some protocols, including Inter-Control Center Communications Protocol (ICCP), and IEEE 1815 (DNP3).
- IEEE 1686-2013, "Standard for Intelligent Electronic Devices Cyber Security Capabilities," addresses several aspects of cyber security of Intelligent Electronic Devices (IEDs), including data access and access control, encryption of communications, and firmware revision.
- ISA/IEC 62443 is a series of standards that address cyber security of industrial control systems.

- IEC 61850 is a series of standards covering communication networks and automation systems for power utilities. IEC 61850-7-420:2021 "Communication networks and systems for power utility automation – Part 7-420: Basic communication structure – Distributed energy resources and distribution automation logical nodes" provides standardization of logical equipment and logical nodes of Distributed Energy Resources.
- ISO/IEC 27000 is a series of standards that provide recommendations for Information Security Management Systems (ISMSs).
- UL 2900, "Standard for Software Cybersecurity for Network-Connectable Products," in particular UL 2900-2-2, "Outline Of Investigation For Software Cybersecurity For Network-Connectable Products, Part 2-2: Particular Requirements For Industrial Control Systems."

6.2.3 Guides

National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," NIST, 2018.

The NIST ICS framework provides a comprehensive set of recommendations for securing ICSs. Organizations can use it alone or in conjunction with other NIST standards, such as its Special Publication (SP) series, notably:

- NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach."
- NIST SP 800-39, "Managing Information Security Risk – Organization, Mission, and Information System View."
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."
- NIST SP 800-82, "Guide to Industrial Control Systems Security."
- NIST SP 800-209, "Security Guidelines for Storage Infrastructure."

IEEE 1547.3-2007 is the "Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems." Its Clause 9 provides security guidelines for distributed resource implementations. The guide discusses security issues and lists options for securing communications. There is an ongoing effort from IEEE Standards Coordinating Committee 21 to produce a new version of the guide. The new version of IEEE 1547.3 will provide more detailed requirements for cyber security and a broadened scope and will picture cyber security as an organization-wide effort.

IEEE 2030 is a guide for Smart Grid Interoperability. It covers energy technology and IT of electric power systems, end-use applications, and loads. This document defines the smart grid interoperability reference model, which organizes the data exchanges between power systems, communications, and IT. The subclause 4.5 briefly discusses security and privacy and makes many mentions to ISO/IEC 27000 series NISTIR 7628, "Guidelines for Smart Grid Cyber Security."

IEEE 2030.2-2015 is a guide for the interoperability of grid ESSs. It discusses how discrete and hybrid energy storage systems can be integrated with electric power infrastructure. Clause 8 discusses security and privacy issues related to interoperability. Even though it is more specific than 2030–2011, it is still a high-level document that covers security issues, standards, security requirements, risk management, and security design. It contains examples of storage applications in bulk generation, transmission, distribution, and BTM, along with their data flows.

The DOE developed the Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline with NIST, NERC, and broad industry participation. The RMP is written with the goal of enabling organizations—regardless of size or organizational/governance structure—to apply effective and efficient risk management processes and to tailor them to meet their organizational requirements. Organizations can use that guideline to implement a new program within an organization or to build on an organization's existing internal policies, standard guidelines, and procedures.

6.3 Best Practices

This section and the following cover cyber security best practices across the data architecture within the energy storage system. While considerations should be analyzed across each component and connection within the data architecture, Figure 6-1 shows examples of how these risk mitigation strategies can be applied to relevant connections.

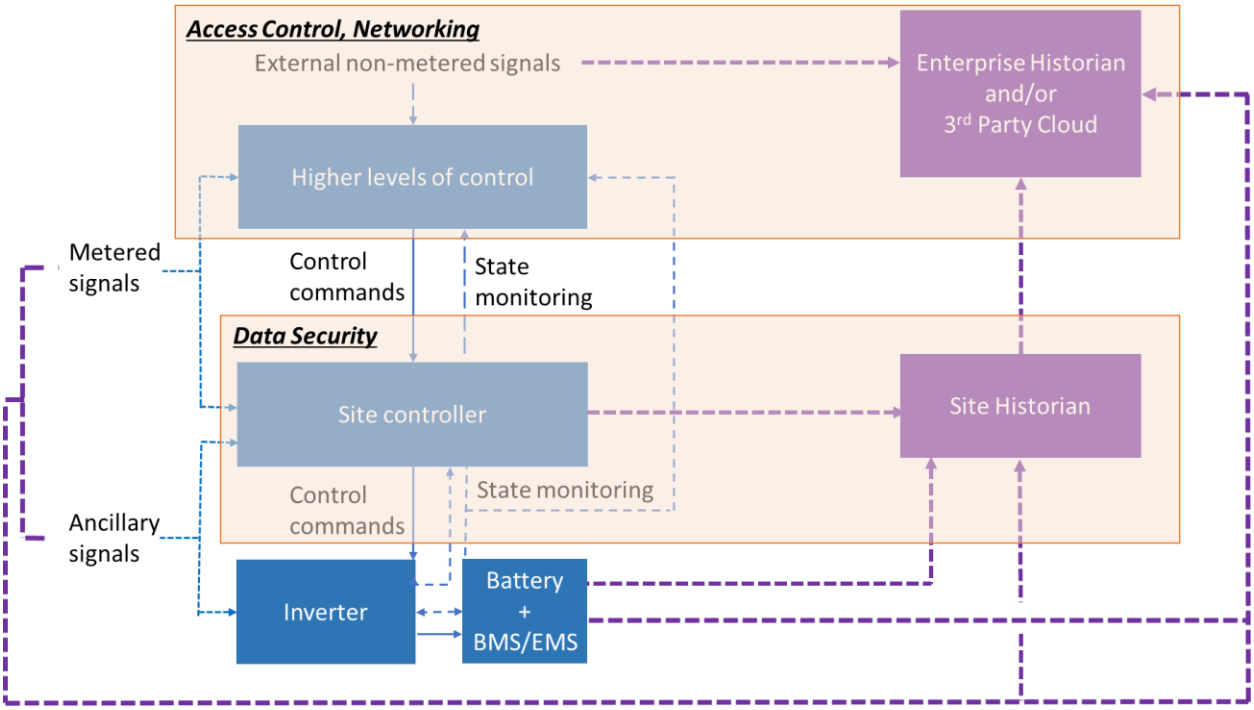

Figure 6-1
Cyber security risk mitigations across the energy storage data architecture

6.3.1 Physical Security

Physical security is usually associated with safety measures to protect people from hazards of physical processes (for example, electrical shock, chemical spills) or to limit the access of locations and devices to authorized personnel only. From the point of view of cyber security, physical access to Operational Technology (OT) and IT systems must be restricted to prevent digital access. Breaches in physical security could allow an attacker to exfiltrate sensitive data, introduce media or other unauthorized systems capable of communicating or eavesdropping, or even access human-machine interface systems.

Commonly used physical security controls include fences, gates, and locks. Systems that require authentication for allowing physical access, such as PINs, key cards, biometric, or even keys, should be employed.

6.3.2 Access Control

All electronic access to ESSs must be protected with an authentication mechanism. A recommended practice is to use a mechanism that employs user identification and a strong password or even multifactor authentication. This authentication should have a timeout to log users out after a certain period of inactivity.

6.3.3 Security of Data

Encrypted communications protect the confidentiality of data-in-flight and most current communications protocols support data encryption. However, there are still industrial communications protocols that do not support encryption, and some legacy equipment might not have the capability to support encryption either. If the need to encrypt communications is identified, bump-in-the-wire systems can be added to legacy equipment. It is recommended that communications over public networks should be encrypted, especially if sensitive information is involved. Stored sensitive data, data-at-rest, should also be protected by encryption.

Cryptographic algorithms such as hashing and digital signatures can be employed for verification of data integrity and origin (authentication). It is important to note, however, that data integrity verification using hashing is ineffective if the integrity of data is compromised before the hash is generated.

Another aspect of data security is to ensure removal of any utility-specific Personally Identifiable Information, unique device identification numbers, and data that may provide visibility into ESS operations. Data sanitization includes proper deletion from vendors and cloud services, and any devices after usage. More information on data sanitization, protection, and storage can be found in Section 2.11 of NIST SP 800-209.

6.3.4 Networking

Increased connectivity with ICSs, including data collection systems, exposes them to the risks that exist in IT systems. Improved network security is one way to mitigate those risks while ensuring system connectivity is maintained.

Network segmentation refers to the logical or physical separation of communications networks and is one way of mitigating network-related risk. It is a broad category that includes the use of firewalls, VPNs, proxies, or other networking technologies that minimize traffic between enclaves and isolate attacks. Network segmentation should be done based on the criticality of the given equipment.

The use of demilitarized zones (DMZs) is also encouraged. DMZs are segments of networks that separate them into an internal and an external part such that the traffic between these segments is isolated. Within ICS-type networks, such as utility-scale BESSs, it is recommended to have at least one DMZ between the enterprise network and the ICS network and another DMZ between the Internet and the enterprise network.

Firewalls are pieces of networking software or hardware that can segment a network by performing rule-based control of the traffic between network segments. Firewall rules allow the creation of network enclaves. The best practice is to block all traffic and only allow data from exceptions.

Unidirectional security gateways and data diodes have similar functionalities, allowing data flow in one direction. However, data diodes are hardwired for the directionality, whereas unidirectional gateways are devices that are configured to be unidirectional via software/firmware but have hardware that could potentially allow two-way communications. These devices can provide additional security to data collection systems by allowing data to flow out of the ESS only. Allowing data not to flow into an ESS prevents the injection of malicious data into the system, but it does not protect against eavesdropping. Data diodes are common in highly secured ICSs such as those of nuclear power plants. Furthermore, data diodes are relatively costly devices, so they might not be well suited for all applications.

6.3.5 Patching

Patching refers to the practice of updating a piece of software to correct for functionality problems or security vulnerabilities. Consequently, some form of patching is necessary for ensuring the security of systems. While remote and automated patching of systems is often a desired feature so that the most secure version of a piece of software is being used, ensuring that these updates are performed following cyber security best practices is key. Software downloads, including downloading patches, have been used to attack IT systems. Therefore, verifying the integrity and authenticity of patches is of utmost importance. Standard methods for verifying the integrity of firmware or software updates and security patches include hashes and digital signatures.

Patching ESS data collection systems can be challenging and will most likely require a scheduled outage. Systems that do not tolerate any downtime require more advanced patching schemes.

In addition to prompting system downtime, the patching process may lead to software modifications that alter how ESSs operate. Therefore, it is good practice to test the patched software before it is deployed. For instance, some utilities test software/firmware upgrades of their protection relays in a laboratory environment before upgrading the software of all relays in the field. In any case, it is important that product suppliers, operators, and operators of ESS have a clearly documented patching policy.

Very often, vulnerabilities are disclosed before patches are made available or it might not be possible to patch a system immediately. Therefore, it is important to develop plans to mitigate vulnerabilities if it is necessary to operate a given asset even though it is deemed vulnerable.

7
CREATING REQUIREMENTS DOCUMENTS AND SOLICITATIONS BASED ON DATA NEEDS

The successful integration of storage depends on clearly defining data infrastructure expectations. This includes defining the data needs, the communication and IT system-specific architectures, interoperability between systems, and the personnel and policies involved in the storage operation. Specifying this detail upfront, prior to contracting a storage system build-out or an off-take agreement from a third party, can alleviate many of the issues being seen with recent deployments. In many cases, specific data needs are not clearly defined prior to contracting and stakeholders then lack access to the necessary data once a system is made operational. Use Case and Requirements documents serve as a basis for creating these definitions, which then inform the Specifications documents used to procure a storage system (Figure 7-1). The following sections describe these three documents. Specific examples of detailed requirements associated with successfully integrated projects are presented in Appendix A.

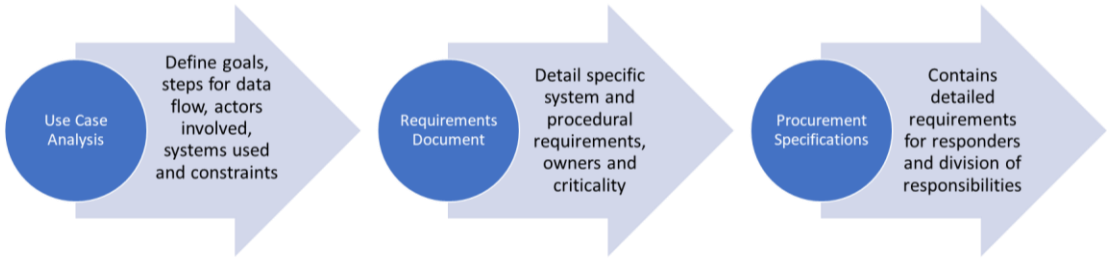

Figure 7-1
Energy storage project documents where data requirements should be defined

7.1 Interoperability

All aspects of system design can be assisted by consideration of existing and emerging efforts to standardize interoperability. The ISO definition of interoperability is "the ability of two or more systems or components to exchange information and use the information that has been exchanged in a meaningful way." Lack of consideration for interoperability can impede the flow of information between different devices. At the grid level, the GridWise Architecture Council has two decades of work related to interoperability. The **Modular Energy System Architecture (MESA) Standards Alliance** is also an industry association of electric utilities and technology suppliers. MESA's mission is to accelerate the interoperability of distributed energy resources (DER), in particular, utility-scale energy storage systems (ESS), through the development of open and non-proprietary communication specifications, based on standards. In November 2022, MESA announced that the MESA-DER De Facto Standard will be formalized into IEEE

Standard P1815.2. The MESA-DER standard "defines the mapping between the commonly-used utility SCADA protocol IEEE 1815 (DNP3) to the IEC 61850-7-420 DER information model."[21] These emerging efforts for interoperability should be considered when establishing requirements for a new project.

7.2 Use Case Documents

Use case documents can be used to define specific goals of the system (for example, specific applications like frequency and voltage control, peak shaving, renewables integration), who and what systems are involved in achieving the goals, and the information exchanged, to allow the goal to be achieved. The effort absorbs the input from all stakeholders to define specific steps to be taken in achieving each goal, including what information needs to be produced and received by each stakeholder.

IEC 62559-2:2015 presents a Use Case template and structure to define actors and how the actors are interrelated.[22] Depending on the location and size of the storage system, input will be required from operators, maintainers, engineering designers, IT personnel, management, and system planners. The Use Case analysis feeds into more detailed Requirements Documentation.

7.3 Requirements Documents

A Requirements Document details specific system and procedural requirements, owners of specific requirements, and criticality of execution. The ISO/IEC/IEEE 29148 standard serves as a template for developing a Requirements Document. This recommended practice "contains provisions for the processes and products related to the engineering of requirements for systems and software products and services throughout the life cycle. It defines the construct of a good requirement, provides attributes and characteristics of requirements, and discusses the iterative and recursive application of requirements processes throughout the life cycle."[23]

This Standard addresses requirements for a variety of perspectives related to the entire life cycle of a project, allowing specifications to address initial construction of the system and provisions through operational phases. These perspectives include:

- Business requirements
- Stakeholder requirements
- System requirements
- Software requirements

Robust documents also differentiate between Functional and Non-Functional requirements. Non-functional requirements describe how the system works, whereas functional requirements describe what the system should do. These structures allow for clear organization of the requirements and assignment of responsibilities for adherence to the requirements throughout the project life cycle.

[21] http://mesastandards.org/mesa-der-std/.

[22] https://webstore.iec.ch/publication/22349.

[23] https://standards.ieee.org/ieee/29148/6937/.

7.3.1 Requirements Document Specifics

The level of specificity in a Requirements Document can be closely tied to project success. Additionally, it is paramount that cyber security policies and structures on data flow, data access, and control actions be explicitly defined. Examples of processes that can be detailed include:

- What data points are needed to achieve the goals in the Use Cases?
- Who uses the data?
- What data transport systems are used to ship data to needed actors?
- How are data stored and accessed, and where are they accessed?

Examples of both Functional and Non-Functional requirements for energy storage data infrastructure are presented in Appendix A.

7.4 Procurement Specifications Documents

After the Use Cases and ensuing Requirements are defined, they need to be explicitly noted in Procurement Specifications or Solicitations to allow proposers to clearly understand the data acquisition system needs. If exceptions are taken to any part of the Requirements, they need to be addressed prior to any contract execution. A summary of what could be in the solicitation includes:

- What points/sensors need to be monitored
  - What is the associated timestamp granularity for each point?
  - What is the bandwidth requirement for data transport? (The Data Optimization Tool is available to determine this bandwidth based on points selected.)
- Who is monitoring?
- What systems are used to monitor or need to be put in place?
- How are data collected, and how often?
  - What data communication protocols (Modbus, DNP3, IEC61850 related, and so on) are used, and in what parts of the data transport system?
    - Where do protocols need to be translated, and how?
    - Where are timestamps placed on data fields?
  - How are discrete points mapped to data storage historian(s), and by whom?
- How are data stored temporarily on site?
- How are data shipped to a formal off-site historian/enterprise network?
- Specific cyber security policies in place
  - Equipment needs
  - Authentication requirements

8
CONCLUSION

Different storage stakeholders have different data needs. Data are used for tasks ranging from monitoring real-time system status to in-depth assessment of system health and degradation via analysis of very granular and large data sets. Meeting these needs from a given system requires a thorough understanding of who needs what data, how they get the needed data, and what they do with it. Additionally, many existing and emerging standards and policies further add to the data requirements.

Data needs can be systematically assessed in Use Case Analysis documents and then translated into formal Requirements documents. These documents can serve as the foundation for detailed Procurement Specifications. Specifying data needs prior to contracting a project will ensure access to the necessary data when a system is made operational.

In contrast to traditional grid equipment such as transformers, relays, breakers, and generating units, the long-term operating characteristics of storage systems are unknown. Stakeholders for all sizes of storage systems need to be cognizant of the benefit of accurate storage data and the consequences of not having correct data.

9
BIBLIOGRAPHY

1. DNP Users Group, “DNP3 Application Note AN2018-001 – DNP3 Profile for Communications with Distributed Resources,” January 2019. [Online]. Available: https://www.dnp.org/Resources/Document-Library?folderId=1261. [Accessed March 2019].
2. Energy Storage Association, “Energy Storage Technologies,” January 2019. [Online]. Available: https://www.energystorage.org. [Accessed March 2019].
3. American National Standards Institute, ANSI C12.1-2014 – Code for Electricity Metering.
4. American National Standards Institute, ANSI cv12.20-2015 – Electricity Meters – 0.1, 0.2, and 0.5 Accuracy Classes.
5. Schneider Electric White Paper, “Regulating Accuracy Impacts of Changes in ANSI C12.1 and ANSI C12.20.”
6. International Electrotechnical Commission. Available: https://www.iec.ch/homepage.

A
ENERGY STORAGE DATA INFRASTRUCTURE

A.1 Extract of NERC Draft Storage Reporting Requirements

Table A-1
NERC-required storage performance data

NERC Draft Reporting Variable	Description	Data Guidance	Data Source
Storage availability status	Active, Inactive, Mothballed or Retired	Could be extracted from a digital register, manually activated, but this field doesn't yet exist in data architectures.	EMS register if mapped; otherwise, manually or field tool sourced
Charge generation (MWh)	MWh of charge to the Energy Storage Group for the month being reported	Meter data need to be captured for the month; may require manual intervention or separate reporting logic.	EMS or site meter
Discharge generation (MWh)	MWh of discharge from the Energy Storage Group for the month being reported	Meter data need to be captured for the month (see above).	EMS or site meter
Charging hours	Number of charging hours to the Energy Storage Group for the month being reported	Reporting system needs to be able to count hours the meter moves in charging direction; may not be a discreet point in standard control architecture and would need to be derived from applied logic to meter data.	Site Meter or EMS or Historian if timing counter is built in, or via logic applied to historian
Discharging hours	Number of discharge hours from the Energy Storage Group for the month being reported	Reporting system needs to be able to count hours meter moves in discharging direction (see above).	EMS if timing counter is built in, or via logic applied to historian
Forced outage hours	Number of hours that the Energy Storage Group is in a forced outage state	If an alarm stops the system, there may be counters (Time Windows) in the control architecture, but these may need to be developed as they aren't present in many architectures.	EMS if timing counter and associated register indicating forced outage is built in, or via logic applied to historian

Table A-1 (continued)
NERC-required storage performance data

NERC Draft Reporting Variable	Description	Data Guidance	Data Source
		Field experience with early systems has shown that even minor components can force a system outage that lasts days or weeks as field response capabilities may be slow and parts availability scarce.	
Maintenance outage hours	Number of hours that the Energy Storage Group is in a maintenance outage state	Assuming this is unplanned (not delineated by NERC), it may have to be manually tabulated unless control architecture can accommodate a maintenance mode specifically and count hours. If the outage causes loss of communications, manual intervention could be required. This value has been very high in early systems, sometimes lasting days to weeks as field response capabilities were immature or parts not available even with planned events.	EMS if timing counter and associated register indicating maintenance outage is built in, or via logic applied to historian
Planned outage hours	Number of hours that the Energy Storage Group is in a planned outage state	May be distinguishable from Maintenance Hours above – clarity by NERC is needed to distinguish.	Source TBD based on definition clarity from NERC

Table A-2
NERC voluntary storage performance data

NERC Draft Reporting Variable	Description	Field Experience	Data Source
OMC (Outside Management Control) forced outage hours	Number of hours that the Energy Storage Group was in a forced outage state due to OMC causes. This is a subset of forced outage hours.	This will require manual intervention to delineate between OMC outages and forced outages.	EMS if timing counter and associated register indicating OMC forced outage is built in, or via logic applied to historian – logic needs to be able to discern between forced and OMS forced outage (based on origin of alarms triggering outage).
OMC maintenance outage hours	Number of hours that the Energy Storage Group was in a maintenance outage state due to OMC causes. This is a subset of maintenance outage hours.	This needs interpretation and manual intervention to report.	This may need to be manually logged due to complexity of distinguishing between OMC forced outage and maintenance hours.
OMC planned outage hours	Number of hours that the Energy Storage Group was in a planned outage state due to OMC causes. This is a subset of planned outage hours.	This needs interpretation and manual intervention to report.	This may need to be manually logged due to complexity of distinguishing between OMC forced outage and planned maintenance hours.

Table A-3
NERC-required event data

NERC Draft Reporting Variable	Description	Field Experience	Data Source
Event start date	Time mm/dd/yyyy HH:MM	Timestamp dictates a logical reporting system to capture time, including hours, minutes. This may have to be manually triggered or logged.	EMS alarm timestamp.
Event end date	Time mm/dd/yyyy HH:MM	See above.	EMS normal condition register timestamp.
Event type	Forced, maintenance, planned	May require manual intervention and determination.	Manually input, or derived from field reporting tool which also requires manual input.
Cause code (needs review)	Selected from an extensive list broken down into Balance of Plant (storage is presently considered Balance of Plant to the PV hybrid system), external, personnel, or procedural errors	This list could become extensive – at present it is not tuned to storage systems but is rather a compilation of legacy causes from other generation units.	See above.
Contributing operating condition	The underlying environment (storm, flood, cold weather)	May require manual intervention and determination.	See above.
MW output (may be PV output) at time of event	(Net actual capacity)	Requires automated capture of MW at time of event.	MW register at same timestamp as alarm (see above).
Production supplied by energy storage (MWh)	Number of MWh of generation that energy storage supplied during the event	This requires automation to determine. May be indicative of storage supporting the grid during a PV outage in a hybrid system.	Needs to tie EMS MW register to stop and start times of PV event (needs clarification).

Table A-4
NERC outage detail reporting (mostly tuned to PV)

NERC Draft Reporting Variable	Description	Field Experience	Data Source
Number of forced occurrences	Number of forced outages associated with the Equipment Outage Detail Code	This must be manually logged or logged through a field O&M data collection tool similar to what EPRI ESIC is developing. The tool would need to be designed to count instances of occurrences.	Field data collection tool (preferred).
Number of maintenance occurrences	Number of maintenance occurrences associated with the Equipment Outage Detail Code	See above.	See above.
Number of planned occurrences	Number of planned outage occurrences associated with the Equipment Outage Detail Code.	See above.	See above.

A.2 IT Requirements Sample

The following is excerpted from the DOE/EPRI 2013 Electricity Storage Handbook in Collaboration with NRECA[24] Appendix C. Note the differentiation between Functional, Non-Functional Performance, and User Interface Requirements. The Handbook also includes many other requirements, which in themselves were excerpted from an actual requirements document conducted by PNM. It should be noted that these requirements dictated specifications, which in turn allowed for successful on-time, on-budget commissioning of the associated storage system.

[24] DOE/EPRI *2013 Electricity Storage Handbook* in Collaboration with NRECA, SAND2013-5131, July 2013.

Table A-5
Functional requirements sample

Requirement	Owner	Critical
The solution shall provide a method for **retrieving specific data** from solar and battery technology source systems that will be located at the storage site, which are itemized in the Interface Requirements section of this document. *Note: Refer to Points List in Appendix.*	UTILITY	x
The solution shall provide a method for **receiving specific data** from over __collection points from various devices located at the site.	UTILITY	x
The solution shall extract data from sources in regular **intervals** ranging from 1 second to every 60 seconds, depending upon stakeholder requirements.	UTILITY	x
The solution shall provide a method for **storing** acquired data from source systems at the site, for a period of time to be defined by the user.	UTILITY	x
The solution shall provide a method for **transmitting** data in 15 minute intervals (or less depending on stakeholder requirements) from a site database to an offsite storage and reporting database.	UTILITY	x
The solution shall provide a method for **storing** extracted data offsite for a minimum of __ years from the date of solution implementation.	UTILITY	x
The solution shall provide a method for **archiving** all stored data into a secondary storage location, at a user-selected time cycle such as every 30 days, quarterly, annually, etc.	UTILITY	x
The solution shall provide a method for **retrieving archived** data within 24 hours of the request for retrieval.	UTILITY	
The solution shall provide a method for setting varying **retention** schedules on specified datasets in both the production storage database and the archived storage database.	UTILITY	
The solution shall provide a method for users to retrieve, display, and otherwise **make available** all data stored in the production database, subject to authorized user permissions and UTILITY's Security Requirements.	UTILITY	x

Table A-5 (continued)
Functional requirements sample

The solution shall provide a method for **authorized vendors** and other external parties to access appropriate systems and resulting datasets, from a point outside the company's network (through a server in the DMZ), subject to UTILITY's Security Requirements.	UTILITY	x
The solution shall provide a method for authorized internal users to create, generate, and produce user-designed **reports** on demand (monthly, quarterly, annual, etc.) subject to UTILITY's Security Requirements.	UTILITY	X
The solution shall perform **time synchronization** functions on all data reads from the devices at the server level and time stamps at the device or gateway level.	UTILITY	
The solution shall be capable of **grouping and segregating** stored records by specific data fields and record characteristics including, but not limited to, the following categories as applicable to the source device: • Operational vs. analytical • Operational vs. financial • Public vs. private • Vendor proprietary and confidential • Identify which data columns are available to user-selected internal and external entities. • Baseline vs. actual achieved operation (for purposes of economics and costing).	UTILITY	x
The solution shall be capable of allowing users to **select and query** data by specific fields and record characteristics including, but not limited to, the following categories as applicable to the specific data type: • Date/time ranges of all data reads. • Test modes in operation at time of read. • PV and Battery configuration settings at time of read. • Weather conditions at time of read.	UTILITY	x

Table A-6
Performance requirements sample

Requirement	Owner	Critical
The solution shall be capable of extracting, transmitting, and storing an estimated __ **million records per day** from pre-identified collection points. *Estimated calculations*: 60 seconds * 60 minutes = 3600 seconds in one hour 3,600 seconds * 24 hours = 86,400 seconds in 24 hours 85,400 seconds * ___ sites = _____ records per day.	UTILITY	x
The solution shall be capable of retrieving, storing and forwarding an estimated 100 byte record length, including all measurements and settings. **Assumptions** Record Length = __ bytes Number of data collection points = __ Reads per minute = __	UTILITY	x
The solution shall be capable of handling the following site data volumes and velocities, based on the assumptions listed in Requirement 3.3.2. **Volumes & Velocities** Records per second = ____ Bytes per second = ____ Records per 15 minutes = ____ Records per hour = _____ MBytes per 15 minutes = ___ MBytes per hour = ___ Hours per day operation = ___ MBytes per day = ____	UTILITY	x
The solution shall be capable of storing and managing data at the following estimated volumes, based on the assumptions listed in Requirement 3.3.2. **Anticipated Storage Volumes** Gbytes Per month(raw data) = _____ Gbytes per year (raw data) = _____ Est DB storage per month (GB) = _____ Est DB Storage per year (GB) = _____	UTILITY	x

Table A-7
Hardware interfaces requirements sample

Requirement	Owner	Critical
The solution must interface with **source devices** that will produce readings that will be interrogated for data acquisition. Source devices include, but may not be limited to: • UTILITY Metering • PCS Controller • Other Sensors • Meteorological stations (wind, temp, etc.)	UTILITY	x
The solution shall include a _____ protocol interface in the solution, which will interface with various source devices at the site.	UTILITY	x
The solution shall **interrogate** source devices at specified internals listed in the Preliminary Data Points document in Appendix, capturing and storing data in one database at the physical site.	UTILITY	x
The solution shall transfer data from the physical site database to _____(location), using ____**(network description)**	UTILITY	x
The solution's communication lines shall be capable of handling a minimum of _____ of transmission per hour.	STORAGE MFTR	x
The storage system utilizes _____ for maintenance and must be supported.	STORAGE MFTR	X
The storage system utilizes _____ for data logging, and must be supported.	STORAGE MFTR	X

About EPRI

Founded in 1972, EPRI is the world's preeminent independent, non-profit energy research and development organization, with offices around the world. EPRI's trusted experts collaborate with more than 450 companies in 45 countries, driving innovation to ensure the public has clean, safe, reliable, affordable, and equitable access to electricity across the globe. Together, we are shaping the future of energy.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

3002025977

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

SANDIA NATIONAL LABORATORIES
Albuquerque, New Mexico 87185 and Livermore, California 94550