Grid Modernization Initiative

Grid Management System Architecture

February 1, 2016
Acknowledgment and Disclaimer Statement

This technical report was prepared by Southern California Edison Company (SCE) and is based on a project undertaken by SCE to address ways of modernizing SCE’s grid to meet emerging needs, including those associated with the use of distributed energy resources (hereafter, the “Project”). SCE acknowledges the contributions of a team of individuals as participants in this Project, including:

David Bass
John Bubb
Michael Garrison Stuber
Erich Gunther
Doug Houseman
Chris Knudsen
Jeremy McDonald
Ricardo Montano
Clint Powell
Peter Reed
Greg Robinson
Ron Sellemi
Steve Van Ausdall

This Project was undertaken using reasonable care and in accordance with professional standards. However, neither SCE nor any individual or entity involved with this Project is making any warranty or representation, expressed or implied, with regard to this report, the merchantability or fitness for a particular purpose of the results described herein, or any analyses, information, or conclusions contained in this report. The results reflected in this report are generally representative of the operating conditions on SCE’s electric grid; however, the results in any other situation may vary depending upon particular operating conditions.

This report is copyrighted by SCE. SCE hereby grants other electric utilities, and those advising or regulating such entities, with a limited license right to review this report, make limited copies related to such review, and use the report to evaluate whether the approach used by SCE, as described herein, is likely to be useful to them in the performance of their own independent grid assessment. SCE does not, however, accept any liability for any use of this report or information contained in this report. Other uses of this report require permission from SCE.

© 2016 Southern California Edison Company
# Table of Contents

1. Introduction ................................................................................................................................. 1
2. Purpose of this Document ............................................................................................................. 2
3. Scope ........................................................................................................................................... 3
   3.1 System Purpose ......................................................................................................................... 3
   3.2 System Description ..................................................................................................................... 4
   3.3 Services Definitions ................................................................................................................... 8
   3.4 Services Domains ..................................................................................................................... 9
   3.5 Domain Interactions .................................................................................................................. 10
   3.6 Architectural Characteristics ................................................................................................. 12
   3.7 Architectural Constraints ......................................................................................................... 16
4. System Decomposition .................................................................................................................. 17
   4.1 Reliability System ..................................................................................................................... 17
   4.2 Optimization System ............................................................................................................... 20
   4.3 Planning System ....................................................................................................................... 23
   4.4 Economics System .................................................................................................................... 27
   4.5 Grid Infrastructure Management System .................................................................................. 30
   4.6 Data Repository System .......................................................................................................... 34
   4.7 Communication System .......................................................................................................... 37
   4.8 Integration System .................................................................................................................... 40
   4.9 Combined Systems View ......................................................................................................... 43
5. Domains ....................................................................................................................................... 44
   5.1 Central Domain ......................................................................................................................... 44
   5.2 Distributed Domain .................................................................................................................. 46
   5.3 Edge Domain ............................................................................................................................ 47
6. Design Principles .......................................................................................................................... 50
   6.1 Safety and Compliance ............................................................................................................. 50
   6.2 Standards & Application Specific Profiles (ASP) .................................................................... 50
   6.3 Intelligence ................................................................................................................................ 51
   6.4 App Architecture ...................................................................................................................... 51
   6.5 Common Dataset ...................................................................................................................... 51
   6.6 Pre-Calculation ......................................................................................................................... 51
   6.7 Groups & Regions ..................................................................................................................... 51
   6.8 Performance .............................................................................................................................. 52
   6.9 Data Validation .......................................................................................................................... 52
6.10 User Interface Portability .................................................................52
6.11 Usability ......................................................................................52
6.12 Maintainability ...........................................................................52
6.13 Modularity ..................................................................................53
6.14 Reusability (Ability to Call) .......................................................53

7 Cybersecurity ..................................................................................53
7.1 Security Principles ........................................................................53
7.2 Controls .......................................................................................54
7.3 Shared Cybersecurity Subsystems .............................................56
7.4 Risk Based Approach .................................................................58

8 Data Architecture ............................................................................58
8.1 Data Mappings & Lifecycle ..............................................................58
8.2 Data Frequency and Periodicity ....................................................58
8.3 Partitioning ..................................................................................59
8.4 Formats .........................................................................................60
8.5 Technologies ................................................................................60
8.6 Conceptual Data Types ...............................................................60
8.7 Model Characteristics .................................................................61

9 Next Steps .......................................................................................62

10 Glossary .........................................................................................63
1 Introduction

Over the last decade, breakthroughs in distributed generation, energy storage, electric transportation and micro-grid technologies, known collectively as Distributed Energy Resources (DERs)\(^1\), have made it increasingly possible for customers to use these technologies to locally generate, store, and manage power at their premises. These customers use DERs to increase the availability and, in some cases, quality of their electricity while benefiting economically through tariffs and programs designed to incent the adoption of DER technologies. The accelerating adoption of DERs across our distribution networks challenges the operational tenets historically used to plan, design, operate, and maintain the electric grid.

Shifting from central management of one-way power flows supplied by relatively few bulk generators to coordinating large numbers of DERs creating two-way power flows may cause grid stability issues. Wide-spread two-way flows will diminish the ability of human operators to prevent cascading events across the distribution system and, potentially, even the bulk electric system. As DER adoption grows, the number of possible control actions will increase and the time to execute those control actions will decrease beyond the capability of human grid operators to react to events on the electric grid. Safety and reliability issues will increase in both frequency and magnitude unless advanced technologies, deployed as part of an actionable grid modernization strategy, are used to stabilize our electric grid.

Furthermore, the electrical commodity markets are accelerating and changing radically with direct impact on the operation and design of the grid. In the 1970s, few electricity markets existed; trading of electricity between utilities was typically done by trading megawatt-hours. Demand Response that existed was direct load control and had a different regulated tariff. In the 1990s, electricity markets began to evolve with movement to wholesale energy pricing and ancillary services. The Regional Transmission Organizations (RTO) and Independent System Operators (ISO) came into existence. Demand Response incentive payments based on participation and performance were instituted. Recently, there has been a push to further evolve the market, moving from a wholesale and incentive-based market to a retail market with many possible aggregators and participants, with each aggregator, retailer, and service provider creating their own programs and contracts.

To meet these challenges, Southern California Edison (SCE) has developed a comprehensive grid modernization strategy and should facilitate the cultural shifts, shorter development cycles, and cohesive strategic alignment across SCE to provide affordable, reliable, and safe power with an electric grid dominated by DERs.

In response to SCE’s Grid Modernization Strategy\(^2\), SCE’s Enterprise Architecture team has been actively engaged in the solicitation and definition of business requirements and the development of a corresponding Concept of Operations that frames the desired modernization capabilities. Building on that progress, this document provides the architecture for a new Grid Management System (GMS) and the various components it requires to adequately meet the emerging needs of the SCE grid.

\(^1\) The complete array of DER is defined in CPUC guidance document for the California utility Distribution Resource Plans (DRP). It includes Distributed Energy Resources such as wind and solar generation, and energy storage, as well as energy efficiency and demand response. It does not specifically call out microgrids; however, we have included them here as collections of DER that operate together with the ability to island as this capability is important to inform the architecture definition. [http://www.cpuc.ca.gov/WorkArea/DownloadAsset.aspx?id=5108](http://www.cpuc.ca.gov/WorkArea/DownloadAsset.aspx?id=5108)

2 Purpose of this Document

This Architecture Definition Document (ADD) is the deliverable for the core architectural artifacts developed for SCE’s future Grid Management System (GMS) and in response to the Grid Modernization strategic initiative.

The GMS is based on an architecture and guiding principles that allow us to proactively support changing requirements minimizing disruption to existing operations, consumer commitments, and regulatory requirements. Recognizing that no one can predict all of the changes coming to our industry, nor can they be implemented all at once, the GMS and its underlying architecture are being designed to allow incremental deployments and transition from legacy systems.

The Architecture Definition Document spans all architecture domains (Business, Information, Application, Technology, and Security) and also examines all relevant states of the architecture (baseline, interim state(s), and target).

The Architecture Definition Document is a companion to the System Requirements Document (SRD), with a complementary objective:

- The Architecture Definition Document provides a qualitative view of the solution and aims to communicate the intent of the architects
- The System Requirements Document provides a quantitative view of the solution, stating measurable criteria that must be met during the implementation of the architecture

This Architecture Definition Document provides a vision for the expanse of capabilities that are needed to realize the 21st century electric system. Many of the capabilities described in this document are foundational to enabling DERs while others depend on the level of participation of DERs in providing grid services as well as the mechanisms to compensate them. SCE, in parallel to the creation of the ADD and Architecture, is issuing Request for Information (RFI) and Request for Procurement (RFP) documents that will inform this work and procure solutions that will become key foundational pieces of the GMS. This document will continue to evolve as SCE continues to update priorities on needed capabilities.

Intended Audience

This document contains systems engineering content and is intended for technical audiences. Non-technical audiences will find that the initial chapters of the document describe a design philosophy that supports the active operation of the distribution grid to support high levels of distributed generation (e.g. more than 50% of total energy consumed), large amounts of customer owned storage, and high levels of demand response. This philosophy will impact business processes, staffing, and tariffs. Non-technical audiences can benefit from reading sections 1 through 4 to understand some of the key philosophical decisions and needed capabilities.
3 Scope

3.1 System Purpose

The Purpose of the Grid Management System (GMS) is to provide an integrated set of operational functions that allow SCE to operate the electrical grid with enhanced situational awareness, automation, reliability, and safety, in a growing Distributed Energy Resources environment. The GMS will also provide advanced analysis capabilities that enable it to manage the distribution network in conjunction with the decisions made by customers and third parties, within the limits provided by the grid-connected equipment, and in the environment the grid is operating in at the time.

The GMS is needed to support:

- The growing installation of distributed generation, distributed storage, energy efficiency, and customer equipment that can respond to demand response signals to turn on and off (all controllable DER)
- The growing complexity of the California energy market, including prices communicated directly to end consumer DER equipment
- The desire to run the distribution and transmission infrastructure closer to its capacity margin
- The highly dynamic two-way power flow in the distribution grid
- The desire for a higher level of reliability and power quality for customers
- The ability to support customers creating micro-grids which can be islanded by the owners, leaving or joining the grid based on customer decisions
- The accurate forecasting by location of the total load on the system, the available power from distributed generation, the amount of energy available in storage, and the available demand response based on market conditions, weather, equipment status, customer decisions, and other internal and external factors
- The ability to provide operators with transmission-like contingency options that reduce the impacts to customers due to shifting grid conditions
- The management of the grid based on multi-objective optimization, including but not limited to customer values, grid capacity, economics, equipment life cycle, reliability, and lowest impact to the environment

The GMS will operate in three time continuums:

1. The future, to support forecasting, grid planning, and other services that need to know what will happen (or a range of scenarios for what is probable) to maintain the grid in a prudent fashion.
2. The current, which varies in interval depending on the actions that need to be taken (e.g. relaying has a very short operations interval, while a tag out for maintenance might have a longer operations interval).
3. The past, which allows the system to provide fault locations and identify wear and tear on equipment for use by operators and external systems for assets management, billing, and other business related services.

Figure-1 shows the GMS in its context within SCE, interacting directly with the electric system to provide reliability, optimization, and planning capabilities to the enterprise, while supporting other organizational activities through business systems. Overall, these activities can be seen as a stack that encompasses all of the activities of a utility.
External systems provide additional context that is required by the GMS to function well. This includes existing SCE systems such as the Work Management System (WMS) and Geographic Information System (GIS), as well as third party systems such as environment/weather data systems, the bulk electric system, market systems, and service provider systems.

GMS Users are SCE personnel that interact with the GMS. This includes operators, engineers/planners, and technicians.

**Operators:** are SCE personnel who manage the electrical network via the GMS, as well as personnel that manage the GMS and its associated communications infrastructure.

**Engineers/planners:** use the GMS to inform longer-range design and planning activities.

**Technicians:** interact with the GMS when deploying, configuring, troubleshooting, repairing, or removing pieces of the electrical network, or the associated communications and computational infrastructure with it.

![Diagram of Grid Management System Architecture](image)

**Figure-1**

### 3.2 System Description

The GMS is a system of systems that interacts with the electrical grid, encompassing all of the activities necessary to modernize the grid, including distributed energy resources management, distribution grid operations, and planning functions. It provides advanced communications and the intelligence necessary to manage the electrical grid as a fully integrated network, which allows the injection and delivery of energy at any point, rather than treating it as a unidirectional distribution system. Such an integrated model allows the optimal use of available resources to meet both reliability and cost priorities in a coordinated fashion.

#### 3.2.1 System Composition

The eight systems (summarized in Table 1) interact across the physical and logical domain boundaries of the distribution network. Such interaction is enabled through a collection of integrated services (discussed further in section 3.3) so as to ensure that grid management and operational functions are performed properly and optimally.
Grid Management System Architecture

<table>
<thead>
<tr>
<th>Grid Management System (GMS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
</tbody>
</table>

Table-1

3.2.2 System Details

An operational definition of each one of the eight systems in the GMS is given below.

3.2.2.1 Reliability System

The Reliability system provides the fault detection, fault isolation, and system restoration capabilities of the GMS. This includes real-time, proactive monitoring of the distribution network; real-time situational awareness of system-wide voltage, power, phase angle, impedance, and frequency, as well as outages, equipment failures, and cyber-security events; sub-cycle monitoring of harmonics, sags, and swells, including the detection of equipment failures and system faults; determining and recommending grid asset/ equipment settings; and the ability to automatically detect, identify, locate, and isolate faults. The Reliability system works in both centralized and distributed configurations and in conjunction with microgrids, islanding, and distributed energy resources.

3.2.2.2 Optimization System

The Optimization system coordinates the activities of the distribution network, and distributed energy resources linked to the network, in the most efficient way possible, balancing electrical efficiency, reliability, and market efficiency. The Optimization system facilitates proactive management of the
distribution grid, including power flow optimization and dynamic use of inverters for phase balancing and Volt/VAR control, as well managing to specific objectives, such as reducing greenhouse gas emissions. The Optimization system supports both system-wide optimization, coordinating with the transmission / bulk electric system, and sub-circuit optimization, in which individual elements are coordinated to maximize the value of DER. The Optimization system works independently of the current configuration of the electrical network, and thus continues to function even when portions of the grid are disconnected, optimizing both the islanded and connected portions. The Optimization system coordinates the transitions between being islanded and connected, and ensures that they are both efficient and seamless. The system also supports predictive capabilities, allowing the operator to anticipate, plan for, and respond to contingency scenarios.

3.2.2.3 Planning System

The Planning system guides the evolution of the electrical network. Specifically, it provides information about how the distribution network is being used, including which areas are growing, which are stressed, and which are under-utilized. The Planning system includes reliability, optimization, and market trends to ensure that a complete view of the needs of the distribution network is considered. This information informs growth projections of both electricity consumers and distributed energy resources, providing SCE with a solid foundation on which to make capital allocation decisions. The Planning system supports not only the traditional planning functions of the utility, but also supports the ability to aggregate data both in time and by location to allow load profiles to be created for any arbitrary node (e.g. transformer, substation, recloser, etc.) and for any arbitrary time period that the user wishes to look at. It will allow exports of the underlying electrical model into simulation and grid design packages to allow planners to create capital investment scenarios, upgrade scenarios, and to do long cycle maintenance planning.

3.2.2.4 Economics System

The Economics system provides correlation between the operations of the distribution network, and the electricity market. This includes alignment with wholesale market policies from the California ISO and other interconnections, and coordination with distribution level DER that may be represented or controlled by 3rd party aggregators. The Economics system supports flexible control mechanisms, such that DER may be market controlled (e.g. driven by price signals), until it reaches a point at which it must be overridden for reliability reasons. The Economics system must maintain respect for ownership boundaries, while allowing the GMS to ensure the safe, reliable operation of the distribution network at all times. Should a distribution level (retail) market or a peer-to-peer market be created in California, the Economic system will have the underlying design to support either construct. This includes wires charges for peer-to-peer markets should they come into existence.

3.2.2.5 Grid Infrastructure Management System

The Grid Infrastructure Management system manages both the IT and OT aspects of the GMS. The Grid Infrastructure Management system manages the computational and communications infrastructure components of the GMS and provides a unified operations console. As discussed later in this document, the GMS is deployed across three deployment domains (Central, Distributed, and Edge). The Grid Infrastructure Management system ensures that the communications systems and computing environments are running properly and efficiently. Management includes asset and configuration inventory, control and retention, plus network discovery as required.

With respect to Information Technology, the Grid Infrastructure Management system monitors communication network performance and faults, providing warning and, where possible, automatic mitigation of communication network faults and congestion. It also monitors computing resources, tracking metrics such as CPU utilization, available RAM, and available storage, to ensure that GMS components are neither misbehaving, nor being starved of necessary resources. Furthermore, the Grid
Infrastructure Management system provides the capabilities for zero-touch provisioning of devices, managing software/firmware implementations, management of virtual resources, database resources, system logging, and integration services, as well as the deployment and monitoring of security parameters.

With respect to Operations Technology, the Grid Infrastructure Management system provides tools to manage the operational systems of the GMS in a holistic, unified manner. The Grid Infrastructure Management system supplies the operator a comprehensive view of the operational activities of the GMS, including resource loading, operational mode, and current tasks.

3.2.2.6 Data Repository System

The Data Repository system serves as the historian and librarian of the GMS, providing SCE users and external systems access to time series data and salient records of its performance and activities. The Data Repository is specifically a centralized system, providing an archive for selected data, which is preserved with integrity for the long term. (Note: selecting which data is recorded in the repository is a function of system design, not an automated process). The Data Repository allows the GMS to provide information to regulators, executives, and analysts. The Data Repository enables data-mining and analysis of information whose current value may not be identified or understood, as well the production of standard data sets required by the business and by regulators. However, the Data Repository is not, itself, a data mining system. Data mining will be performed by specialized tools using data extracted from the Data Repository. Use of the Data Repository by external systems and users will comply with all regulatory requirements.

3.2.2.7 Communication System

The Communication system employs a “Communication Fabric”, which interconnects across all systems and provides services to each application based on its specific requirements, including throughput, latency, security, reliability, and coverage. The specific technology components of the system can be segmented into an extensible set of tiered services, where each service will provide a particular level of performance. Technologies and tiers will be overlapping. Specific technologies will be selected and/or defined for each tier and different applications can be mapped to one or more of the tiers depending on their needs.

3.2.2.8 Integration System

The Integration system facilitates the logical, flexible, extensible interconnection of the components that comprise the GMS. In practice, the GMS will be made of many different technologies, sourced from different vendors, including custom components, commercial-off-the-shelf products, and legacy systems. The integration system will provide the marshalling, brokering, queuing, and data translation services necessary to integrate these components. The integration system will be required when GMS components do not share the same data-model, but may also be involved in other transactions or inter-system interactions when its inclusion makes the system more flexible, extensible, or manageable. The integration system spans the three domains (Centralized, Distributed, and Edge) of the GMS, integrating components both within and between those domains.
3.3 Services Definitions

Services are the base level building blocks of the GMS. They provide a common set of low-level operational functions across all of the systems. The GMS provides five core services as follows:

- **Monitor** – a service that obtains internal and external data for system operations
- **Control** – a service that processes system data for the purpose of actuation
- **Analyze** – a service that applies a method to data in order to produce derivative data
- **Exchange** – a service that facilitates the import and export of data
- **Persist** – a service that stores system data

The **Monitor** service is the mechanism whereby the GMS obtains dynamic information about grid system activities. This includes sensing, measurement, and data acquisition both regarding the electrical network and the communications infrastructure that facilitates the other data services. Monitoring also extends to receiving dynamic data from external systems, such as environmental systems and market systems that provide data on weather and price.

The **Control** service is a system that processes data in order to make actuation decisions. Data may originate from any of the Monitor Services, as an output of the Analysis Service, or can be locally derived from control algorithms based on any combinations of available data.

The **Analyze** service creates insights and derived data from the data obtained through the other services. Analysis may happen over different time horizons, including the relatively short windows of computing the impacts of the day-ahead and hour-ahead markets on the expected load within the system, or afternoon cloud-cover estimates on photovoltaic generation capabilities, as well as long-term windows, such as determining where network investment should be made.

The **Exchange** service provides mechanisms for efficient, at scale, import and export of data to and from external services. Such services may include reporting, external information sources, input of configuration information, and the Bulk Electric System.

The **Persist** service stores all forms of system data in a format that is highly extensible, has the ability to ingress and egress needed data at the rates necessary to support other services, and most importantly, provide a mechanism to maintain master data for the GMS System. The service also provides for data integrity, redundancy, and relevant-time disaster failover.

**Figure-2** below depicts the logical organization of the GMS core operational services and the interaction flows with the users and external systems (both within SCE and outside SCE). The Monitor, Control, and Exchange services use the Communication system to interact with external systems. While the Control and Exchange services interact bi-directionally with external systems, the Monitor service is unidirectional, as the external systems will not be allowed to monitor SCE grid assets. Internal SCE users will interact with the GMS through a user interface layer.
3.4 Services Domains

The services that comprise the GMS will be realized across three primary domains:

- Centralized
- Distributed
- Edge

The **Centralized** domain is the data center environment operated by SCE, or on SCE’s behalf in the cloud. The Centralized environments are few in number (tens), relatively easy to update, have shorter infrastructure lifetimes (three to five years), extensive processing power, and effectively unlimited bandwidth.

The **Distributed** domain is provided by infrastructure in the middle of the communications and electrical systems. This includes equipment in substations, poles, and underground vaults. The Distributed domains are larger in number (thousands), require medium levels of effort to update, have intermediate infrastructure lifetimes (five - fifteen years), have intermediate levels of processing power, and bandwidth which varies from a fiber optic link to the equivalent to a cellular data connection.

The **Edge** domain is provided by infrastructure at the edge of the network. This includes transformers, reclosers, cap-bank controllers, meters, and the like. The Edge domain is not segmented by element ownership. Any device that can be controlled by the GMS is assumed to be within the boundary of the system. For example, a residential PV system may be owned by the customer but the interface to the
GMS system allows the device to be controlled to effect DER load balancing. The Edge environments are multitudinous in number (millions), require high levels of effort to update, have extended equipment lifetimes (fifteen years or more), may have very low levels of processing power, and may have bandwidth equivalent to a dial-up modem link.

*Table-2* below summarizes the GMS domain characteristics with examples.

<table>
<thead>
<tr>
<th></th>
<th>Centralized</th>
<th>Distributed</th>
<th>Edge</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location</strong></td>
<td>Data Centers</td>
<td>Substations, pole tops, and other intermediate network points</td>
<td>End devices (e.g. reclosers, meters, enrolled customer devices [PV])</td>
</tr>
<tr>
<td><strong>Quantity</strong></td>
<td>Tens</td>
<td>Thousands</td>
<td>Millions</td>
</tr>
<tr>
<td><strong>Ease of update</strong></td>
<td>Easy</td>
<td>Moderate</td>
<td>Challenging</td>
</tr>
<tr>
<td><strong>Expected lifespan</strong></td>
<td>3-5 years</td>
<td>5-15 years</td>
<td>15+ years</td>
</tr>
<tr>
<td><strong>Processing Power</strong></td>
<td>Effectively unlimited - Servers</td>
<td>Equivalent to current smartphones / PCs</td>
<td>Typically a limited embedded device</td>
</tr>
<tr>
<td><strong>Bandwidth</strong></td>
<td>Effectively unlimited gigabits+</td>
<td>gigabits to hundreds of kilobits</td>
<td>megabits to bits</td>
</tr>
</tbody>
</table>

*Table-2*

3.5 **Domain Interactions**

In order to accommodate the variety of system use cases and to ensure proper governance, it is important to define the allowed interactions between the three domains, external systems, and the users. As shown in *Figure-3*, the following approach has been devised:

1. Exchange with external systems will only occur through the Central domain.
2. Users may interact with any or all of the three domains (Central, Distributed, and Edge).
3. The Distributed and Edge domains will not have the Exchange service.
4. The Central domain can interact with the Distributed and Edge domains either directly or through either the Central or Distributed integration system.
5. Services within any of the three domains can use the integration system (for intra-domain interactions).

---

3 Note: it is possible that technological evolutions may make monitoring of external systems at the Distributed domain desirable in the future, if security and business governance issues can be resolved.
As previously stated, the GMS Integration service provides translation, prioritization, brokering, queuing, and marshalling capabilities between the services in the Central, Distributed, and Edge domains. To facilitate these capabilities two distinct types of integration systems have been defined for use within the GMS:

- **Central-to-Distributed Integration system**: is focused on the utility IT environment, and is anticipated to be an enterprise services bus / enterprise message bus, running on an effectively unlimited network, providing high scale, high throughput services.

- **Edge-to-Distributed Integration system**: is on the Field Area Network environment, and is anticipated to be a field message bus, with decentralized resilient messaging capabilities, to ensure that devices can coordinate action without requiring round trips between the edge and central domains.

A representation of the GMS “system of systems” high-level conceptual architecture is depicted in Figure-4 below. The Communication system spans all of the domains and each domain is comprised of a set of systems, which in turn provide a set of services. In general, there are very few instances of the central domain, a greater number of instances of the distributed domain, and many instances of the edge domain. Within each domain similar functions are performed but in a distributed fashion. For example, at the Central domain, the Reliability system ensures overall distribution stability while at the Distributed domain the Reliability systems manages at the substation, feeder, and lateral level, and finally, at the Edge domain, the Reliability systems maintain stability at the individual devices such as a single solar photovoltaic (PV) installation or energy storage element. Each of the individual domain subsystems also provides the base set of services to meet its required function. In the above example a central reliability system employs the control service to actuate systems or devices in the Distributed or Edge domain. A Distributed Reliability system directly actuates Edge devices, while an edge Reliability system controls its own behavior. Overall, the construct depicted in Figure-4 establishes an architectural framework that defines the structure for further decomposition of the GMS.
3.6 Architectural Characteristics

As a system of systems, the GMS has a series of characteristics it must fulfill in aggregate. Simultaneously, the subsystems, applications, and devices that comprise the GMS may not directly embody the broad characteristics of the overall system individually. These characteristics are both functional and non-functional in nature. This list is specifically not ordered in a priority order, because depending on the aspect or system they are being applied to, the priority may change.

3.6.1 Resilience

Resilience is the ability to prepare for and adapt to changing conditions, and to withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. In the context of the GMS, this includes supporting
deployment and integration of centralized and distributed energy sources and their supporting controls in normal and emergency (time constrained) situations. Electrical network resilience is primarily provided by the Reliability subsystem, but this characteristic must be embodied across the GMS, in elements from communications networks to databases to end devices. Maintaining the resilience of the GMS extends beyond the system itself, requiring organizational units - especially those managing critical facilities and hazard event-related functions - to make decisions and take actions that contribute to resilience.

Resilience also involves providing the systems and external interfaces to interact with third party stakeholders engaged in recovering from major energy system disrupting events. These stakeholders include disaster relief personnel, local governments, community leaders, mutual aid resources and the press.

3.6.2 Performance

Performance is the ability of the system to accomplish tasks in a timely manner, where timeliness may vary from milliseconds to hours. Performance must be tied to accuracy as a fast incorrect result may be worse than a late correct one. Performance must be maintained even under degraded conditions, such as deliberate attacks, accidents, or naturally occurring threats or incidents.

The GMS must provide a comprehensive set of services that cover a wide range of measurement, analysis, decision, and control time frames. These services range from localized high speed protection, control, and optimization functions involving individual and closely clustered devices to long term planning services that require analyzing decades of historical data, customer behavior, and climate trends to make future infrastructure investment decisions. Each of the underlying subsystems involved in managing these varied application time frames have unique performance requirements in terms of communications bandwidth, latency, reliability, resiliency, security, and redundancy and many of these performance metrics also apply to the physical electrical infrastructure components. This implies that a wide range of technologies will be employed to appropriately support each application. The California Institute of Energy and Environment (CIEE) recognized these operating time frames associated with a modern grid as shown in Figure-5. The Electric Power Research Institute (EPRI) introduced the concept of decision making cycles in various time frames, such as those described in the following table.

![Figure-5](source: California Institute for Energy and Environment (CIEE))
| 1  | Hour-ahead | Assure adequacy of resources (markets, forecasting, scheduling, etc.) |
| 2  | 5-minute   | System reliability, efficiency, and calculation of control parameters and limits for next 5 minutes: |
| 3  | 1-minute   | Maintain efficiency and reliability according to the control parameters identified by the 5 min cycle |
| 4  | 2-second   | Traditional continuous closed loop controls (AGC, etc.) |
| 5  | 1-second   | Data collection/validation for use by control area or interconnection: Data may be from the 10 msec cycles (PMUs) |
| 6  | 100-msec   | Recognizing and reacting to imminent system instabilities. Includes execution of: |
| 7  | 10-msec    | Primary cycle for intelligent protection and faster iSPS (load shedding, generation reaction, system separations) |

Source: EPRI Advanced Simulation and Modeling Decision Making Cycle Time Frames

Table-3

### 3.6.3 Time

The GMS consists of a multitude of systems and devices that directly measure or otherwise create data that must be associated with its time of creation for it to be effectively utilized or trusted within the GMS. This implies the use of one or more time sources both centralized and distributed using a variety of standards and technologies with characteristics (e.g. trust, precision, resolution, redundancy, accuracy) appropriate for the application.

### 3.6.4 Security

The GMS is involved in four (4) aspects of security:

- Cybersecurity - the ability to maintain the operational availability and integrity of communications and data of the electric grid and supporting communications infrastructure.
- Physical Security - maintaining the integrity of the devices and equipment in the field and knowing if there has been intrusion or tamper of those items.
- System Security - maintaining the operation of the grid within the operating parameters that are required for safe operation and compliance.
- Security of Supply - maintaining a balance between the demand for energy with the available supply of energy.
While the GMS is not the only system that deals with these aspects, the GMS has to be aware of these four aspects of security in order to operate.

3.6.5 Trust

Trust is a combined view of multiple measures of the veracity of a system component, piece of information, or other element. Trust is made up of more than security. Physical damage to a device, or aging can have an impact on the quality of the information coming from a component and the reliability of the operation of the component. Trust is a composite characteristic that includes the quality of the data coming from the component, the known reliability of the component and the likelihood that the component is secure, and the information flowing to and from the component have not been tampered with in a fashion that impacts the integrity of the grid. Trust includes verification of the identity of the device, who owns the device, the calibration status of the device, the history of the device reporting, tamper indicators, and other characteristics of the system or device.

3.6.6 Safety

Safety is the ability to ensure the protection of people and equipment in the electrical system. Worker safety is a key piece of what the GMS supports. Both human and equipment safety are critical concerns for the implementation of the GMS.

Safety is fundamental to the GMS. All system components must ensure that safety is preserved in all operating conditions and operating modes. This includes failing in safe and predictable ways. Safety must also be considered with respect to the interaction between cyber and physical systems, for example the coordination of lockouts and tagouts between workers in the field and the GMS. The GMS is the system of record for managing field worker and equipment safety, where:

- connected distributed generation and storage devices are correlated against specific electrical network segments
- a tamper on a device, which may impact the ability to tag-out the device, can be tracked
- a device might not be able to be trusted to perform as expected while maintenance is being done
- other conditions may impact the status and condition of the grid and attached devices.

The GMS has to manage the health and protection of the equipment attached to the grid as part of the safety aspect of the GMS. The GMS has to deal with maintaining this equipment safety by supporting the protection of the system and its equipment (e.g. relaying). In many cases the GMS will be the primary interface to these equipment safety schemes in the future.

3.6.7 Maintainability

Maintainability is the ease with which a system can be maintained within an acceptable timeframe and cost. There are several aspects of maintainability that the GMS has to deal with:

- The maintainability of the GMS itself – providing a path for updating, fixing and improving the GMS
- The maintainability of the models and tools that support the GMS, including the network model
- The maintainability of the data both within the GMS and in systems that are supported by the GMS data
- The maintainability of the physical equipment that is attached to the grid. While the GMS does not make the actual maintenance tasks easier, it should help prioritize the maintenance tasks to improve the overall maintainability of the grid.
3.6.8 Economical
The Economical characteristic captures the relationship between the cost and benefits of a system. Economical systems deliver value equal to or greater than their costs.

The GMS must deliver value to each stakeholder while complying with the various regulations and statutes that the grid operates within.

3.6.9 Compliance
The Compliance characteristic captures the relationship between the regulations and statutes that the GMS must operate under. Regulatory requirements govern the operation of the grid. Compliance encompasses not just economic compliance, but compliance with respect to safety, reliability, efficiency, environmental, and other regulations, as well as contractual commitments. The regulatory environment is complex and ever changing, the GMS must be able to operate within all of these regulatory requirements and constraints.

3.6.10 Common Data Store
The Common Data Store characteristic captures the relationship between subsystems and systems within the GMS. The GMS and its component parts needs to share a common data store for as much of the data as is reasonable.

3.7 Architectural Constraints
Design and deployment of the GMS faces a wide range of constraints over its lifetime. Some of the most challenging constraints are those related to the fact that the entire business and energy delivery enterprise and infrastructure must continue to operate seamlessly and transparently to all stakeholders as the GMS is rolled out. This implies that many systems currently in place may be required to operate well beyond the time their GMS functional equivalents are deployed to support an orderly transition. Some constraints are related to vendor capability such as the ability for vendors to evolve their technology to support GMS defined interface requirements. For example, the Simulation subsystem (part of the planning system) relies on products from numerous vendors in a mature but niche market that will be challenged to support common data input and output formats in a timely manner. Some technologies envisioned for use in the GMS are relatively immature with limited vendor support which may limit the ability to fully implement GMS functionality - at least initially.

Other constraints include:
- Numerous systems and interfaces are subject to some form of current and/or anticipated regulation (e.g. NERC CIP) that must be considered
- Testing and certification for many technologies being considered for the GMS do not yet exist
- Spectrum availability and cost will influence numerous aspects of the GMS architecture and design.
4 System Decomposition

4.1 Reliability System

The Reliability system ensures reliable and safe operation of the distribution management system. As depicted in Figure-6 below, the Reliability system is composed of the following subsystems:

- Protection subsystem
- Restoration subsystem
- Supervisory and Management subsystem

The Protection subsystem provides the near instantaneous response required to isolate faults when they occur. The restoration subsystem provides fault location and system restoration services. These automated subsystems are controlled by a supervisory and management system which allows operators to control both current behavior of the system, and the parameters and settings which dictate ongoing behavior.

While it interfaces with the Supervisory & Management subsystem, the Protection subsystem is able to operate completely independently of any other GMS component. This enables the protection subsystem to ensure the safety of the electrical network regardless of the state or actions of the rest of the GMS. In addition to providing a user interface for operators, the Supervisory & Management subsystem allows coordination between the Protection and Reliability subsystems when needed.
4.1.1 Protection Subsystem

The Protection subsystem prevents damage to people, property, and the electrical grid itself when faults occur. Its response must be effectively instantaneous. The most common action is to disconnect the asset for which a fault has been detected. The overall protection subsystem includes both edge devices (circuit breakers, relays, reclosers, fuses, etc.) that isolate faults and protect assets, and the distributed and centralized control components that coordinate action. The Protection subsystem must accommodate wide-spread deployment of distributed energy resources. DER may impact how circuits respond to faults and over-current events, requiring changes to protection circuit designs and the addition of new protection devices.

Protection systems must be predictable and dependable. Historically, this resulted in emphasis on simple, reliable, electromechanical devices. More sophisticated, programmable devices are broadly available, but have not always been chosen because of concerns regarding longevity and reliability, as well as the costs associated with more complex protection devices. The major critical functions of the protection subsystem are carried out by the protection devices themselves: circuit breakers, relays, reclosers, fuses, etc.

The Protection subsystems in the Central and Distributed domains provide coordination between protection devices. Protection schemes which include central or distributed coordination are particularly important for circuits with distributed energy resources, as the appropriate protection action may change dynamically depending on operational, weather, or market conditions. The Protection subsystems must actuate protection devices sufficiently quickly as to prevent damage to people, property, or utility equipment. In some cases, this means taking action in a fraction of a 60 Hz cycle. The choice of the central versus the distributed domain is determined by the computational power, latency, and cost needed to meet the safety, reliability, and economic requirements of SCE. (Note that a Distributed Protection subsystem may be contained directly within a protection device.)

The Protection subsystems in the Central and Distributed domains also provide coordination with distributed energy resources, informing them of fault conditions and providing instructions when appropriate. (Note: this does not replace or preclude automatic fault detection behavior, such as IEEE-1547 islanding).

While many protection actions are reactive (e.g. a fault occurs and a recloser activates), the Protection subsystems in the Central and Distributed domains also perform analysis on information collected from edge protection devices to provide predictive protection capabilities. Depending on the severity and immediacy, predicted failures can result in coordinated protective actions (i.e. direct actuation of edge devices), or in messages being sent to other GMS subsystems for further action.

All programmable protection devices may receive configuration changes from the Supervisory and Management subsystem. Typically, these changes adjust parameters used by the device to take action. Instrumented and intelligent devices may provide status information back to the Supervisory and Management subsystem, which in turn may update the Grid Awareness subsystem as needed.

4.1.2 Restoration Subsystem

The Restoration subsystem locates the fault, determines the system configuration which allows the greatest restoration of service while still maintaining safety, and executes the appropriate reconfiguration. Historically, restoration has been a manual process of isolating a fault to the smallest possible portion of the distribution network, and then physically clearing it. Once the fault was cleared, the remaining isolated element could be returned to operation. The Restoration subsystem enhances this process, and in some cases automates it completely.
Within the GMS, restoration is automated as much as possible through the use of intelligent restoration devices. Evolving the distribution network from the current state to one capable of ubiquitous automated restoration will take many years. As a result, it is critical that the Restoration subsystem be able to facilitate automated, partially automated, and manual restoration.

To support manual restoration, the Restoration subsystems in the Central and Distributed domains must provide guidance to operational personnel regarding fault location. (Note: such guidance is made possible through operational information provided via the Data Repository or the Integration system.) When a fault location is confirmed, the system must then provide guidance regarding the preferred system configuration to safely and quickly restore service. Specifically, the Restoration subsystem evaluates known loads, capacities, and DER to determine which devices should be opened or closed to restore maximum service while awaiting resolution of the fault, and communicates this information to line crews.

Automatic restoration is performed by edge restoration devices working in conjunction with either the Distributed or Centralized Restoration subsystem to provide coordination. As in manual restoration, the first actions of the Restoration subsystem are to safely restore service to as many customers as possible. Once this is complete, the Restoration system awaits indications from the work management system that the identified fault is resolved. If resolving the fault restored service to all customers, then no further work is done by the Restoration subsystem. The Optimization subsystem (discussed below) may make further adjustments to the distribution network to return it to a more optimal state.

In cases where the distribution network is only partially automated, restoration activities will be a hybrid of automated and manual processes. Partially automated devices are those which have had automation technologies retrofitted to them, but do not have the same capabilities as natively automated devices. The distribution network is also likely to have partially automated installations. For example, a single remote intelligent switch may be installed on a circuit where the ideal configuration for full automation requires three or four switches.

Automated edge restoration devices can be classified into two broad categories: sensors and actuators. Sensors provide data back to the Restoration subsystem. Pure sensors are devices like remote fault indicators and meters. Actuators are able to change the configuration of the electrical network. This includes switches and sectionalizers. A given edge device may be both a sensor and an actuator. Many intelligent actuators also include data collection and reporting capabilities. Edge devices may also be both protection and restoration devices, such as an intelligent recloser that automatically attempts to clear a fault and restore service, is able to report the actions it has taken, and the conditions which triggered those actions.

4.1.3 Supervisory & Management Subsystem

The Supervisory & Management subsystem is the interface operators use to control and monitor the Reliability and Protection subsystems. The Supervisory subsystem allows manual control when required, ensuring that operators can override the automated systems at any point. The Supervisory & Management subsystem also controls the settings, parameters, and configurations used by protection and restoration devices in their operations. The subsystem allows the operator to reconfigure devices to ensure the most effective operation possible. With the notable exception of instantaneous action taken by protection devices, the more centrally located systems are granted higher authority than more distributed ones, with the Supervisory & Management system retaining ultimate authority over all protection and restoration actions.

Generally, the Supervisory subsystem relies on the Data Repository for external information, such as market conditions, the state of the bulk power system, and long term weather forecasts.
4.2 **Optimization System**

The Optimization system is responsible for operation of the distribution grid and the operational tuning to achieve specific performance, reliability, and economic goals. The Optimization system performs analysis based on policies and rules, the state and status of the grid, and the DER state and status, as well as external data sources such as weather and market pricing. This analysis is used to determine the optimal operational scheme for the grid and DER. Optimization objectives and behavior are determined by an operator selected “mode” of operation. In addition to automated operation, the Optimization system provides a user interface for operator visualization, interaction, and intervention.

The Optimization system is composed of three distinct subsystems that interact with GMS devices:

- Optimization Management subsystem
- DER and Electrical Automation subsystem
- Grid Awareness subsystem

The Optimization Management subsystem prescribes this operational scheme through rules and policies passed down to the DER and Electrical Automation subsystem. The DER and Electrical Automation subsystem is then responsible for controlling the grid devices and DER equipment to implement the prescribed operational scheme.

This control process is then repeated with feedback from the Grid Awareness subsystem, changes to operational goals, or input from external systems such as weather or energy markets or other such external stimulus such as user intervention that would affect the optimal operational state of the grid.

During abnormal conditions, affected sections of the grid and DER control would be overridden by the Reliability subsystem until such time that normal operations can be restored. During abnormal conditions, the Optimization Management subsystem would continue to optimize the normally operating areas of the grid. Pending acceptance by the Reliability system, it may also provide optimization instructions for degraded portions of the grid, using alternate optimization objectives. Once normal operations have been re-established by the Reliability system, the Optimization system would then resume optimization of the restored grid sections.

*Figure-7* below illustrates the components of the Optimization system and their interactions.

---

4 “state” and “status” are discussed further below in sections 4.3.1 and 8.7.
4.2.1 Optimization Management Subsystem

The Optimization Management subsystem is the analysis engine and controller that exerts control on the DER and Electrical Automation subsystem to establish optimal operating conditions of the grid and connected DER equipment. The Optimization Management subsystem analyzes all available data on the grid state, current and future DER availability, external systems such as weather or energy market data and regulatory controls, and establishes an optimal operating scheme based on the currently selected operational "mode," as illustrated below.

The Optimization Management subsystem governs this scheme through operational rules and parameters passed to the DER & Electrical Automation subsystem. The Automation subsystem is responsible for equipment control to implement the prescribed operational scheme.

In addition to the analysis and control functions, the Optimization Management subsystem provides a user interface for the analysis, control schemes, and real-time state and status awareness for both the grid and DER. This interface provides the GMS user with the ability to alter the goals, rules and parameters of the optimizer, and to override control schemes with user directed control.

The GMS will have many parameters which alter and adjust its behavior. The ability to tune the behavior of the Optimization and Reliability systems in particular will be critical to enabling the GMS to respond to varying operational conditions. Tuning these parameters manually would be both tedious and inefficient. To address this, the GMS has different modes. By changing modes, the operator can effectively retune the entire GMS to respond to a different set of operational conditions. For example, "BlueSky" mode might reconfigure the system to maximize energy production from DER, while "Storm"
mode might tune the system to use the most conservative protection settings and prioritize clearing faults and other reliability concerns over the use of DER. Modes can also be localized such as “Fire” or an emergency that covers only a portion of the SCE territory.

4.2.2 DER and Electrical Automation Subsystem

The DER and Electrical Automation subsystem is responsible for the control of grid and DER equipment to implement the scheme prescribed by the Optimization Management subsystem. Rules and parameters for the optimal operating scheme are received by the Central DER and Electrical Automation subsystem from the Optimization Management subsystem. The DER and Electrical Automation subsystem then works autonomously to balance resources and device settings to implement the operational scheme that matches the rules and parameters from the Optimization Management subsystem.

The Central DER and Electrical Automation subsystem distributes the relevant rules and parameters to its Distributed counterpart. The Distributed DER and Electrical Automation subsystem communicates with the grid devices and DER equipment to place each device into the desired operational mode. The Distributed DER and Electrical Automation subsystem has local grid state and status awareness and is able to continue to operate in the prescribed mode until directed to change by the Central DER and Electrical Automation subsystem.

4.2.3 Grid Awareness Subsystem

The Grid Awareness subsystem maintains the electrical connectivity model of the distribution network, as well as information regarding status. This includes phase connectivity, switch positions, and the operational status of every device that can change the state of the electrical network. Also included are the available energy resources for a given device such as available VARs, generation, or load shed. Additionally, the subsystem monitors all available electrical network telemetry available including voltage, current, phase balance, VAR, and others. Finally, this subsystem tracks device telemetry such as temperature, health, or other available data. This is achieved through a combination of real time monitoring, state inference, and active determination. The Grid Awareness subsystem allows the GMS as a whole to make fully informed decisions.

The electrical network model is the framework for all grid status and state data maintained by the Grid Awareness subsystem. This electrical network model is developed and maintained through the Planning System, specifically the Electrical Network Model Update subsystem. This model update subsystem provides the planning and engineering interfaces to develop and maintain all aspects of the electrical network model in use by the GMS.

In order to provide local real-time information to the Distributed DER and Electrical Automation subsystem, the Grid Awareness subsystem has a Distributed instance to collect and analyze local status and state data. This local state and status data is shared with the Distributed DER and Electrical Automation subsystem for control purposes and is also passed up to the Central Grid Awareness subsystem for further aggregation and analysis. The Central Grid Awareness subsystem makes the aggregate model, status, and state data available to the Central DER and Electrical Automation subsystem for central control functions as well as to the Optimization Management subsystem for further optimization.
4.3 Planning System

The Planning system is the engineering and planning component of the GMS. Its purpose is to support the engineers, planners, and operators with analysis, future capital needs, contingency analysis, integration of new DER components, simulation of various future scenarios, and assistance in verification of tariffs, programs, incentives, and offers. The Planning system provides core functionalities related to planning over wide time frames from very near term planning issues, as well as supporting long range planning efforts. Different applications, tools, and business processes will be used depending on the planning horizon, but they will all utilize aspects of this system and its subsystems. As shown in Figure-8, the system is composed of five subsystems:

- The Electrical Network Model Update subsystem
- The Scenario Planning subsystem
- The Asset Maintenance subsystem
- The Profiling and Forecasting subsystem
- The Simulation subsystem

![Figure-8](image)

4.3.1 Electrical Network Model Update Subsystem

The Electrical Network Model Update subsystem (ENMUS) provides the interface into the electrical network model (ENM) maintained by the Grid Awareness subsystem (described previously as part of the Optimization system) that underpins the GMS. This subsystem allows users to make manual updates to the model. These updates are performed in a separate “layer” of the model in a way that does not impact the operational model, but can be released to the operational model using a release process by users with the proper GMS roles and authority. These manual changes include items such as adding new power line segments, replacement of a transformer, or the addition of a new storage system by a customer. The
ENMUS will allow the entry of all the physical grid elements, their connectivity, and characteristics including:

- switches and their possible positions
- electrical characteristics of each device
- locations of sensors and the information they can provide
- controls and the actions they can take (e.g. move switch 123 between positions A, B, and C)
- other characteristics that can be used for simulation, planning, operations, and other purposes, such as installation date, name plate information, construction material, and dimensions

The electrical network model contains far more than the information that can be updated by the ENMUS, including the state of the grid (calculated), the status (sensed or reported), tag-outs (recorded), and current operating conditions (e.g. temperature [sensed]). The ENMUS must be able to link these elements together and characterize the nature of the link, for instance, recording which sensors are attached to which physical location and device in the grid model.

To do its work, all elements in the ENMUS have the dimensions of perspective, scenario, and time. These dimensions allow the data in the electrical network model to encompass the complete life-cycle of grid elements. Perspectives provide a way of partitioning the electrical network model into different views, including as-forecasted, as-planned, as-designed, as-contracted, as-built, and as-operated views. Scenarios allow for different variants within a given perspective. For example, an as-forecasted perspective might have multiple scenarios based on different levels of population growth, or an as-contracted perspective may have different scenarios which reflect different contract options. Finally, the temporal (time) dimension allows all of the data in the electrical network model to change over time.

Using these dimensions, the GMS allows the operator both compare and combine views. For example, an operator might want to run a circuit analysis on an as-operated view and compare it with an as-designed view as part of a forensic analysis, or a planner might want to overlay an as-planned view on top an as-built view to determine the impacts of design deviations.

Planning typically starts with a set of planning assumptions and then options are considered by the planners for the project. Perspectives allow the design to be maintained within the network model throughout the design’s entire lifecycle, from as-planned to as-operated. Because any of the early steps can have multiple options, scenarios can exist under each of the perspectives, allowing a user to choose a perspective and then develop multiple options under that perspective. A selection process will exist to pick the desired scenario and a release process will move the project from one perspective to the next. Since multiple projects may be done on the same area of the grid, a temporal element is also included to allow differentiation between projects over time to tag when a specific project progressed through a specific perspective.

The ENMUS allows users to update categories of devices (e.g. add whole new categories, or update the characteristics of an existing category), device models and their characteristics, and specific elements in the ENM (e.g. exchanging a 30 KVA transformer for a 10 KVA transformer). The subsystem also provides the automated interfaces to the exchange service so that external systems like SAP can load asset management information into the electrical model and extract updated asset information for use in the financial systems, as well as other external systems. Coordination with other external systems is also required and these exchanges may result in changes to the ENM that will flow into an appropriate perspective. The subsystem can be used to trigger analytics on the grid to confirm connectivity after storms, construction, maintenance, and other evolutions to verify that the restoration matches the prior connectivity model, and if not, allow an automatic update based on the way the physical grid was rebuilt.

A user in the correct role has the ability to make updates active (operational), which means that they exist in the physical world and can be pushed to the as-operated grid model. Planning updates can be held as
future or inactive which allows the model to be used for analysis, but the updates will not impact the operational model used by the other systems, such as the optimization system. Similarly, pending and in progress maintenance updates can be displayed and reflect status as the work progresses and eventually be committed to the model when the work completes.

Temporary reconfigurations while working an outage may be shown in the user interface and possibly be committed to the model, and then reverted depending on the timing and user judgement as to the value of reflecting temporary changes in the active model. One example is temporary jumpers for maintenance work or to restore power flow after an outage. Some of these changes have higher priority than others and could be put into a modification queue based on priority to make it easier for the user to make good decisions on what to approve for update and when. Longer-lived temporary reconfigurations are to be pushed to the model, relying on the temporal dimension of the model to persist changes over time. Status changes (such as switch reconfigurations) may be automatically persisted to the model by the GMS when technology allows. Automatic updates will be done by the Grid Awareness subsystem making requests to the ENMUS.

Once an update is completed in the ENMUS, then the update is released to the appropriate perspective where the GMS systems have access to the updates, if warranted.

The ENMUS also provides users with an indication of model issues, flagged either automatically or manually, for resolution by an engineer. (Model issues may occur when physical events in the real world occur, but the model is not updated, such as a manual switch may be operated by a lineman, but not reported.)

### 4.3.2 Scenario Planning Subsystem

The **Scenario Planning** subsystem allows planners, engineers, and operators to run “what if” scenarios with the ENM and use the Simulation subsystem (described below) to run analyses on each of the scenarios they create. The Scenario Planning subsystem allows users to select arbitrary sections of the grid, or pieces of equipment, and do analysis on the selection. The purposes of this analysis include, but are not limited to:

- Medium and long range capital planning
- Approval of new DER
- System upgrades to create hosting capacity for DER
- Protection scheme analysis
- Switching order development
- Impact of new equipment
- Positioning of sensors (e.g. micro-PMUs)

This subsystem can take full advantage of the EMN making a copy of the selected area for analysis and simulation. The user can interact with the model to create each scenario of interest and save the scenario for future simulations, capital planning or review. The user can select the types of simulations that are to be run on the model in the Scenario Planning subsystem and have the requests made automatically to the Simulation subsystem.

The Scenario Planning subsystem can also interact with the Profiling and Forecasting subsystem (described below) to select the corresponding (or correct) set of profiles for the scenario, including selecting scaling factors for classes of devices for medium and long range planning scenarios and other longer-term based scenarios.

---

5 Note: In this case a “reversion” does not remove or undo the change to the model, it creates a new temporal record which returns the model to the previous configuration. The record of the temporary reconfiguration for that period of time remains.
The Scenario Planning subsystem can interact with the Asset Maintenance subsystem to allow the user to determine the additional maintenance required for dynamically rating equipment over (or under) the nameplate rating and other changes in equipment usage.

The Scenario Planning subsystem can also be used to export a “package” of data for external analysis, including but not limited to: (a) connectivity model (b) electrical characteristics of the model (c) re-rating of equipment (d) loading, profiles and other historical usage data (e) other data required for running the simulation. The package will be exported using the Exchange service.

Approved changes to the model can be saved until the construction is completed and then activated by an engineer or a planner to extend the operations model to include the new changes.

4.3.3 Asset Maintenance Subsystem

The Asset Maintenance subsystem monitors equipment usage, loading, temperature, number of operations, environmental sensor data, and other parameters to adjust maintenance directives on equipment to improve reliability of the overall electrical system and to prioritize maintenance to maximize the value of work done.

The subsystem interacts with the Profiling and Forecasting subsystem to get information on asset loading, externally with SAP for asset information, the electrical network model for connectivity, and the Simulation subsystem to run asset life cycle simulations.

The results from the Asset Maintenance subsystem are recommendations for de-rating or re-rating equipment, changing the maintenance cycle, replacing equipment that is uneconomical to maintain, and other maintenance recommendations based on the data collected by the GMS.

Output from the Asset Maintenance subsystem is sent to the external asset management system, the external work management system, and to the electrical network model, when the asset has had restrictions placed on it. Once these restrictions are in the electrical network model, they can be picked up by other systems for operations, protection, and other functions.

4.3.4 Profiling and Forecasting Subsystem

The Profiling and Forecasting subsystem has five major functions:

- Processing of historical data and data streams to create device level load profiles that are normalized for weather and other conditions. Profiling is provided not just for metered points but also for DER and other devices where sensors that can collect data exist.
- Using the developed profiles to create a wide range of temporal forecasts from annual forecasts for the whole system on one end of the scale to forecasts that are seconds in length for specific locations on the grid on the other. The forecasts can be for any arbitrary section of the grid or device on the grid. Using the electrical network model the forecasts can aggregate any underlying devices, including estimating losses.
- Create historical data profiles for any device based on the saved states of the grid connectivity for any arbitrary period of time in history.
- Create “day-of” forecasts based on current usage, weather forecasts, and other available data to feed to the optimization subsystem for use in grid optimization.
- Validation, Editing, and Estimation (VEE) on raw data that is not verified by other systems (e.g. weather data).

The Profiling and Forecasting subsystem interacts through the Exchange service with data collection systems like the meter data management system, business systems like SAP, and third party system like the US Weather Service.
The profiling and forecasting subsystem can be triggered by the scenario planning subsystem, the simulation subsystem, and other components of the GMS to support their operations.

### 4.3.5 Simulation Subsystem

The **Simulation** subsystem is a comprehensive collection of simulation engines that incorporate event based, time synchronized, Power Flow, Market Simulations, and Communications Flow into a common co-simulation environment. The system provides highly granular event-based integrated solutions to highly complex grid operation scenarios. These scenarios may simultaneously include elements such as protection cases, weather scenarios, communication interference, and market fluctuations. The system is capable of providing simulations across multiple time horizons, from seconds ahead to years ahead. Simulations may be used both for short term and long term optimization, anomalous event forensic analysis, as well as providing services to the Planning subsystem.

The Simulation subsystem includes five major types of simulations: Steady-State Simulation, Quasi Steady-State Simulation, Dynamic Simulation, Transient Simulation, and “Hybrid” Simulation. Each of these simulation types have different data input and fidelity requirements and generally use different mathematical techniques for their solution. The Simulation subsystem provides a set of simulation services that can be accessed by any other subsystem (e.g. Scenario Planning subsystem). Jobs are submitted using a common data format and results are returned in a common format. The Simulation subsystem also supports particular formats and models as required by SCE regulators (e.g. The Western Electric Coordinating Council (WECC) uses PSLF from GE for steady state and dynamic simulation of the transmission system).

The Simulation subsystem includes off-line state estimation. This is a version of the state estimation system similar to what is described in the Optimization System. Off-Line state estimation has a more robust user interface to allow engineers to do forensic analysis of historical situations on the grid, and for engineers to also be able to run future state estimation for potential changes to the grid. The Simulation subsystem has the ability to define arbitrary areas of the grid for study, to define changes to load and demand response, and other differences that the engineer may wish to check. On the forensic level, the engineer can view the state estimation that the Optimization system created against the off-line state estimation re-run of the historical data that may include information that was not available at the time the original results were created.

### 4.4 Economics System

The Economics system interfaces with the distribution market (emerging), the CAISO, and other emerging markets, including any internal market-like mechanism that SCE might end up creating over time. The Economics system is not only about supply, but also about demand, ancillary services, balancing, storage, energy banking and the other aspects of the economic interplay between the grid, service providers, aggregators, customers, suppliers, and the organized markets. In some cases the Economics system will be dealing with multiple regulatory tariffs (including incentives) that support the use of storage, electric vehicles, demand response programs, and distributed generation. In many cases, the distribution system operator may be responsible for optimizing the system costs for energy as one of many objectives that the GMS is responsible for.

In the case of economics, the regulations will constantly change to support the stakeholder needs. The GMS Economics system needs to be flexible enough to support these changing requirements including but not limited to changes in tariffs, incentives, customer programs. The Economics system may use cost, price, value, tariff, incentive algorithms for optimization, depending on future regulatory decisions.
The Economics system operates both pre-operational interval and post-operational interval and is comprised of three subsystems:

- Economic Interaction subsystem
- Contractual Parameters subsystem
- Performance Verification subsystem

The Economic Interaction subsystem operates primarily pre-operational interval, but also has to operate post-operational interval to support billing and incentives. The Contractual Parameters subsystem primarily operates post-operational interval, but supports the Economic Interaction subsystem with needed data in both intervals. The Performance Verification subsystem focuses purely on the post-operational period. See Figure-9.

![Figure-9](image)

### 4.4.1 Economic Interaction Subsystem

The Economic Interaction subsystem is the primary GMS component interacting with external economic factors and dealing with external economic inputs into operational decisions. This subsystem is responsible for the information coming into the Economics system from all external entities about energy, ancillary services, transmission rights, and other commodities. This may include constraints on imports, exports, prices, and other factors. Because this aspect is still changing, the system needs to be flexible enough to deal with existing markets like the CAISO and potential future markets like a retail market. Additionally, there are expectations that some of the tariffs that are currently in place may change significantly to support very high levels of distributed energy resources. In some cases there may be a

---

See the June 8, 2015 CPUC white paper on future utility business models.
need to optimize across multiple demand response programs to either reduce or increase demand in specific locations, or to provide economic signals to storage or other devices installed in the grid. The Economic Interaction subsystem will have the primary responsibility for interacting with aggregators and other third parties for demand response, storage operation, and distributed generation. The Economic Interaction subsystem will interact with the Contractual Parameters subsystem for information, as well as the Forecasting subsystem for forecasts in the time ranges that are required for bids and asks from the external entities.

By 2040, there may be as many as 100 million customer owned devices in SCE’s service territory that can respond to signals. The number of devices and the speed of operation may mean that messaging has to be automated because it is too complex and rapid for human operators to respond to in a timely fashion. At this level of penetration, control signals will likely need to include both economic and direct messaging.

4.4.2 Contractual Parameters Subsystem

The Contractual Parameters subsystem tracks and stores all the contracts for supply, demand response, and storage that are available to SCE. This includes contracts for both additional supply and demand response. The subsystem tracks items that include but are not limited to:

- Contracted price
- Performance period
- Any penalties for performance or other factor
- Number of hours or times that a contract can be called or has to be called
- Characteristics of the contracted resources (e.g. capacity, operating hours, fuel availability, etc.)
- Allowed (required) duration of call on the resource
- Remaining contract values (e.g. the system is updated each time the contracted resource is called)
- Any environmental costs or benefits (e.g. carbon production) of the resource per unit of energy
- Special instructions (e.g. outage) and contract information
- Other operational factors for the contracted resources

On a regular basis (e.g. hourly, daily) the Contractual Parameters subsystem will create a pre-processed list of available options for the Optimization subsystem. This will allow the Optimization subsystem to rapidly offer options to the operator in a prudent fashion for supply/demand balancing.

The Contractual Parameters subsystem will interact with the Economic Interaction subsystem to provide input for market/bid ask to provide the internal economic and capability information to allow the Economic Interaction subsystem to complete bid/ask transactions with external parties and systems.

The Contractual Parameters subsystem will feed the Forecasting and Profiling subsystem with contracted resource characteristics so that forecasts can be prepared for use by both the Optimization and the Economic Interaction subsystems.

4.4.3 Performance Verification Subsystem

The Performance Verification subsystem is responsible for interacting with the Meter Data Management system and other sensor aggregation systems to retrieve and verify that contracted resources actually performed when called upon. The Performance Verification subsystem will rely on the other sensor aggregation systems (e.g. the Optimization system and its supporting subsystems) to interact with the sensors on a regular schedule, to retrieve, verify the validity of the readings, and forward those readings to the Performance Verification subsystem.

The Performance Verification subsystem will provide invoice quality information to the customer information system for billing and accounting purposes. The subsystem will also interact with the Contractual Parameters subsystem to update actual performance and trigger penalties as accrued.
The Performance Verification system will:

- Pull information from the Optimization subsystem on contracted resources that were tasked
- Interact with the Contractual Parameters subsystem for resource information required to do its job (e.g., the capability)
- Interact with the sensor aggregations systems to pull verified data for the time periods that the contracted resources were tasked for those resources
- Compare the tasking from the Optimization subsystem to the measured performance
- Interact with any third party systems via the exchange service for data coming from external parties for their contracted performance
- Determine if any penalties are due from either party
- Calculate any performance related invoices
- Update the Contractual Parameters subsystem on actual performance of contracted resources
- Update the Customer Information System on any billing related information that results from performance or lack thereof
- Update the Forecasting and Profiling subsystem on the performance and commercial reliability and any changes in observed performance of the contracted resource

The Performance Verification subsystem validates that all components of the forecast-notify-operate-verify loop for third party resources that SCE depends on to balance supply/demand are complete.

4.5 Grid Infrastructure Management System

The Grid Infrastructure Management system manages the computing and communication functions used by the GMS, as well as providing tools for operational management. The computing elements include the servers, processors, and storage located in the Central and Distributed domains. The Communication system (discussed below in section 4.6) provides the network connectivity between the Central, Distributed, and Edge domains. The IT users of the Grid Infrastructure Management system are concerned with the communications network and computing/storage operations. The OT users of the System Management system are concerned with managing the overall operational activities of the GMS, including system loading and priorities. As a result, Grid Infrastructure Management users are spread across multiple SCE organizations. The Grid Infrastructure Management system is also responsible for providing policies and managing security infrastructure for the GMS.

Excluded from direct management by the Grid Infrastructure Management system is external infrastructure that is not under the management of the GMS users. An example of this infrastructure is Cellular 4G/LTE backhaul. However, the Grid Infrastructure Management system will receive operational fault/event messages from the GMS assets that are dependent upon such external infrastructure. This will enable fault management and isolation for all infrastructure including assets not directly managed by GMS.

The Infrastructure Management system is comprised of the following subsystems:

- Manager of Managers subsystem
- Network Management subsystem
- Security Management subsystem
- Log Management subsystem
- Virtualization Management subsystem
- Health Management subsystem
- Software Management subsystem
- Integration Management subsystem
- Operations Manager subsystem
These subsystems are described below. Figure-10 shows how these subsystems interact with the communication infrastructure and devices across the GMS domains.

4.5.1 Manager of Managers Subsystem

The Manager of Managers subsystem maintains and provides a GMS-wide view of all communications and computing resources. The GMS communications network, computing topology, and route state information are displayed to users responsible for GMS network operations. Communication fault and exception events are pushed to the subsystem via industry standard protocols from the other Infrastructure Management subsystems.

All communication nodes in the GMS will be capable of sending autonomous event messages to the Manager of Managers subsystem via the Network Management subsystem. The users responsible for the GMS infrastructure will have visibility to all communication and computing infrastructure event occurrences and clearing.

The Manager of Managers subsystem also performs analytics for communication fault isolation by use of inputs from the other Infrastructure Management subsystems and potentially fetching directly from the
communication nodes. The resulting isolated communication faults are then displayed to the GMS user. An example of the analytics is that of timing, where knowledge of the GMS infrastructure’s hierarchical model is necessary for fault isolation.

The Manager of Managers subsystem is the aggregation and correlation/fault isolation point for all events detected by the other subsystems in Infrastructure Management system. This subsystem provides the visualization for the GMS user to enable appropriate response to an event that occurred within the infrastructure. The Manager of Managers subsystem includes the trouble ticket management functionality to maintain state and assignment of GMS faults.

Persistence and access to any combination of the Data Repository system and the management subsystems enables the GMS user to perform forensics and rely on historical events for root-cause analysis and reporting.

The trouble ticket function interfaces with external infrastructure work-order management pushing trouble tickets to those systems. The trouble ticket function receives trouble resolution information back from the external work-order management updating, or closing the particular trouble ticket.

4.5.2 Network Management Subsystem

The Network Management subsystem includes a communication node management function designed specifically for configuration and management of communication nodes that are part of the GMS including meeting the routing and Quality of Service (QoS) management requirements in the Communications system.

The Network Management subsystem maintains the configuration backups and IP addressing plan for all communication nodes. Configuration backups can be used for restoration or insertion of replacement communication nodes of the GMS, and for audit by engineers without the need to access an in-service communication node. The Network Management subsystem also requires knowledge of the network topology and asset inventory with geolocation. It works in conjunction with external asset management systems to maintain this information, and makes it available to other subsystems within the Grid Infrastructure Management system.

The Network Management subsystem provides performance management capabilities working in conjunction with the Security Management subsystem, and the Virtual Management subsystem. It monitors utilization of the communication nodes and measures latency over critical paths within communications system. The subsystem may monitor heartbeats and poll communication nodes on a periodic basis for faults and topology discovery, although polling may at times be a function of the Manager of Managers subsystem.

The Network Management subsystem has the responsibility of detecting and reporting anomalies of the underlying communication infrastructure it has responsibility for. By way of example, communication nodes are able to detect key metrics directly (e.g. GPS signal lost) that communication nodes may then trap (in the Simple Network Management Protocol (SNMP) sense) or report (in the syslog sense, see Log Management subsystem). The Network Management subsystem implements analytics to correlate its knowledge of multiple communication nodes to isolate the fault/alert to a particular time source.

7 ITU M.3010, “Principles for a telecommunications management network”
4.5.3 Security Management Subsystem

The Security Management subsystem provides the required functions to fulfill security policy distribution and management. Examples of policies are user credentials and authorization. Devices and computing resources security policies are managed by this subsystem.

The Security Management subsystem provides the management interface for all of the GMS security infrastructure, as well as system wide cyber security key management (e.g., Public Key Infrastructure (PKI)). The Security Management subsystem provides its clients management of these security services.

Security event notifications are sent to the Manager of Managers subsystem for display and remediation. Security violations are typically determined via audits of infrastructure elements or messages from the Log Management subsystem. Security events sent to the Security Management subsystem include events external to the GMS, such as open doors detected by External Management system(s). The Security Management subsystem processes the notifications and sends appropriate event information to the Manager of Managers subsystem for display/visualization and action by the GMS users.

Cybersecurity for the GMS is managed within the Security Management subsystem. While many of the security functions are common for both computing and communication, it is recognized that there will also exist specific functions within each.

4.5.4 Log Management Subsystem

The Log Management subsystem manages all logs from all sources such as Windows events, syslog, flat file, NetFlow/IPfix, databases or applications, and infrastructure change management. This subsystem performs analysis of messages for functions such as security rule violations or as specific as a timing fault in an infrastructure entity. All detected security events and alerts will be forwarded to the Security Management subsystem for appropriate action. Network anomalies detected in applications, databases, systems, and devices will be forwarded to the Manager of Managers subsystem for appropriate action.

4.5.5 Virtualization Management Subsystem

The Virtualization Management subsystem comprises server virtualization, storage virtualization, and network virtualization. In the GMS computing and storage environment, resource management is critical to ensure resources are always available to all GMS applications. A significant portion of the GMS functionality will be database driven. Server virtualization converts one physical server into multiple virtual machines, where each virtual machine acts as a unique physical device, capable of running its own operating system. Essential to server virtualization is the monitoring, display and control of server resources such as CPU load and storage activities. Storage virtualization extends server virtualization into a complete computing solution.

4.5.6 Health Management Subsystem

The Health Management subsystem monitors the computing resources such as CPU load and storage activities. All faults/events affecting the health or availability of GMS resources are sent to the Manager of Managers subsystem for display and remedial action. All log files are sent to the Log Management subsystem for further analysis and archival.

4.5.7 Software Management Subsystem

The Software Management subsystem manages, coordinates, and distributes software/firmware loading and patches of the physical servers and communication nodes. Updates to GMS components may be provided through reinstallation, via embedded update capabilities, and through the infrastructure provided by and managed through the software management system. Regulatory rules require operating system patches be done in an expedient manner, especially with regards to security vulnerabilities.
4.5.8 Integration Management Subsystem

The Integration Management subsystem manages the Central Integration and Distributed Integration systems. The Integration Management subsystem allows GMS users, GMS systems, and external systems to define events and rules used by the Orchestration and Event subsystems within the Integration system. The Integration Management subsystem monitors the events, queues, orchestration execution, and other metrics of the Integration system allowing GMS operators to ensure that integration system is working well and take corrective action if necessary. The Integration Management system also provides a mechanism for managing queues within the Integration system, including the ability to create, delete, and flush queues as well as update queue policies and permissions.

4.5.9 Operations Manager

The Operations Manager serves as a manager of managers for the operational systems of the GMS, drawing together views from the Supervisory and Management subsystem and the Optimization Management subsystem in particular, but also from all the other operational subsystems, like the Profiling & Forecasting subsystem and the Economic Interaction subsystem. The Operations Manager allows the operator to manage the GMS’s work, identify and resolve failures, manage global states, and track system resource loading. The Operations Manager provides situational awareness for the operator of the actions of the GMS as a whole.

4.6 Data Repository System

The Data Repository system serves as the historian and librarian of the GMS, providing GMS applications and external systems access to data stored and managed by the GMS system. The Data Repository is specifically a centralized system, providing an archive for selected data, which is preserved with integrity for the long term. As depicted in the following diagram, the Data Repository system is made up of the following subsystems:

- Data Management subsystem
- Central Data Store subsystem
- Archival Data Store subsystem
Data repositories mitigate problems arising from data proliferation and eliminate the need for separately deployed data storage solutions because of the concurrent deployment of diverse storage technologies running diverse operating systems. The Data Repository system provides centralized management for all deployed GMS data storage resources. Note that data access refers to software and activities related to storing, retrieving, or acting on data housed in the overall data repository system.

While individual GMS systems may speak their own language (proprietary, standards-based, etc.) among their subsystems, and sometimes to other systems, one enterprise semantic vocabulary must span all contributions to, and uses of, structured enterprise information in order to achieve cost-effective and flexible business intelligence, analytics, visualization, reporting, and business process automation, as well as other applications that draw upon data from multiple systems. Many of these analytic and reporting capabilities will also be included within procured systems, but it is important that the scope of those capabilities is limited to only the data contained within those systems. If a significant amount of data is required from other GMS systems and/or external systems, then the business intelligence, analytics, visualization, reporting, etc. solutions should be done in the external Business Analytics system, using data from the Data Repository and other systems. GMS subsystems which provide analytical capabilities that require data not native to the subsystem, obtain the necessary data from the Data Repository. The GMS avoids data duplication and replication between subsystems whenever possible.

4.6.1 Data Management Subsystem

The Data Management subsystem manages the data stores which comprise the Central Data Repository. It provides facilities for GMS operators to govern, cleanse, and ensure the quality of data held within the data stores. The Data Management subsystem capabilities include:

- GMS information model design and management
- GMS information model services, including data governance and metadata management
- GMS performance management, to support tuning and scalability of data resources
- GMS data quality services including reporting and cleansing tools
- GMS data repository management and administration including security
- GMS document, record and content management
Note that data warehousing and business intelligence will need data from GMS Central Data Repository. Since Business Analytics is being developed in a separate project, general-purpose analytics functionality is not included in GMS; however, coordination between these projects will be important to ensure seamless integration and usability between the systems.

The Central Data Store will rely on data integration services to synchronize data from many systems, including back office, operations, and front office that store their transactional data in relational databases. Integration is also needed to support data movement into Business Analytics for reporting and analytics.

4.6.2 Central Data Store Subsystem

The GMS Central Data Store is a centralized coordinated collection of databases and other persistence platforms to facilitate achieving the following objectives:

- Provides a cohesive view of all GMS data, regardless of which systems use it. Integration with a central interface improves maintainability and simplifies integration by minimizing the number of translations needed.
- Data integrity is maximized and data redundancy is minimized. This aids in the maintaining of data as accurate and as consistent as possible and enhances data reliability. However, because the system of record will often exist in GMS systems, the Master Data Management (discussed in the Data Architecture section) is required to ensure one version of the truth across the whole GMS.
- Data security is enhanced as a single data storage location minimizes the opportunities to attack the database, and the sets of data that can be stolen or tampered with.
- Optimized data preservation with fault-tolerant setup.
- Generally easier data portability and database administration.
- More cost effective than other types of database systems as storage, labor, power supply, and maintenance costs are all minimized.
- Data kept in the same location is easier to be changed, re-organized, mirrored, or analyzed.
- All the information can be accessed at the same time from the same location.
- Updates to any given set of data are immediately received by every end-user.

The Central Data Store may utilize different database types for various purposes. These database types are discussed in the Data Architecture section.

Note that while “central” is used for describing the logical view of the GMS Central Data Store, the implementation of this store may be physically distributed. The Central Data Store supports structured data from many sources, including distribution automation devices, smart meters, field devices, and external systems. The Central Data Store includes support for both structured and semi-structured data. Some data is stored in their original forms in the Central Data Store for future analysis, without requiring a big effort to design and implement an Enterprise Data Warehouse solution ahead of time. The Central Data Store must support being able to turn unstructured and/or semi-structured data into structured data. When analysis results cross many areas, those results should be stored in a relational or graph database portion of the Central Data Store for reporting and future analysis. The Enterprise Semantic Model can provide the necessary data relationship across domains such that the analysis results can be integrated and have an impact beyond their immediate business functions.
4.6.3 Archival Data Store Subsystem

The GMS Archival Data Store moves inactive data out of the production databases to improve overall performance without losing critical historical data. GMS data archives protect older information that is not needed for everyday operations but may occasionally need to be accessed. As such, data archives consist of older data that are still important and necessary for future reference, as well as data that must be retained for regulatory compliance. Archived data are indexed and have search capabilities so that files and parts of files can be easily located and retrieved. Archiving must meet regulatory and corporate governance requirements with support for data immutability, file system auditing for chain-of-custody, and encryption to prevent data theft.

4.7 Communication System

The Communication system facilitates connectivity and transport of information across all systems of the GMS. The subsystem interfaces with the other communication nodes of the GMS based on IP routing with every device having a unique IP address. In addition to facilitating transport between the different domains, peer-to-peer transport across device and subsystems, the Communication system supports transport across multiple groups comprised of communication nodes spanning Substation, Feeder, Lateral/Edge, photovoltaics, electric vehicles, energy storage, meters, and more. As it is impossible for all routes to be maintained across millions of devices, a hierarchical routing and forwarding information service will be incorporated as part of the overall GMS Communication system. This service enables all communication nodes of dynamically intersecting groups to reliably communicate peer-to-peer, either directly, through exchanges, or redundant paths supported by multiple possible routes with the other members of the group in a time frame that satisfies the system’s control requirements.

The Communication system is composed of the following subsystems as depicted in Figure-12 below:

- A Wide Area Network (WAN) Infrastructure subsystem
- A Field Area Network (FAN) Infrastructure subsystem
- A Local Area Network (LAN) Infrastructure subsystem

The Communication system will ultimately be comprised of multiple sets of WAN, FAN, and LAN technologies. For instance, the Wide Area Network Infrastructure subsystem may include high-speed fiber, 4G cellular, 5G cellular, and dedicated Utility owned cellular, Point-to-MultiPoint, or Point-to-Point systems. Similarly, the Field Area Network Infrastructure subsystem may include meshed networks, long range Point-to-MultiPoint-networks, Power Line Carrier networks, and legacy FAN systems. The Local Area Network Infrastructure subsystem will manifest multiple locally distributed subsystems which may include fiber, Ethernet, and Wi-Fi requiring specific levels of local security or connectivity performance. These different communication subsystems effectively provide a hierarchy of connectivity between the Central, Distributed, and Edge domains.
4.7.1 Wide Area Network Infrastructure Subsystem

The Wide Area Network Infrastructure subsystem provides connectivity services to the Field Area and Local Area counterpart subsystems extending over large geo-spatial areas. The Wide Area Network Infrastructure subsystem can also provide communications directly to Edge devices where either high performance or hard to reach coverage is required.

4.7.2 Field Area Network Infrastructure Subsystem

The Field Area Network Infrastructure subsystem provides the primary connectivity to the field distribution control and monitoring devices. It can also provide connectivity to the Distributed domain’s Local Area Network Infrastructure subsystem.

4.7.3 Local Area Network Infrastructure Subsystem

The Local Area Network Infrastructure subsystem provides localized communication to specific sets of devices integrated into a common subnetwork (e.g. substation, microgrid, residential network, commercial and industrial site).

At the boundary between each network type, transitions related to security, tier of service, routing, and quality of service (QoS) are managed. Communications management, including QoS functionality and route management are contained within the Infrastructure Management System.
4.7.4 Communication System Tiers of Service

The specific technology components of the communication system can be segmented into an extensible set of tiered services, where each service will provide a defined level of performance. Both the Wide Area Network Infrastructure and Local Area Network Infrastructure subsystems provide high and mid performance tiers of service while their Field Area counterpart provides mid and low performance tiers of service. Table 4 depicts a possible segmentation of the different tiers of service and rough order of magnitude performance boundaries. As the system is realized and the natural break points in performance and system requirements are mapped against the available technical solutions, the exact number of tiers may change to match the requirements.

<table>
<thead>
<tr>
<th>Dimension/Tier</th>
<th>High (WAN/LAN)</th>
<th>Mid (WAN/FAN/LAN)</th>
<th>Low (FAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latency/data rate</td>
<td>msec/Gbps</td>
<td>10msec 1 hop, &lt;100 msec net / Mbps</td>
<td>sec / kbps</td>
</tr>
<tr>
<td>Example Technologies</td>
<td>fiber, PTP, 5G</td>
<td>4G cellular, Mesh, PTMP, PTP</td>
<td>PLC, Mesh, long-range wireless</td>
</tr>
<tr>
<td>Device Examples</td>
<td>uPMUs</td>
<td>Dist Control, distributed uPMUs, sensors</td>
<td>battery sensors, hard to reach vaults, locations</td>
</tr>
<tr>
<td>distributed compute power / memory</td>
<td>High (multicore) / GBytes</td>
<td>Moderate (ARM9) / MBytes</td>
<td>Low (ARM7, μController) / kBytes</td>
</tr>
</tbody>
</table>

Table 4

Technologies and tiers will be overlapping and may incorporate multiple types of systems (e.g. wired and wireless). Specific technologies will be defined for each tier and different applications can be mapped to one or more of the tiers depending on their needs as defined by business requirements. The composite set of tiers provides the necessary subsets of communication services to cover all service requirements and also to allow for the relation of the tiers to currently available and future technologies.

The tiers and technologies of the communications services can be related to one another, and compared with each other, through communications dimensions. Communications dimensions specify a range of capabilities or characteristics, including throughput, latency, security, reliability, and coverage that facilitate a mapping of application requirements to tiers of service and vice versa. A minimum set of tiers will be defined that provides the necessary subsets of dimensions to cover all service requirements and also to relate the tiers to available technologies. Specific systems of technologies can be implemented to meet sets of communications dimensions. These implementations provide tiers of communication services. Specific applications can also be defined by sets of dimensions derived from requirements. By recursing (e.g. making repeated use of the communications principles) through possible technology sets and applications sets, an optimum set of tiered communications services can be defined for the GMS.

---

8 In a conceptual architecture, specific performance numbers are not normally defined, but since the "natural" technology breakpoints for the WAN, FAN, and LAN are understood, it is informative to the architecture discussion to set order of magnitude boundaries which will be finalized after all the non-functional requirements are mapped from use cases to applications.
4.8 Integration System

The Integration system facilitates application level or semantic communication between components of the GMS. The Integration system also provides a toolbox for facilitating coordination between GMS components, allowing the creation of ad hoc behaviors within the GMS. The Integration system can be thought of as existing between the three domains (central, distributed, and edge), connecting the other systems together. The Integration system is composed of eight major subsystems:

- a Queuing subsystem which provides specialized message delivery
- a Data Transformation subsystem which facilitates conversion, aggregation, and marshalling
- a Protocol Translation subsystem which translates between different protocols
- an Event Processing subsystem which performs analysis and correlation based on data flows
- an Orchestration subsystem which coordinates and enables compound actions across subsystems
- a Discovery subsystem which allows system components to register, solicit, and advertise services
- a Scheduler which allows the execution of tasks based on time and date
- an Operations Coordinator subsystem which facilitates unified action by the operational components of the GMS

The Central Integration system exists primarily to provide services between systems in the Central and Distributed domains. The Distributed Integration system exists primarily to provide services between the Distributed and Edge domains. The seven of the eight subsystems exist in both the Central Integration system and the Distributed Integration system, though the prevalence of their use varies between the two domains. For example, discovery is likely to be far more important in the Distributed Integration system, while queuing is likely to be richer in capability and used more frequently within the Central Integration system. While not the typical path, both the Central Integration system and the Distributed Integration
system may be used to connect Central systems directly to Edge devices. For the Central Integration system, this is anticipated to happen when advanced Edge systems need direct access to Central systems. For the Distributed Integration system, this may occur when a Central system natively supports a Distributed Integration technology. The Operations Coordination subsystem exists only within the Central Integration system, as it is focused on coordinating between the operational systems in the Central domain.

The subsystems that comprise the Central and Distributed Integration systems may or may not participate in any given transaction. For example, one transaction between an Edge device and the Integration system may include queuing and data transformation, while another may require protocol translation. Some transactions may require the use of all eight subsystems, while others may only require one.

While the Integration system is the preferred method for interfacing different components of the GMS, low latency specialized subsystems such as Protection may forego its use in favor of direct interfacing. The Central Integration system is expected to be realized as an Operations Bus (i.e. a set of Enterprise Application Integration technologies that are explicitly used as the basis for integration). The Integration subsystems will exist both centrally and distributed, but the Distributed Integration system is more likely to exist as a series of discrete components. The GMS architecture assumes the presence of a pervasive Field Message Bus; however, designs such as OpenFMB may be realized as common implementations of a shared protocol (e.g. Data Distribution Services (DDS) or Message Queuing Telemetry Transport (MQTT)) rather than employing a specific piece of infrastructure, as is typical with Central Integration technologies (e.g. TIBCO, WebSphere, etc.).

The Integration subsystems are managed by the Integration Management subsystem of the Infrastructure Management system.

4.8.1 Queuing Subsystem

The Queuing subsystem provides asynchronous message delivery services between components of the GMS. The Queuing subsystem supports a variety of different service levels to facilitate integration of the GMS components. These include:

- Guaranteed delivery
- Timely delivery (e.g. delivery within a given time-to-live, or discard)
- Best effort delivery
- Deliver at least once
- Deliver no more than once

Additionally, the Queuing subsystem provides services such as the batching of messages (note that the batching of messages is distinct from aggregation of data, which is provided by the Data Transformation service), delivery confirmation, and message security. The service levels available may differ between the Central and Distributed Integration systems.

4.8.2 Data Transformation Subsystem

The Data Transformation subsystem facilitates the “in-flight” transformation of data as it flows between systems. This includes conversion from one data model to another as well as selection, distillation, and aggregation activities. Data transformation should be based in the Semantic Data Model whenever possible. For example, the data transformation subsystem could be used to provide five minute summary data from a stream of two second RTU data, or to derive a peak or average value. It can also be used to convert from IEC 61850 data to IEC 61968. System level marshalling and unmarshalling are also provided by the data transformation subsystem.
4.8.3 Protocol Translation Subsystem

The Protocol Translation subsystem translates between different protocols. It is only required when a given subsystem is unable to support the standard protocols used within the GMS. Protocol translation is distinct from data transformation, as protocol translation is only concerned with addressing differences in formatting, not in structure or meaning. However, protocol translation may also require specialized adaptation between protocols with different interaction patterns. Both services may be required when integration is required between different systems. For example, integrating a DNP3 based Intelligent Electronic Device (IED) into an IEC 61850 based SCADA system may require both protocol translation and data transformation. More complex adaptations between protocols may require use of the Orchestration subsystem.

4.8.4 Event Processing Subsystem

The Event Processing subsystem monitors selected flows of data through the integration system to detect events, including complex and inferred events. The Event Processing subsystem analyzes transactions identifying events based on criteria such as type, frequency, and magnitude as well as correlation. Event detection may be requested and configured by the GMS User via the Infrastructure Management system, or by other GMS components. The Event Processing subsystem may work in conjunction with the Orchestration subsystem to initiate an action when an event occurs. Events may be simple as an IED issuing an alert, or as complex as inferring that an electrical network disturbance is occurring, based on a series of message flows.

4.8.5 Orchestration Subsystem

The Orchestration subsystem coordinates and enables compound actions across subsystems. These compound actions may be defined by the GMS User, via the Infrastructure Management subsystem, or by other system components. Compound actions may be needed for a variety of reasons including execution of business processes, integration of disparate subsystems to create derived applications, and automation of manual procedures.

Typically, orchestration of separate subsystems will be slower than a given subsystem natively supporting a desired process. In this regard, use of the Orchestration subsystem trades performance for flexibility. Architecturally, the preferred path is not to use the Orchestration subsystem for any core GMS use case. Rather, the Orchestration system exists to allow the GMS to be flexible and adaptable to unanticipated needs, and to support ad hoc processes that may not warrant the time and expense associated with adding native support.

Note that orchestration and automation are distinct. Within the GMS there will be automated behavior at multiple levels, especially with the Reliability subsystem, but extending to all other GMS systems. Automated behavior by devices working in concert is not orchestration. Orchestration is when the action of devices and subsystems are specifically coordinated by the Orchestration subsystem.

4.8.6 Discovery Subsystem

The Discovery subsystem allows system components to register, solicit, and advertise services. The Discovery subsystem facilitates self-organization within the GMS. Key features of the Discovery subsystem are the ability of system components to register or advertise both their presence and their capabilities, and the ability of components to search for other components and advertised services. For example, a photovoltaic system with integrated communications could use the Discovery subsystem to register its presence, and to discover a source for electrical network connectivity information. Using the connectivity information, the subsystem could determine its parent transformer, and exchange data with it regarding available capacities.
4.8.7 Scheduling Subsystem

The Scheduling subsystem provides a mechanism for executing tasks within the GMS on a periodic basis. The Scheduling subsystem is used internally by GMS components, as well as for user scheduled tasks. User scheduled tasks are maintained through the GMS Operations Management subsystem. The scheduling subsystem supports a rich set of periodicities, including absolute, relative, and offset. It also includes support for holidays and operational calendars to ensure that tasks run at the appropriate times. Scheduled task periodicities can range from seconds to years.

4.8.8 Operations Coordinator Subsystem

The Operations Coordinator subsystem coordinates the actions of the GMS operational systems to ensure that the GMS functions as a single unified solution, even if major GMS components are provided by separate vendors. It prevents the GMS systems from taking divergent, or worse, conflicting action. The Operations Coordinator is autonomous, ensuring that GMS systems do not conflict without requiring operator intervention; for example, automatically delaying a less important but compute or network intensive job during emergency operations.

The Operations Coordinator plays a particularly critical role during “mode” transitions, such as when the GMS as a whole needs to switch from normal operations to emergency operations. Using the Operations Manager (as discussed in the Grid Infrastructure Management section) the operator can identify current work occurring throughout the GMS, and assess the impact of a mode switch. The mode switch can be initiated by the operator through the Operations Manager. The Operations Coordinator then facilitates the ongoing and orderly reconfiguration of the GMS.

4.9 Combined Systems View

Figure-14 below shows a simplified combined system view.
The major systems interface with each other through the Central Integration System. The Distributed Integration System is used primarily by the Reliability and Optimization Systems. The Grid Infrastructure Management System provides cross-cutting monitoring and management services. The Communications System (not pictured), provides the communications fabric necessary for the systems to interact.

5 Domains

As initially discussed in section 3.4, the components that comprise the GMS exist in one of three domains: Central, Distributed, and Edge. While each element will have its own specific features and capabilities, certain characteristics will be driven by the domain itself. The domains within the GMS can be described in general terms, in reference to the types of elements typically deployed within them, and in reference to a set of characteristics common to those elements. For example, the Central domain is the back-office computing environment; it contains applications, servers, firewalls, etc., and it is characterized by a small number of elements in a highly controlled, fault-tolerant environment.

At the highest level, components in the Central domain are generally information technology elements like applications, servers, and routers, whereas components in the Edge domain are generally devices. Distributed domain components facilitate communications and coordination between components. This section reviews the elements associated with each domain and their respective characteristics.

5.1 Central Domain

Components in the Central domain are software applications and the IT infrastructure needed to host and protect those applications: operating systems, servers, routers, firewalls, and the like. Applications are the key actors of the GMS, but without dependable infrastructure they fail. As such, the Central domain provides a fully controlled environment with redundant power, redundant high bandwidth network connections, and disaster recovery locations.

5.1.1 Elements

Applications

Applications are the productivity engines of the GMS in the Central domain, providing the required functionality. In some cases, an application may be the complete embodiment of a GMS subsystem. In other cases, delivering the requirements of a given subsystem may require multiple applications. Applications are deployed on servers. In most cases, applications will have one or more dedicated servers, though these servers may be virtual. Applications are written to run on server operating systems, and assume the presence of the operating system to provide basic services like data persistence and network communications. GMS applications will be instrumented, allowing remote monitoring and management by the Infrastructure Management system; however, it is expected that Central domain applications are not automatically updated, and instead rely on a manual update process when required. This is done because the number of central applications is few relative to distributed components or edge devices; the update process is likely to be specific to a given application; and the risks and operational impacts involved in updating a major application may be large.

Operating Systems

GMS applications will run on either Windows Server or Linux. The operating system instances hosting the GMS applications will be configured to run the minimum necessary services and features, reducing both the attack surface in the event of a cybersecurity event, and number of elements which need to be updated or interact with the application. Operating system deployments within the GMS are standardized, managed, and include standard elements such as third party anti-virus and password management tools.
Operating systems will be managed by the Infrastructure Management system to ensure they are regularly patched and running properly.

**Databases**

GMS applications will depend on a variety of databases, including embedded databases, relational database management systems (RDBMS), and online analytical processing (OLAP) engines, as well as large scale data warehouses, data lakes, and big data clusters. Where possible, like operating systems, database engines will be deployed in a standardized, consistent fashion, and managed through the Infrastructure Management system to ensure they are patched and running properly.

**Servers**

Servers may be real or virtual, though clearly virtual servers eventually must be hosted on real servers. Servers are the base building block for provisioning computing resources within the GMS, providing a mechanism to make processing power, memory, and storage available to applications. Many GMS applications will require a dedicated server instance.

**Containers**

GMS applications may be deployed using container technology (e.g. Docker), facilitating application isolation without the full overhead of virtual machines. Containers are the preferred mechanism for facilitating “Dev-Ops” style transitions between development and production environments.

**Routers**

Routers in the Central domain are largely transparent to the GMS, with the exception of the role they play in security. Specifically, routers segment the network and terminate VPN links.

**Firewalls**

Firewalls facilitate an overall defense-in-depth strategy and advanced threat prevention. Firewalls are used to allow traffic between trusted and untrusted network segments only if that traffic meets certain criteria. Firewalls can also perform deep packet inspection, and monitor connection states. This will be critical to the GMS, as applications and other elements in the Central domain will need to communicate with less trusted or untrusted networks to work effectively.

5.1.2 **Characteristics**

**Redundant and Fault Tolerant**

Components in the Central Domain are deployed in a redundant, fault tolerant fashion. This includes both local redundancy through clustering or virtualization, as well as failover capabilities to a disaster recovery site. Individual Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) will be determined for each Central domain component. The RTO and RPO will determine the specific requirements, and, by extension, the type of supporting technology used to support those requirements.

**Global Perspective**

Elements in the Central domain have a global view of the status of the electrical distribution network and GMS’s supporting systems. This global view potentially allows elements in the Central domain to make more informed decisions; however, this is counterbalanced by the fact that data in the Central domain may have been summarized or aggregated, and it may not be as timely as data available in the Distributed or Edge domains.

**Concentrated**

The Central domain is concentrated. While there are many Central domain assets, they exist in just a handful of locations. This makes disaster recovery and failover capabilities critical.
5.1.3 Users

Operator
Operators use GMS components in the Central domain to manage the electrical distribution system. Most operators will have subject matter expertise in one or more particular aspects of the GMS: reliability, optimization, planning, or market operations. GMS applications are likely to be foundational tools for performing their duties.

IT Staff
IT Staff maintains the applications, servers, operating systems, databases, and network technology of the Central domain. The intricate nature of the GMS technology in the Central domain, such as the Data Repository system and the Integration system, will require ongoing IT maintenance and support.

5.2 Distributed Domain

The Distributed domain is a key enabler of federated control and optimized management. If bandwidth, reliability, and economics were such that all edge devices could always communicate directly and quickly with the Central domain and with each other without an intermediary, the Distributed domain might not be required at all. The Distributed domain is effectively the space between edge devices and the Central domain, providing a place for computing and communication to occur without the overhead of returning to the central domain, and without the limitations in resources and perspective typical of an edge device. The Distributed domain is particularly important when the need for fault tolerance and fast response times is considered. Performing selected functions in the Distributed domain allows the GMS to continue operating, even when portions of it are disconnected, unreachable, or unavailable.

The Distributed domain is composed primarily of the computing and communications platforms that facilitate the interconnection between the Central and Edge domains. As such, it includes routers, RTUs, distributed servers, and other devices in the middle of the network.

The Distributed domain includes both information technology elements and embedded elements. For example, a distributed optimization application may run on a server, or a router, or directly on a field device. It may also run across a group of peer devices sharing local information and making local optimized control decisions based on predefined configurations. The Distributed domain application is distinguished not by the form factor of the platform it runs on, but by the scope and breadth of its influence, lacking the global nature of applications in the Central domain, but extending beyond the singular nature of an Edge device.

5.2.1 Elements

Routers
Routers in the Distributed domain function both invisibly to route and segment traffic and visibly as platforms. As a platform, routers may provide a place to execute SCE or 3rd party provided code, allowing distributed processing.

RTUs and Gateways
RTUs and Gateways connect the GMS to edge devices without native GMS communications capabilities. When RTUs and Gateways are connected to multiple edge devices, or implement distributed intelligence they can serve as Distributed domain platforms. Note that when RTUs and Gateways are paired with a single edge device they are considered part of a compound edge device. See section 5.3 below for further discussion.
**Servers**
Servers may be deployed in the Distributed domain to provide regional or distributed compute capabilities. For example, a server might be deployed in a substation to provide a platform for running a Reliability application locally. This could be particularly valuable in the event that communications links to the Central Reliability subsystem were down. This might be done as part of an overall system resilience strategy. As in the Central domain, servers may be real or virtual.

**Containers**
Containers can be particularly important elements in the Distributed domain, as they can provide isolated environments for running distributed grid applications without the overhead of full virtualization. Containers will allow centralized development and deployment of new distributed applications.

**Applications**
Applications may be deployed on a variety of distributed platforms. Distributed applications may work in conjunction with central applications to provide a hierarchy of functionality, or they may stand alone, providing independent regional functionality.

**Firewalls**
Firewalls also exist in the Distributed domain, providing the same services that are required in the Central domain: filtering, protection, isolation, and inspection. Firewalls in the Distributed domain are likely to be integral, rather than standalone.

### 5.2.2 Characteristics

**Regional Perspective**
Elements in the Distributed domain can be considered “regional” in nature, meaning that while they lack the global awareness of system status and components held by elements in the Central domain, they have information from more than a single source. This regional view may be quite large (spanning multiple substations), or quite small (a neighborhood microgrid), but regardless of size, allows coordinated action between multiple edge devices.

**5.2.3 Users**

**Field Personnel**
Distributed components may be integrated into field equipment such that troubleshooting requires not just a laptop, but a bucket truck as well. Distributed components must be maintainable by field personnel, including those with limited computer skills. The design implication is that support tools for the distributed space must be accessible to a rich variety of users, and must prioritize returning devices to a connected state so that they can be maintained over the network by advanced operators.

**Substation Operators / Managers**
Operations personnel are primarily concerned with the safe and efficient operation of their assigned assets. GMS components installed in the substation must enhance and not distract from this mission.

### 5.3 Edge Domain

The Edge domain is populated with devices. This includes protection devices such as circuit breakers, protection relays, intelligent switches, and reclosers; optimization devices such as capacitor bank controllers, voltage regulators, and load control devices; and distributed energy resources such as electric vehicles, photovoltaic arrays, and advanced storage. These devices may include integrated communications, or may be tied into the GMS via an intelligent communications module. In either case,
devices in the Edge domain include communications, computing, and some combination of local actuation and sensing for the electrical distributions grid.

Edge devices can be broadly split into three categories:

- Traditional
- Instrumented
- Intelligent

Traditional devices are effectively stand-alone. While some may be programmable, these devices generate energy, protect a circuit, or provide other beneficial services to the grid using only locally available information, and without communicating status to remote systems. Even as more sophisticated devices are available, simple devices like fuse cutouts and mechanical switches will continue to be a critical part of the SCE distribution system for years to come. Traditional devices can be particularly challenging in the context of the GMS, as they rely on human action to maintain and communicate current state information. Replacing every traditional device with an instrumented or intelligent device is both impractical and prohibitively expensive, but a failure to complete a manual process may leave the GMS with inaccurate state information.

Instrumented devices provide the same capabilities as traditional devices, but also provide dynamic status information to upstream systems. Instrumented devices can indicate directly that they have taken an action or are generating power, rather than relying on SCADA technologies to infer it. Note that a traditional protection device may be externally instrumented to provide a combined instrumented offering.

Intelligent devices are capable of communicating dynamically with other intelligent devices to make decisions on the optimal action. For example, an intelligent inverter might exchange state information with an intelligent protective relay to determine the feasibility of undocking during a period of grid instability. Intelligent protection devices often include automatic fault location and restoration capabilities.

All three types of Edge devices are fundamental to the GMS, but the interactions available between the Distributed and Central domains and the Edge devices vary based on type. Traditional devices will take action irrespective of other independent devices, or the systems in the Distributed and Centralized domains. Instrumented devices will also take independent action, but may be monitored by the systems in the Distributed and Central domains. Intelligent devices work with systems in the Distributed and Centralized, as well as other intelligent devices in the Edge domain to take coordinated action.

### 5.3.1 Elements

As discussed above, there are broadly three types of Edge devices: traditional, instrumented, and intelligent. When considering the elements within the Edge domain, it is helpful to recognize that there is often an electrical or mechanical device coupled with an electronic controller and some form of sensing: the capacitor bank with a switch and the capacitor bank controller; the voltage regulator with the voltage regulator controller and a voltage sensor; the overhead switch with the automatic switch operator. For the GMS, both the electronic controller and the electromechanical device are important. It is not sufficient for the controller to have received a command and acted upon it. The actuator itself must have completed its operation, and the system must be able to verify this completion. As this equipment evolves, it is likely that in more and more cases the controller and the electromechanical unit will be a single device; however, there is sufficient deployed equipment that the GMS must support them as separable elements for the foreseeable future.
Communications Modules
Communications modules provide the ability to link devices to the field area network. Additionally, GMS field area network communications modules will include the ability to run applications locally. This will be particularly important when coupled with less sophisticated grid devices. The communications module may be the primary source of intelligence and point of interaction with the GMS. The communications module may be responsible for translating vendor proprietary information to/from a standards based form as well as interfacing with the physical communications layer.

Protection & Optimization Devices
Protection & optimization devices include circuit breakers, relays, reclosers, fuses, switches, tap changers, voltage regulators, fault indicators, capacitor banks, line sensors, and phasor measurement units. In the context of the GMS, instrumented and intelligent protection and optimization devices provide the most dynamic and responsive capabilities, but the state of traditional devices remains important for effective grid management.

Distributed Energy Resources
The active and potentially controllable Distributed Energy Resources include photovoltaics and inverters, wind generators, rotating mass generators, electric vehicles, energy storage systems, and demand response. Distributed Energy Resources may be directly manageable (for example using the CEC Rule 21 inverter interface), or they may operate solely based on line conditions and predetermined rules such as IEEE 1547.

Applications
Applications may be installed on Edge domain devices. These applications may work in conjunction with each other, and with applications running in the distributed domain to provide a distributed application. Alternatively, they may operate stand alone, having minimal or no interaction with other applications.

5.3.2 Characteristics

Local Perspective
Elements in the Edge domain are inherently local. The Edge component measures, controls, or protects the thing or things (typically electrical components of the distribution grid) it is directly connected to.

Diffuse
Individual elements in the Edge domain are spread throughout the entire service territory. While in some cases, data or control capabilities from one element may be substituted for another, most elements in the Edge domain are not redundant. When a failure occurs, data and control capabilities are lost, but the diffuse nature of the Edge domain means that loss is limited to a very small portion of the overall system.

5.3.3 Users

Field Personnel
The Edge domain is maintained by field personnel. Beyond ensuring that the electromechanical aspects of protection and optimization devices are safe and effective, field personnel must be able to establish and verify connectivity between intelligent and instrumented devices and the field area network. Advanced configuration is likely to be performed by system operators over the network.

Consumers
Consumers may be direct purchasers of DER. Actions by the utility may limit or enhance the usefulness and effectiveness of electric vehicles, storage, and photovoltaics. Additionally, while the consumer may
be the purchaser and maintainer of DER equipment, the utility will still be held accountable for safe operation of the distribution grid.

**Aggregators**

Aggregators may provide DER to consumers, and manage those resources on their behalf. Aggregators seek to maximize their financial return. The development of tariffs, regulations, and market systems which enable the use of DER for grid services, such as VAR support, will be critical to ensuring the safe and stable operation of the grid with high penetration of DER, and continued cooperation by aggregators.

### 6 Design Principles

This section presents the design principles deemed applicable for the development of the GMS architecture, and recommended for the engineering and procurement of the GMS.

#### 6.1 Safety and Compliance

When designing, installing, configuring, or operating the GMS, it will be designed in a manner that fully incorporates safety and compliance. Safety is the prime consideration in every aspect of the way the GMS is designed and operates the electric grid. GMS needs to fail both safe and operating, delivering power to customers in a safe and reliable fashion regardless of the state of the GMS or the environment it operates within. Safe grid operations is the prime consideration in the design of GMS, followed by reliability, resiliency, and other factors. Compliance to a large extent defines the objectives for all aspects of the GMS and the system has to be able to incorporate the compliance rules as part of the architecture, realizing that regulations and laws that define that compliance are ever changing.

#### 6.2 Standards & Application Specific Profiles (ASP)

Wherever possible, the choice of specific technologies will be based on their support of industry standards. The use of standards based technology has many benefits including: multi-vendor sourcing, multi-vendor interoperability, backwards compatibility, extensibility, and graceful migration to future technologies. The standards bodies that are recognized include (but are not limited to): ANSI, IEC, IEEE, IETF, ITU, Open Group, and other similar organizations. In the absence of industry standards for a specific needed technology, minimal non-standard optionality will be employed.

Because so many of the current standards have multiple options for the vendors to choose from, the GMS will be setup to support particular Application Specific Profiles (ASP) for each protocol used. The ASP will select a single option from the standard at each point that one or more options exist in the standard, such that vendors will know the specifics of how the GMS expects devices to report and behave when attached to the GMS. The GMS will be agnostic to how the vendor meets the ASP requirement, but the GMS will expect the vendor to meet the ASP requirements at all interface points. Wherever possible the ASPs will be provided to a neutral third party for use in testing proposed devices, equipment, and software that will interact with or be part of the GMS. When a detailed ASP is not available, a local profile will be defined by SCE such that internal compliance can be maintained across vendors, and also to create the artifacts necessary to move the industry to a more formal industry alliance supported interoperability model. The selected ASP(s) shall be used by industry certification bodies or SCE labs to hold the vendor community to interoperable compliance.

The use of ASPs is critical to the GMS, as the alternative is to accept proprietary systems, vendor lock-in, and a limited or impractical path for technologies to evolve and extend over time. Interoperability, backwards compatibility, and extensibility are key tenets of the overall system. Maintaining compatibility through standards allows for older systems to migrate gracefully to newer technologies, and
provides a path for future technologies to be added over time without service disruption or forklift upgrades.

6.3 **Intelligence**

Unlike many of the existing Distribution Management Systems and Energy Management Systems, the GMS will be designed to push the intelligence and computing environment as close to the device as it is reasonable to do. For applications like system protection, the Central domain may only know that the relays have specific parameters set and that the relays have tripped. The actual decision to trip may be completed at the device level. Autonomous decision making with reporting after the fact may happen at both the Edge and the Distributed levels, with the operator only seeing that an action has been taken and why. While this intelligence will exist at the Edge and the Distributed levels, the expectation is that sensors will still report readings to the Central domain for use by apps, analytics, and operators, including verification of equipment positions (e.g. a switch’s current setting) and the mode of operation for the device (e.g. daytime, allow reverse power flow for a relay).

6.4 **App Architecture**

The GMS will be designed with the idea that the basic core of the system can be extended with a simple app, similar to what is found in mobile architectures. This structure will have a common set of services that can be provided to any app. Apps will be deployable at the Central, Distributed, and Edge domains, though they may have different behavior depending on the domain(s) in which they are deployed.

Localized computing algorithms may encompass a wide variety of functionality. Some of the possible functionality includes peer-to-peer communication sessions, field bus-like services, local processing and analysis of incoming SCADA and other data, real-time responses to electrical network events, enhanced security functionality not already resident in the device, and tools for network operations.

The ability to make use of future unidentified Apps enables GMS to continue the deployment of innovative functions and services in a cost effective, fast-to-market manner. An open architecture for App development and execution broadens the community of potential developers which enables innovation.

6.5 **Common Dataset**

Wherever possible, the GMS and its apps will draw from a common dataset that is available to all apps. The common dataset will include both external data from other sources (e.g. weather) and data gathered internally by the components of the GMS system.

6.6 **Pre-Calculation**

Wherever possible, the GMS will pre-calculate values, forecasts, profiles, and other information that will allow the system to off-load extended calculations to overnight operation. Renewable energy sources are variable in nature and highly weather dependent. In SCE’s service territory, the dominant source of renewable generation is photovoltaics. As a result, system operations on a typical day will tend to be more complex during daylight hours than overnight. Overnight pre-calculation will maximize the responsiveness of the system during the most sensitive operational periods.

6.7 **Groups & Regions**

Whenever possible, GMS will support the use of groups and regions. Groups are a way to operate or visualize equipment or devices as a set. Actors will have the ability to define any arbitrary group within the GMS. GMS users will be able to operate on a group, as well as the intersection, union, or relative
complement (difference) of two or more groups. Regions are geographic areas on a map that an operator may define on a map in some arbitrary fashion. The GMS will also support predefined regions, such as city limits or climatic zones that are known to be useful for grid operations.

6.8 Performance
Whenever possible, GMS will be designed to support round trip performance that is within the operationally significant interval for the activity or equipment in question. For capacitor bank operations that might be ten minutes, while for a system protection action it might be less than one second. The GMS will be able to operate for each of these different intervals and prioritize resources for each application depending on the needed performance. The GMS will actively measure performance and manage the allocation of resources as needed.

6.9 Data Validation
The GMS will have the ability to validate data from all devices and from all external sources. This includes the ability to do traditional VEE (validation, estimation, and editing) and other numerical validation needed to prevent operations on corrupt or invalid data. The GMS shall archive the raw data when correction is done and use the corrected data.

6.10 User Interface Portability
The GMS will provide a user interface that is capable of being used on a wide range of different devices from mobile phones to tablets to computers.

6.11 Usability
The GMS will be designed for ease of use for not just the operator, but for engineers, planners, GMS maintainers and other users. The GMS will provide a user interface that allows users to intuitively interact with the GMS, in a fashion that does not have a steep learning curve. Additionally, the GMS will support “expert” modes of operation which allow skilled system operators to efficiently execute operations with minimal user interface interaction.

6.12 Maintainability
The GMS will be designed to be easily maintainable. The system will have appropriate fault monitoring on its servers, databases, and applications such that a monitoring console for the health of the GMS is available for review. The GMS will have detailed logging for errors and abnormal conditions that the system itself sees in operation (not the equipment or communication with the equipment installed in the grid, but the GMS internally). The GMS will meet or exceed the IEEE standards for commenting and documentation. The GMS platform and all GMS apps will have full test harnesses and regression capability for testing changes. The GMS will be managed in a five level environment:

1. Sandbox - for testing new ideas and code
2. Test environment - where the full test suite is run on patches and updates
3. Staging environment - where code that is deemed ready for deployment can run on the real world data in a shadow mode
4. Operational environment - where the live GMS applications are run
5. Reversion environment - where the last deemed operational code is available should there be a need to revert.

Note: There may be multiple instances of these environments. This is especially likely for sandbox and test environments to facilitate testing of various scenarios.
6.13 **Modularity**

Wherever possible, the GMS will be designed to be highly modular with well-defined interfaces based on industry standards and Application Specific Profiles; each module will function like an app on a mobile phone or a tablet. The goal of the modularity is that each module be able to support a business function.

6.14 **Reusability (Ability to Call)**

Wherever possible, the GMS will be designed so that a module can call another module or routine. This is not inheritance like one finds in Java, but rather the ability to use an “Application Programming Interface (API) call” to feed data to another module and pull the results for further processing, decisioning, or display. Modules and interfaces will be fully documented, including example code, assumptions, pre-conditions, post-conditions, and side-effects. They will also be subject to change control to ensure that updates to GMS sub-components do not degrade the overall system.

7 **Cybersecurity**

Cybersecurity is the ability of the system to remain operationally available to SCE and to ensure the integrity of the data, messages, and actions of the GMS, and the systems and subsystems that comprise it. Cybersecurity also includes ensuring that confidential data remains confidential, that users and system elements are fully authenticated, that only authorized actions are taken, and that appropriate audit logs are recorded. This ability must persist even when the system is under active attack, running in a non-standard or degraded mode, or both.

Cybersecurity is fundamental to the GMS. Security is a systemic concern. Security failures are often cumulative in nature. An attacker compromises one aspect of a system component and uses that access to compromise another aspect of the component. Once a component is compromised it can then be used as a staging point to compromise other system components. Preventing this from happening requires that security be considered across all aspects of the GMS, and that breakpoints exist between GMS components. Specifically, cybersecurity must include:

- Device Security
- Network Security
- Database Security
- Operating System Security
- Application Security

Across each of these cybersecurity domains the information security fundamentals of Confidentiality, Availability, Integrity, Authentication, and Authorization must be considered.

7.1 **Security Principles**

A series of cybersecurity design principles inform the overall approach to security taken within the GMS. The nature of systems design is to require tradeoffs. The GMS must balance risk, cost, maintainability, and usability to provide a system that is functional and secure. At points, support for some principles may be limited in favor of others that are deemed more important. All other things being equal, designs which address these principles are preferred to those that do not.

- No Cascading Failure -- A security failure within one component must not (in and of itself) result in general system compromise.
- Least Privilege -- Grant users, systems, and devices only enough access to accomplish their tasks.
• No Proprietary Algorithms -- Cryptographic algorithms shall be published, publicly vetted algorithms. The solution shall not use cryptographic suites deprecated by the National Institute of Standards and Technology (NIST).
• Economy of Mechanisms -- Use the fewest and simplest methods to accomplish a task.
• Assume External Systems are Insecure -- Systems and devices that the GMS interfaces with should be assumed to be untrusted and a potential source of attack.
• Protect Information at All Times -- Whether information is in process, in transit, and/or at rest, it should be protected.
• Layered Security -- Apply cybersecurity at multiple layers, such that if a given mechanism is defeated, the system is degraded, not owned.
• Audit -- Actions taken by the system (security or otherwise) shall be fully auditable.
• Comprehensive Authentication -- Authenticate all users, devices, and systems which interface with the GMS before allowing any access.
• Unique Identities -- Every user, system, and device which interfaces with the GMS must be uniquely identified. Cryptographically verifiable identification mechanisms are preferred.
• Separation of Duties -- Sensitive tasks should require multiple operators, such that a single user identity cannot be used to deliberately or inadvertently take down the system.
• Proportional -- Over-protecting systems is just as problematic as under-protecting systems. The means used to protect a given portion of the GMS shall be appropriate for that which is being protected.

7.2 Controls

Security controls are mechanisms which ensure the security of a given system, preventing, avoiding, and detecting misuse. Security controls can be classified many ways. One classification scheme is to break security controls into management, operational, and technical controls. Management controls are the policies, procedures, and standards which address security. Operational controls are the actual execution or actions taken by the organization. Both of these are distinct from technical controls, which are specific behaviors built into implementations which facilitate security. By way of example, a policy which indicates exterior doors are to be locked is a management control, the security guard checking all the doors daily to ensure that they are locked is an operational control, and the lock itself is a technical control. Any of these controls individually may be effective. Collectively the controls reinforce each other, making it more likely the overall security objective is achieved.

There are a rich set of documents which detail security controls for utilities. NIST IR 7628\footnote{http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf} and NIST SP 800-82\footnote{http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf} both provide a comprehensive set of management, operational, and technical controls that could be applied to Smart Grid (SG) Systems. NERC CIP\footnote{http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx} goes farther, mandating specific requirements to utilities for FERC regulated critical infrastructure assets. These standards consider controls comprehensively, considering many facets of utility operations and all stages in a system’s lifecycle.

NIST IR 7628 describes almost two hundred security controls in nineteen “families”:

- Access Control (SG.AC)
- Awareness and Training (SG.AT)
- Audit and Accountability (SG.AU)
- Security Assessment and Authorization (SG.CA)
● Configuration Management (SG.CM)
● Continuity of Operations (SG.CP)
● Identification and Authentication (SG.IA)
● Information and Document Management (SG.ID)
● Incident Response (SG.IR)
● Smart Grid Information System Development and Maintenance (SG.MA)
● Media Protection (SG.MP)
● Physical and Environmental Security (SG.PE)
● Planning (SG.PL)
● Security Program Management (SG.PM)
● Personnel Security (SG.PS)
● Risk Management and Assessment (SG.RA)
● Smart Grid Information System and Services Acquisition (SG.SA)
● Smart Grid Information System and Communication Protection (SG.SC)
● Smart Grid Information System and Information Integrity (SG.SI)

While necessary for the deployment of the GMS, management and operational controls are beyond the scope of the GMS architecture definition. This section specifically focuses on high-level technical controls to be supported by the GMS. It is expected that appropriate management and operational controls will be developed to support, guide, and maintain these technical controls. Furthermore, given that a catalog of specific controls has been explicitly defined in various industry standards, this section considers methods for providing technical controls, rather than the controls themselves. These methods for providing technical controls can be further divided into two broad categories: preventive and detective. Specific guidance on controls will be more fully developed in the System Requirements document.

7.2.1 Preventive Methods

Preventative methods are technologies and architectural techniques which prevent an actor from misusing a system. These controls vary widely from encryption of data which prevents confidential data from being exposed, to access controls which restrict access to systems, to physical features of a product. Most preventative technical controls use one or more of these methods:

● Limiting Attack Surface
● Physical Hardening
● Segmentation
● Authentication and Authorization
● Integrity Checking
● Encryption

Limiting Attack Surface is the technique of minimizing what is exposed to actor and other systems which interact with a given system or subsystem. The fewer interfaces available, the less there is to attack. This technique is valuable both internally and externally valuable, as it can aid in system segmentation as well.

Physical Hardening ensures that system access and sensitive materials cannot be obtained simply because an actor has physical access to a system. This can include locks, sealed enclosures, conformal coatings, buried circuit traces, and specific security components and design principles in the electronics used to monitor and operate the grid. It also includes disabling manufacturing and programming interfaces.

Segmentation is breaking the system into a series of subsystems, components, applications, and application sub-components, which each have distinct security perimeters. If a given portion of the system is attacked and compromised, it is only able to access other portions of the system through well-
defined interfaces with limited access rights. The attacker must mount another attack to move further within the system, rather than obtaining blanket access.

Authentication and Authorization is verifying both the identity of an actor interacting with the system, and the access permissions granted to that actor. This verification is typically done cryptographically, though it can also involve physical tokens such as keys, fobs, or badges.

Integrity Checking is ensuring that messages, data, and programs have not been tampered with. Commonly this is done using hashing algorithms or digital signatures.

Encryption underlies most cryptographic security mechanisms, including many authentication and integrity techniques. When used directly and correctly, encryption can ensure the confidentiality of data, preventing actors from obtaining information, even if they have physical access to the files, network, database, message, or device which contains it.

7.2.2 Detective Methods

Detective methods are technologies and architectural techniques which allow the system to detect and report when it is being used in some anomalous manner. Detective methods include:

- Logging
- Alerting
- Monitoring
- Correlation

Logging is the act of recording what was done by or to the system, who or what performed the action, and the time of the action. Logging serves a rich variety of purposes beyond cybersecurity, including debugging and data recovery. When coupled with integrity methods, logging can provide non-repudiation of events.

Alerting is proactively informing an operator, actor, or system component when an event occurs. Alerting enables responding to anomalous rather than merely recording them.

Monitoring is the act of observing and recording the environment in which the system exists. Monitoring can be used to detect potential nascent attacks.

Correlation is the process of analyzing logging, monitoring, and event data to discover patterns and determine if events are deliberate and persistent in nature.

These detective methods, in conjunction with the preventative methods above, provide the foundation for creating specific security controls which can be used to ensure that the system detects, recognizes, and reports misuse. Additionally, detective methods can be coupled with preventive methods to provide an automated response to security events.

7.3 Shared Cybersecurity Subsystems

While security is a pervasive concern within the GMS, requiring each subsystem to provide its own implementation of all security services would be inefficient at best. Worse, providing comprehensive security would require federation across multiple security implementations, increasing the available attack surface and the likelihood of a breach or failure due to mismanagement or misconfiguration. Given these concerns, the GMS will provide a set of shared cybersecurity subsystems which can be used by other GMS systems and subsystems.
7.3.1 User Management Subsystem

The User Management subsystem provides authorization services to other GMS systems and subsystems. This includes a centralized user directory for identity, group, and permission management. The User Management subsystem allows the GMS to provide strong role-based access control without requiring local user management implementations. Simultaneously, the User Management system facilitates central management of user permissions. System administrators can use the User Management subsystem to obtain a single comprehensive view of the permissions granted to a GMS user, and to alter those permissions as necessary.

7.3.2 Password Management Subsystem

The Password Management subsystem provides user authentication services to other GMS systems and subsystems. This includes support for multi-factor authentication, password policies, and selective login controls, such as time of day and concurrency restrictions. The Password Management subsystem allows single sign-on by GMS users, and supports identity federation for subsystems which cannot integrate with it directly. The Password Management system also include tools for managing shared administrative accounts (e.g. “Administrator” or “root”), allowing administrative users to authenticate with their personal accounts.

7.3.3 Cryptography Subsystem

The Cryptography subsystem manages the keys and digital certificates required for cryptographic operations. This includes generating, issuing, distributing, updating, and securely destroying both symmetric and asymmetric keys. The Cryptography subsystem provides large scale cryptographic credential management, with the ability to manage all of the keys for every device within the GMS. The Cryptography subsystem also tracks cryptographic credential lifetimes to inform and assist the GMS operator in consistently maintaining GMS security policy.

7.3.4 Segmentation and Filtering Subsystem

The Segmentation and Filtering subsystem facilitates the creation and management of security partitions with the GMS. By managing VLANs, VPNs, Network Virtualization, firewalls and routers, the Segmentation and Filtering subsystem prevents security compromises from cascading through the GMS. The Segmentation and Filtering subsystem allows the creation of a “zero trust” computing environment in which systems are automatically isolated from each other. The Segmentation and Filtering subsystem also manages isolated execution environments when necessary for specific security purposes. This allows centralized management of trusted execution environments and similar technologies, such that uniform security policy can be enforced across multiple devices and computing environments.

7.3.5 Security Configuration Management Subsystem

The Security Configuration Management subsystem manages the security configurations of operating systems used across the GMS. This includes security services such as anti-virus, anti-malware, group policy enforcement, and application whitelisting. The Security Configuration Management subsystem works to ensure that only trusted applications are allowed to run within the GMS environment.

7.3.6 Security Event Detection Subsystem

The Security Event Detection subsystem provides auditing and log correlation services. The focus of the Security Event Detection subsystem is specifically on events that have security implications. Log correlation allows detection of coordinated and low intensity but persistent attacks. Auditing provides records of both authorized actions and attempted unauthorized actions.
7.4 Risk Based Approach

Cybersecurity work is inherently asymmetrical: attackers only have to be “right” once. Defenders must be constantly vigilant, delivering flawless systems if they are to be truly impregnable. Perfection is unachievable in a system with the size and complexity of the GMS. Given these realities, pragmatic cybersecurity must be risk driven. Risk, defined as the probability of loss multiplied by the magnitude of loss, must be used to determine which assets warrant the greatest protection. When risk is measured economically, it becomes possible to compare the cost spent on protecting the system with the value of element being protected.

8 Data Architecture

Data is fundamental to the operations of the GMS. The GMS must deal with rich and diverse sets of outside data, such as weather forecasts and economic conditions; high volumes of internal data, such as telemetry data; and large amount of self-generated data, such as forecasts and state estimations. Data exists to serve the operational needs of the applications which comprise the GMS, but if not carefully managed it can become a barrier to integration and a drag on performance. As with many enterprise utility systems the GMS follows a formal data lifecycle process based on industry standard data models. To ensure optimal performance, the GMS uses data storage technologies and formats tuned for the tasks at hand, and partitions data between the Central Data Repository and other subsystems. The electrical network model is of particular importance within the GMS and has some special architectural features.

8.1 Data Mappings & Lifecycle

The industry has developed a comprehensive set of models describing utilities assets (model types of equipment and specific purchased instances) and their relationships. Standards such as IEC 61968 and IEC 61850 both provide logical data models. Interface models like Multi-speak capture the data requirements for specific transactions. The GMS will use these standard models as the basis for integration and interfacing.

In order to ensure ongoing integration and coordination, SCE will implement a Reference Data and Master Data Management process in the development and deployment of the GMS. This process will ensure that within the GMS, there is a single version of the truth. The Master Data produced by this process will be used to facilitate integration with the rest of the enterprise.

The GMS relies on the use of a common semantic model across systems and subsystems. Individual applications within the GMS may use other models internally, but transactions with the Data Repository must use the Semantic Data Model. The GMS uses a Semantic Data Model based on industry standards to drive the design of both integration services and data services. This ensures that what is exposed to the enterprise from the GMS is a consistent representation of the data and information managed by GMS. The GMS Semantic Data Model serves as the basis for the Master Data model implementation, as well as all GMS interfaces and integration.

8.2 Data Frequency and Periodicity

The electrical grid operates on a real-time basis, but the data required for the GMS has a wide range of periodicities and update frequencies. On one extreme, measurements from grid devices may be collected on a four second (or less) basis, and streamed to GMS live. On the other extreme, cartographic data may be static for the entire life of the system. To provide clarity and avoid design conflicts, data within the GMS can be considered to fit into one of six categories: Flow: Measurement, Flow: Heartbeat, Status, Derived, Reference, or Foundational:
Data Category | Data Rate | Source | Stored | Examples / Notes
--- | --- | --- | --- | ---
Flow: Measurement | Time series data provided on a fixed periodicity. May be as frequent as every second. | Devices & Systems | In most cases | Measurement data from RTUs and other sensors. May be examined in flight by the Event Processing subsystem.
Flow: Heartbeat | Heart-beat or keep alive messages sent on a fixed periodicity to report status or maintain a communications link. | Devices & Systems | No | May be examined in flight by the Discovery or Event Processing subsystem.
Status | Updated with each device or system change. No fixed periodicity. | Devices & Systems | Yes | May be “unknown” if communications are lost. May be examined in flight by the Event Processing subsystem.
Derived | Based on analytics such as state estimation. | Analysis | Yes | Some derived data will be produced on a periodic basis, making it similar to flow data. Other derived data will be produced on an as needed basis. Derived data may be generated regularly to provide status for “hidden” areas of the network, or to true up the electrical network model. It may also be generated to replace Status data when communications are unavailable.
Foundational | For practical purposes does not change. | Manual entry or update from external reference source | Yes | Topography, street maps, physical characteristics of devices. If this data is changing regularly, it is probably Reference data, not Foundational data.

Table-5

8.3 Partitioning

The GMS will have defined systems of record for all relevant data. That is, as part of defining the data architecture of the GMS, specific systems and subsystems will be identified as the owner/generator of particular data elements. Data that is required within a single system or subsystem, and does not have a broader purpose or regulatory requirement for archiving may be retained in that system or subsystem alone. Data which is broadly used will be persisted to the Central Data Repository. Whenever possible, the Central Data Repository will be both the system of record and system of engagement for broadly used data. In select cases it may be necessary for systems or subsystems to work with local data stores which are synchronized with or persisted to the Central Data Store separately.

Generally, the preferred architecture within the GMS is to obtain data from the system of record directly, rather than maintaining and synchronizing additional copies. The known exception to this is subsystems within the Distributed domain. Many Distributed subsystems must be able to continue to operate when communications are unavailable. Because of this they are expected to cache needed data as a matter of normal operations, though they should seek fresh data from the system of record whenever it is available.
8.4 Formats

Data will need to be exchanged both within the GMS and with external systems. To facilitate this, the GMS will need to support a variety of data formats. Internal formats, such as those used between GMS systems and over the FAN with devices, will favor compact and efficient representations. External formats will be determined based on ease of interfacing, provided performance requirements can be met.

8.5 Technologies

The GMS will use a variety of different data technologies to ensure efficient and optimal performance. No one technology is currently envisioned to be able to support all of the functions of the GMS. Relational and time-series databases remain a critical technology, but newer technologies such as graph databases and geospatial databases, as well as big data solutions such as Hadoop, and stream processing systems such as Storm, all have a place in the GMS. To meet the performance objectives of the GMS, it is critical that GMS components use the most appropriate data technologies available, rather than simply relying on ones which have traditionally been used.

8.6 Conceptual Data Types

The GMS must consider a rich variety of conceptual data types, from details about the grid assets themselves, to data quantifying their operation, to records of how it has been maintained.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Examples / Description / Related Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locations</td>
<td>defined regions, functional locations, or GPS positions</td>
</tr>
<tr>
<td>Customers</td>
<td>profiles, service location, billing, etc.</td>
</tr>
<tr>
<td>Weather</td>
<td>temperature, precipitation, solar irradiance, wind</td>
</tr>
<tr>
<td>Engineering</td>
<td>planning, purchasing, scheduling</td>
</tr>
<tr>
<td>Work</td>
<td>schedule, compatible units, designs</td>
</tr>
<tr>
<td>Construction</td>
<td>construction, as-built, in-service, retired</td>
</tr>
<tr>
<td>Crews</td>
<td>capabilities, work orders, location</td>
</tr>
<tr>
<td>Asset</td>
<td>ratings, usage tracking, lifecycle, maintenance</td>
</tr>
<tr>
<td>Equipment Model</td>
<td>transmission, distribution, substations, structures, comms, protection</td>
</tr>
<tr>
<td>Measurements</td>
<td>voltage, current, etc. associated with functional locations (not physical equipment)</td>
</tr>
<tr>
<td>State Estimate Result</td>
<td>measured and estimated current, averages by day / season, etc.</td>
</tr>
<tr>
<td>Economics</td>
<td>agreements, programs, operational cost / rules</td>
</tr>
<tr>
<td>Control</td>
<td>immediate, hourly schedule (curves); set points, pricing</td>
</tr>
<tr>
<td>Grid State</td>
<td>breaker positions, tap changers, inputs (gen), outputs (loads), measurements</td>
</tr>
<tr>
<td>Trouble</td>
<td>planned and unplanned, restoration planning, including comms</td>
</tr>
<tr>
<td>Perspective</td>
<td>subset of layers, entities, properties, etc. appropriate for a purpose</td>
</tr>
<tr>
<td>Scenario</td>
<td>a named variant of data within a perspective, such as a private or shared collection of possible changes</td>
</tr>
</tbody>
</table>

*Table-6*
8.7 Model Characteristics

The GMS relies on having a comprehensive set of models of the distribution network, and the systems that support it. These models include all of the elements and the relationships between those elements. The models also include characteristics of both the elements and the relationships. In some cases characteristics may be represented through the presence or absence of a given relationship.

There are three identified models used by the GMS: the electrical network model, the control model, and the communications model. The electrical network model is discussed in detail in section 4.3.1. It represents all of the elements that comprise the physical distribution network. The control model shows the control relationships between different elements, such as relays and breakers, or remote intelligent switch clusters. The communications model represents all of the elements that comprise the communications network. These models cross-linked to each other to allow operators to understand how changes or failures in one system may affect other systems.

The models used within the GMS are multi-dimensional, with all data elements having dimensions of perspective, scenario, and time. Section 4.3.1 discusses these dimensions in detail, in context of the Electrical Network Model Update System (ENMUS), but these dimensions apply to the control and communications models as well. These dimensions allow a single model to support many views. Models will be sparsely populated such that only divergent data needs to be created within a given perspective, scenario, and time combination. The GMS will overlay different model views as required to establish a comprehensive data set for a given operation. For example, an operator might choose to perform a “what-if” analysis, overlaying a planning view on top of an historical as-operated view to determine how the system might have behaved.

In addition to characteristics, many elements within the model have status and state. Status reflects known settings or values provided through data acquisition. For example, a remote intelligent switch might indicate that its position is open, or provide current and voltage data. State, in the context of the GMS, refers to values calculated by the state estimator indicating what “should” be being measured at a given point. Generally, when status and state do not align, there is something wrong which needs operator review. A mismatch might indicate that a change has been made to the physical distribution network which has not been reflected in the electrical network model. It might also indicate an issue with a measuring device, or an unexpected condition like unregistered DER.

Conceptually, these models are independent of the method of storage. The GMS requires that the model, status, and the state be persisted, maintained, and made available via interfaces. Persistence, maintenance, and interfacing are independent of the model and the state from a technology standpoint. Ideally, the GMS will persist the model and the status in one place, such that they are maintained together, as it is critical that the models are fully maintained and are not allowed to go out of sync. In practice, status information may need special handling for performance reasons.

The GMS will rely on well-defined interfaces to hide the details of persistence from apps and services. Apps within the GMS should not have to “walk” the model to obtain answers. They should be able to call interfaces which address their needs. These interfaces will also provide abstraction from data sources, so that apps do not have to seek out model data from multiple locations. Logic that converts statuses to characteristics should be handled in services, ideally in one place, one time – not in apps.

The GMS deals with multiple different time horizons, data sources, and business rules for making updates. As a result, maintenance services for characteristics and status, as well as for the different models, are likely to be different. Characteristics may be updated asynchronously. Update intervals should be proportional to the rate of change, the operational interval, and the resolution of the characteristic. Status and state may require more synchronous updates.
9  Next Steps

This Architecture Definition Document not only sets the foundational principles for SCE’s vision for grid modernization and how to achieve it with the Grid Management System, it also provides guidance to the technology and equipment manufacturing community on what devices, communications, software, and systems are going to be required to fulfill SCE’s vision over the next several years. SCE believes that most aspects of our vision, this architecture, and the Grid Management System itself are applicable to other utilities such that this document and others we publish will be useful in accelerating the implementation of the new concepts for power systems operation and management described herein.

SCE cannot achieve our goals for a new, comprehensive Grid Management System alone. We are asking for the support of the entire industry to help us refine these concepts and architecture, develop the new products and services necessary to succeed, and share their experiences in deploying like systems. To further this objective, and to accelerate technology transfer, SCE will be working closely with other utilities in a new Grid Management Working Group (GMWG) convened under the Smart Grid Interoperability Panel (SGIP).

The GMWG aims to bring together Grid Operations technology and business leaders from utilities, vendors, academia and other stakeholders across North America to discuss key operational concepts/capabilities and architecture principles relating to future Grid Control & Operational technologies. These technologies are needed to manage a more complex grid due to the rapid rise of DERs. The GMWG will encourage members to share use cases, collaborate on business & technical requirements, exchange insights, and coordinate on research & development opportunities that will help drive vendor solutions and industry standards.

This Architecture Definition Document will evolve as we uncover more requirements, validate concepts through technology evaluation and demonstration, develop more architectural artifacts, and as input is obtained through the GMWG and other venues. SCE looks forward to a successful collaboration with industry on this effort.
# 10 Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADD</td>
<td>Architectural Definition Document</td>
</tr>
<tr>
<td>AGC</td>
<td>Automatic Generation Control</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ASP</td>
<td>Application Specific Profile</td>
</tr>
<tr>
<td>CAISO</td>
<td>California Independent System Operator</td>
</tr>
<tr>
<td>CIEE</td>
<td>California Institute of Energy and Environment</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical Infrastructure Protection</td>
</tr>
<tr>
<td>DDS</td>
<td>Data Distribution Service</td>
</tr>
<tr>
<td>DER</td>
<td>Distributed Energy Resource</td>
</tr>
<tr>
<td>DG</td>
<td>Distributed Generation</td>
</tr>
<tr>
<td>DMS</td>
<td>Distribution Management System</td>
</tr>
<tr>
<td>DR</td>
<td>Demand Response</td>
</tr>
<tr>
<td>DVVC</td>
<td>Distributed Volt/VAR Control</td>
</tr>
<tr>
<td>EE</td>
<td>Energy Efficiency</td>
</tr>
<tr>
<td>EMS</td>
<td>Energy Management System</td>
</tr>
<tr>
<td>ENM</td>
<td>Electrical Network Model</td>
</tr>
<tr>
<td>ENMUS</td>
<td>Electrical Network Model Update Subsystem</td>
</tr>
<tr>
<td>EPRI</td>
<td>Electric Power Research Institute</td>
</tr>
<tr>
<td>ES</td>
<td>Energy Storage</td>
</tr>
<tr>
<td>FAN</td>
<td>Field Area Network</td>
</tr>
<tr>
<td>FERC</td>
<td>Federal Energy Regulatory Commission</td>
</tr>
<tr>
<td>GIS</td>
<td>Geographic Information System</td>
</tr>
<tr>
<td>GMS</td>
<td>Grid Management System</td>
</tr>
<tr>
<td>GMWG</td>
<td>Grid Management Working Group</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent Electronic Device</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Taskforce</td>
</tr>
<tr>
<td>ISO</td>
<td>Independent System Operator</td>
</tr>
<tr>
<td>iSPS</td>
<td>Intelligent Special Protection Scheme</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>KVA</td>
<td>Kilovolt-ampere</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MQTT</td>
<td>Message Queuing Telemetry Transport</td>
</tr>
<tr>
<td>NERC</td>
<td>North American Electric Reliability Council</td>
</tr>
<tr>
<td>NIST IR</td>
<td>NIST Interagency Report</td>
</tr>
<tr>
<td>NIST SP</td>
<td>NIST Special Publication</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OLAP</td>
<td>Online Analytical Processing</td>
</tr>
<tr>
<td>OMS</td>
<td>Outage Management System</td>
</tr>
<tr>
<td>OT</td>
<td>Operations Technology</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>PEV</td>
<td>Plug-in Electric Vehicle</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PMU</td>
<td>Phasor Measurement Unit</td>
</tr>
<tr>
<td>PQ</td>
<td>Power Quality</td>
</tr>
<tr>
<td>PV</td>
<td>Photovoltaic</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RDBMS</td>
<td>Relational Database Management System</td>
</tr>
<tr>
<td>RFI</td>
<td>Request for Information</td>
</tr>
<tr>
<td>RFP</td>
<td>Request for Procurement</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>RTO</td>
<td>Regional Transmission Organization</td>
</tr>
<tr>
<td>SCE</td>
<td>Southern California Edison</td>
</tr>
<tr>
<td>SG</td>
<td>Smart Grid</td>
</tr>
<tr>
<td>SGIP</td>
<td>Smart Grid Interoperability Panel</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SRD</td>
<td>System Requirements Document</td>
</tr>
<tr>
<td>VAR</td>
<td>Volt-ampere Reactive</td>
</tr>
<tr>
<td>VEE</td>
<td>Validation, Editing, and Estimation</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WECC</td>
<td>Western Electric Coordinating Council</td>
</tr>
<tr>
<td>WMS</td>
<td>Work Management System</td>
</tr>
</tbody>
</table>