Customer Communications Portal Management – System Issues

1 Descriptions of Function

Issues confronting an Energy Company's Management Systems responsible for management of Telecommunications and Access Networks to support Customer Communications Portals.

1.1 Function Name

Customer Communications Portal Management – System Issues

1.2 Function ID

IECSA identification number of the function

C-2.2

1.3 Brief Description

This scenario attempts to describe key issues relevant to the operation of Management Systems in a large Energy Company (Electric and/or Gas and/or Water with several million customers) that provide access to information from and access to control devices located at customer sites. Access to information from devices and access to control one or more devices on the customer premises is provided via Customer Communications Portals.

Here, we focus on system management issues.

1.4 Narrative

The management of many facets of obtaining data from and sending commands or sending data to the Customer Communications Portals/Devices is a necessary and very important undertaking from a data protection, access control, security and network management perspective. There are several key elements that must be managed; issues and assumptions for these diverse areas will be covered separately. The first area to be covered will be System Management, the second Network Management and lastly, Security

Management. There are no assumptions made as to how these management systems will be implemented; there may be one, two, three or many separate computing systems or many distributed systems to accomplish these management tasks. What is important is that the principal issues are identified and that essential tasks are defined well enough to understand what must be done to manage the Customer Communications Portals and the access networks.

System Management functions are functions that deal with the highest-level issues that are required in order to effectively manage the Customer Communications Portals and the access networks. Many of these functions are critical, e.g., addressing of all Customer Communications Portals, devices supported by the portals and indeed every access network system, subsystem or functional element. The ability to access any of these devices is necessary in order to be able to communicate with the device as to its status, to obtain stored data, to download software upgrades and patches, to change set points, read registers, etc. Without a unique address for each device this becomes a very difficult task, if not unmanageable task. It would seem on the surface that unique addresses would be supplied by vendors of these products, however, many vendors have proprietary addressing schemes, or feel that addresses should be unique only on sub networks, i.e., replicate addresses for different networks, etc. Thus one of the first critical steps that need to be taken by a System Manger is to ensure that there are indeed unique addresses for every element of the Customer Communications Portal and access network that requires any form of intercommunications.

In order to support the many users of data within the Energy company as well as Customers and external entities, regulators and Governmental entities many different computer applications will be employed in the gathering of data, management of data and applications that provide needed functionality in the Customer Portals and Devices. Many of these applications will be written and supported by the Energy Company, others will be commercially available applications, and third parties will develop others. In all of these cases it is essential from an operational perspective to ensure that applications are functioning correctly, have the latest revisions running, are up to date in terms of security and other patches and are accessible only by business entities, other applications and individuals authorized to utilize them.

A key function that is needed to ensure efficient operation of a large distributed network such as the Customer Communications Portal network is the use of a common digital clock. The clock should be referenced to a highly stable and accurate clock such as ones maintained and operated by the National Institute of Standards and Technology (NIST). This will ensure that each Portal and Device is synchronized to an accurate time reference and enable any event occurring (equipment fault, alarm, component switching, etc) on the network to be accurately logged and any command issued to a Portal/Device to be accurately time stamped. This is also necessary as a means of analyzing data from many devices on the network to investigate operational anomalies and for resolving complex maintenance problems that might occur.

In addition to the utilization of a common clock there is a clear need for identifying the location of each Portal, Devices and key Communications Access systems and subsystems. Indeed there are many Energy Company applications (such as Customer Information Systems [CIS], and Geographic Information Systems [GIS]) that have location information by customer, some electrical elements (such as distribution transformers) etc. Other Energy company systems, including Outage Detection / Service Restoral Systems, may in fact make use of some CIS or GIS information to aid in the rapid location of outages so that service may be restored quickly. Given that Customer Communications Portals may be extensively deployed, it is essential that a universal means of defining locations of the portals, devices and key communications systems components be developed that can be utilized for Customer Portal identification and applications serving them and which can also be applied to existing applications such as CIS and GIS.

1) Addressing of all Customer Communications Portals, EO/CDs and Communications Systems observable and controllable elements, applications and management entities must be unique and identified in a consistent manner

2) Management Integration: Since there will be many different types of communications systems and subsystems used to interconnect the Energy Company to Customer Communications Portals, there will be many different Network Management Systems used by the Communications service providers. It is critical that the "Energy Company Management Systems" be capable of communicating and interacting with the Communications Service provider Network Management Systems and especially with their "Network users management application entity" (software in communications subsystems and devices providing network management services) in a consistent manner[1].

3) Use of a consistent clock that is referenced to a primary time source. It is absolutely critical that all communications systems, subsystems, Customer Communications Portals and customer premises devices be linked to this clock.

    a) All transactions, communications messages, alarms, control actions, network management system messages and control actions must be time stamped

    b) Different levels of time synchronization with consumer and energy systems may need to be established depending on the requirements of the applications. Categories may include the definition of operating environments linked to time management requirements. Possible categories include:

        i) "X" time range at the remote device (Tight Phasor Measurement Quality). The exact deviation from the reference clock will be determined by the requirements of the particular device. For example, measuring phase differences of a Transmission Line voltage or current at two different locations for protection purposes will require the highest level of synchronization with respect to a reference clock.

        ii) "Y" time range at the remote device (PQ event Measurement Quality).

        iii) "Z" time range at the remote device (Transaction Management Quality

[1] Service providers Network Management Systems will not allow users to directly access and control their various systems and subsystems, but they will generally enable large users to access information from their systems and many cases their subsystems. As generally the protocols used in these Network Management Systems (especially the protocols used to interconnect to subsystems and devices in the communications network) are proprietary, substantial effort will be required to adequately implement Energy Company access to service provider telecommunications networks in a consistent manner.

iv) "V" Other

4) All transactions, communications messages, alarms, control actions, network management system messages and control actions must be logged

   a) Since several diverse Energy Company Management Systems may be used to manage different aspects of communicating with Customer Communications Portals (e.g., Energy Conservation/Load Control Systems, Telecommunications Network Management System, Security Management System, etc) "log data" from diverse logging systems must be either merged, or applications developed to intelligently audit and manage various data sent to or received from the Customer Communications Portals and/or the various telecommunications networks used to connect with the Portals.

5) The location of all Customer Communications Portals (and for major customers, critical devices), critical communications system components and subsystems must be uniquely identified.

   a) The method used to identify the location of the Customer Communications Portals, communications systems and devices must be compatible with or easily mapped to the method used by Energy Company

      i) Geographical Information Systems.

      ii) Customer Information Systems

      iii) Outage Detection and Work Management Systems

      iv) Transmission (electric and gas) and Distribution (electric and gas) SCADA Systems

1.5 Actor (Stakeholder) Roles

Describe all the people (their job), systems, databases, organizations, and devices involved in or affected by the Function (e.g. operators, system administrators, technicians, end users, service personnel, executives, SCADA system, real-time database, RTO, RTU, IED, power system). Typically, these actors are logically grouped by organization or functional boundaries or just for collaboration purpose of this use case. We need to identify these groupings and their relevant roles and understand the constituency. The same actor could play different roles in different Functions, but only one role in one Function. If the same actor (e.g. the same person) does play multiple roles in one Function, list these different actor-roles as separate rows.

Grouping (Community)		***Group Description***
Actor Name	***Actor Type (person, device, system etc.)***	***Actor Description***

Grouping (Community)		*Group Description*
Actor Name	*Actor Type (person, device, system etc.)*	*Actor Description*

Replicate this table for each logic group.

1.6 Information exchanged

Describe any information exchanged in this template.

Information Object Name	*Information Object Description*

1.7 Activities/Services

Describe or list the activities and services involved in this Function (in the context of this Function). An activity or service can be provided by a computer system, a set of applications, or manual procedures. These activities/services should be described at an appropriate level, with the understanding that sub-activities and services should be described if they are important for operational issues, automation needs, and implementation reasons. Other sub-activities/services could be left for later analysis.

Activity/Service Name	*Activities/Services Provided*

Activity/Service Name	*Activities/Services Provided*

1.8 Contracts/Regulations

Identify any overall (human-initiated) contracts, regulations, policies, financial considerations, engineering constraints, pollution constraints, and other environmental quality issues that affect the design and requirements of the Function.

Contract/Regulation	*Impact of Contract/Regulation on Function*

Policy	*From Actor*	*May*	*Shall Not*	*Shall*	*Description (verb)*	*To Actor*

Constraint	*Type*	*Description*	*Applies to*

2 Step by Step Analysis of Function

Describe steps that implement the function. If there is more than one set of steps that are relevant, make a copy of the following section grouping (Preconditions and Assumptions, Steps normal sequence, and Steps alternate or exceptional sequence, Post conditions)

2.1 Steps to implement function

Name of this sequence.

2.1.1 Preconditions and Assumptions

Describe conditions that must exist prior to the initiation of the Function, such as prior state of the actors and activities

Identify any assumptions, such as what systems already exist, what contractual relations exist, and what configurations of systems are probably in place

Identify any initial states of information exchanged in the steps in the next section. For example, if a purchase order is exchanged in an activity, its precondition to the activity might be 'filled in but unapproved'.

Actor/System/Information/Contract	*Preconditions or Assumptions*

2.1.2 Steps – Normal Sequence

Describe the normal sequence of events, focusing on steps that identify new types of information or new information exchanges or new interface issues to address. Should the sequence require detailed steps that are also used by other functions, consider creating a new "sub" function, then referring to that "subroutine" in this function. Remember that the focus should be less on the algorithms of the applications and more on the interactions and information flows between "entities", e.g. people, systems, applications, data bases, etc. There should be a direct link between the narrative and these steps.

The numbering of the sequence steps conveys the order and concurrency and iteration of the steps occur. Using a Dewey Decimal scheme, each level of nested procedure call is separated by a dot '.'. Within a level, the sequence number comprises an optional letter and an integer number. The letter specifies a concurrent sequence within the next higher level; all letter sequences are concurrent with other letter sequences. The number specifies the sequencing of messages in a given letter sequence. The absence of a letter is treated as a default 'main sequence' in parallel with the lettered sequences.

Sequence 1:

```
1.1 - Do step 1
1.2A.1 - In parallel to activity 2 B do step 1
1.2A.2 - In parallel to activity 2 B do step 2
1.2B.1 - In parallel to activity 2 A do step 1
1.2B.2 - In parallel to activity 2 A do step 2
1.3 - Do step 3
1.3.1 - nested step 3.1
1.3.2 - nested step 3.2
```

Sequence 2:

```
2.1 - Do step 1
2.2 – Do step 2
```

#	Event	Primary Actor	Name of Process/Activity	Description of Process/Activity	Information Producer	Information Receiver	Name of Info Exchanged	Additional Notes	IECSA Environments
#	*Triggering event? Identify the name of the event.*[2]	*What other actors are primarily responsible for the Process/Activity? Actors are defined in section0.*	*Label that would appear in a process diagram. Use action verbs when naming activity.*	*Describe the actions that take place in active and present tense. The step should be a descriptive noun/verb phrase that portrays an outline summary of the step. "If …Then…Else" scenarios can be captured as multiple Actions or as separate steps.*	*What other actors are primarily responsible for Producing the information? Actors are defined in section0.*	*What other actors are primarily responsible for Receiving the information? Actors are defined in section0.* *(Note – May leave blank if same as Primary Actor)*	*Name of the information object. Information objects are defined in section 1.6*	*Elaborate architectural issues using attached spreadsheet. Use this column to elaborate details that aren't captured in the spreadsheet.*	*Reference the applicable IECSA Environment containing this data exchange. Only one environment per step.*

2.1.3 Steps – Alternative / Exception Sequences

Describe any alternative or exception sequences that may be required that deviate from the normal course of activities. Note instructions are found in previous table.

#	Event	Primary Actor	Name of Process/Activity	Description of Process/Activity	Information Producer	Information Receiver	Name of Info Exchanged	Additional Notes	IECSA Environments

[2] Note – A triggering event is not necessary if the completion of the prior step – leads to the transition of the following step.

2.1.4 Post-conditions and Significant Results

Describe conditions that must exist at the conclusion of the Function. Identify significant items similar to that in the preconditions section.

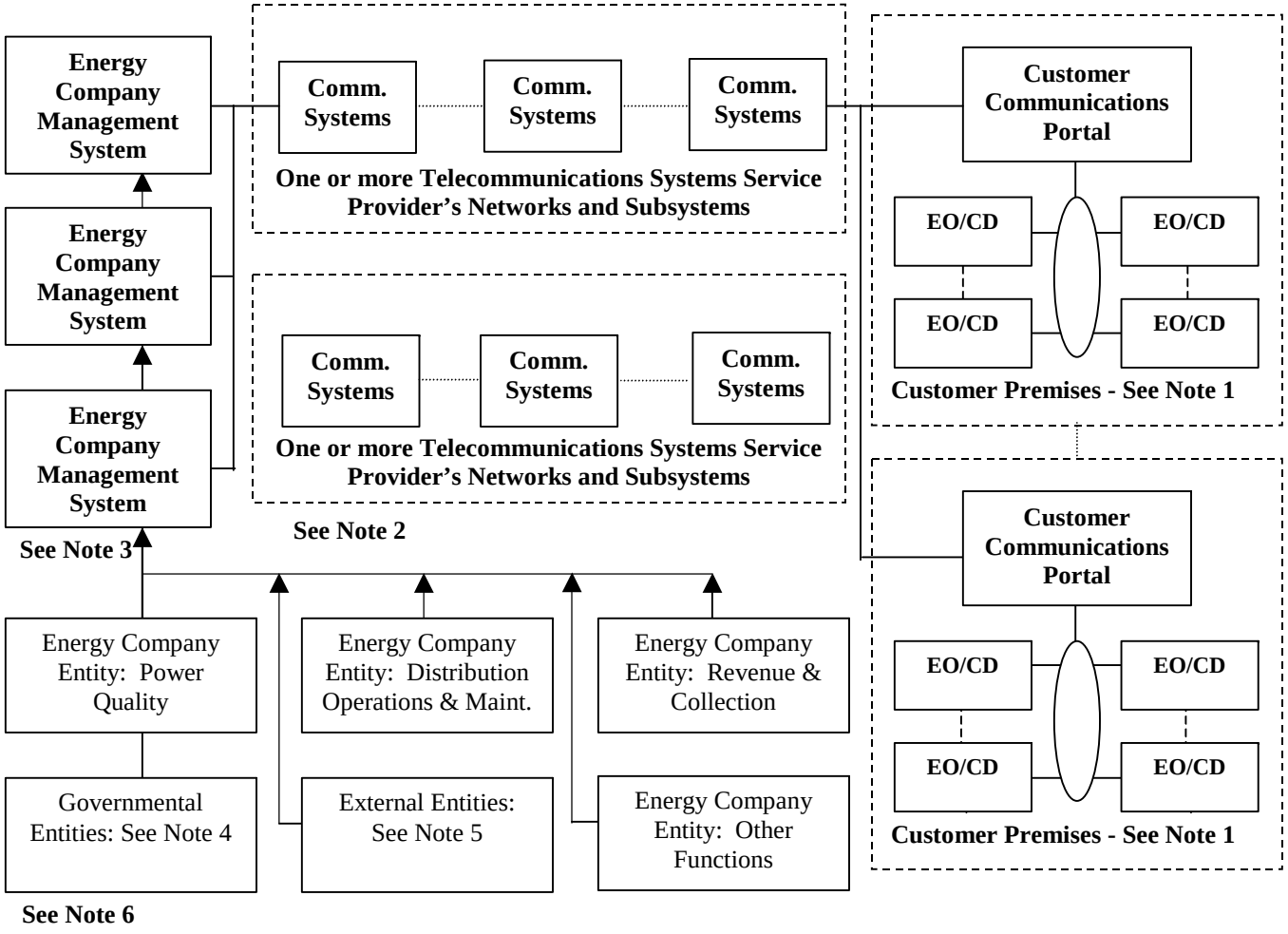
Describe any significant results from the Function

Actor/Activity	*Post-conditions Description and Results*

2.2 Architectural Issues in Interactions

Elaborate on all architectural issues in each of the steps outlined in each of the sequences above. Reference the Step by number..

2.3 Diagram



Legend:

EO/CD Energy Company Observable/Controllable Devices

(Systems, Hardware, Software, Applications, etc.)

Notes:

1. EO/CD's may be interconnected to the Customer Communications Portal by various LANs or wired/wireless systems
2. Many diverse Telecommunications Access Networks may be used to connect to Portals
3. Several different Energy Management Systems may be required including an overall "System Manager" (that deals with overall policies, views of various business entities, etc.) a Security Management System (that deals with authorization, security, reporting and related issues) and a Network Management System (that deals with the Customer Portal Access Networks and data communications issues)
4. Several Governmental Entities will need to access certain information that will be obtained via the Customer Communications Portals. Some of these are: PUC's, FERC, FTC, FCC, FBI, DHS, NIST, various State and Local Governmental Agencies, etc.
5. Several Entities outside of the Energy Companies will need to access certain information that will be obtained via the Customer Communications Portals. Some of these are: ISO, RTO, Independent Power Generators, various appliance manufacturers, etc
6. All of the Entities shown in the boxes are routed through the various Key Management Systems. This is meant to signify that the policies, procedures, access control rights, security and other enablers and constraints of these Management Systems will tailor the views of the data that these entities can access and the control messages that they are authorized to initiate. This does not imply that there will actually be individual computer/software systems that these entities must be routed through. The diagram represents a logical view , not a physical view.

3 Auxiliary Issues

3.1 References and contacts

Documents and individuals or organizations used as background to the function described; other functions referenced by this function, or acting as "sub" functions; or other documentation that clarifies the requirements or activities described. All prior work (intellectual property of the company or individual) or proprietary (non-publicly available) work must be so noted.

ID	Title or contact	Reference or contact information
[1]		

[2]		

3.2 Action Item List

As the function is developed, identify issues that still need clarification, resolution, or other notice taken of them. This can act as an Action Item list.

ID	Description	Status
[1]		
[2]		

3.3 Revision History

For reference and tracking purposes, indicate who worked on describing this function, and what aspect they undertook.

No	Date	Author	Description
0.			