The Integrated Energy and Communication Systems Architecture

Volume II: Functional Requirements

Appendix C:
Description Of The Domain Template

EPRI Project Manager

Joe Hughes

Cosponsor

Electricity Innovation Institute Consortium for Electric Infrastructure to Support a Digital Society (CEIDS)

EPRI • 3412 Hillview Avenue, Palo Alto, California 94304 • PO Box 10412, Palo Alto, California 94303 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ORGANIZATIONS THAT PREPARED THIS DOCUMENT

General Electric Company led by GE Global Research (Prime Contractor)

Significant Contributions made by
EnerNex Corporation
Hypertek
Lucent Technologies (Partner)
Systems Integration Specialists Company, Inc.
Utility Consulting International (Partner)

ORDERING INFORMATION

Requests for copies of this report should be directed to EPRI Orders and Conferences, 1355 Willow Way, Suite 278, Concord, CA 94520. Toll-free number: 800.313.3774, press 2, or internally x5379; voice: 925.609.9169; fax: 925.609.1310.

CITATIONS

This document describes research sponsored by EPRI and Electricity Innovation Institute.
The publication is a corporate document that should be cited in the literature in the following manner:
THE INTEGRATED ENERGY AND COMMUNICATION SYSTEMS ARCHITECTURE, EPRI, Palo Alto, CA and Electricity Innovation Institute, Palo Alto, CA: 2003 {Product ID Number}.

APPENDIX C – Description Of The Domain Template

This section contains an unpopulated IECSA Domain Template. (Note that the populated templates are formatted in landscape mode to allow for better legibility. However, it has been compressed somewhat for this section to make it easier to read as part of this document).

Each section, subsection, and table column has a footnote attached. This footnote describes the default mapping of the content into the IECSA UML model. Also in these footnotes are notations as to the mapping of these components to RM-ODP concepts. These mappings are used in the architectural analysis description to convey the natural language based templates into rigorous requirement descriptions in the architecture.

An electronic copy of the Domain Template is available **HERE**.

This page intentionally left blank.

Name of Domain Template

1 DESCRIPTIONS OF FUNCTION

All prior work (intellectual property of the company or individual) or proprietary (non-publicly available) work should be so noted.

1.1 Function Name[1]

Name of Function

1.2 Function ID[2]

IECSA identification number of the function
IECSA assigns a unique identification number to each function and/or sub-function described in the Task 1 deliverables. The identification number starts with a letter that denotes one of the six domains, i.e.

M – Market Operations Domain

G – Primary Generation Operations Domain

T – Transmission Operations Domain

D – Distribution Operations Domain

C – Consumer Services Domain

L – Distributed Resources Domain

The letter is followed by "-" and then the integer numbers delimited by "." to show the function hierarchies. For example L-3.1.3 is the IECSA identification number of the "ADA load model update" function.

1.3 Brief Description[3]

Describe briefly the scope, objectives, and rationale of the Function.

1.4 Narrative[4]

A complete narrative of the Function from a Domain Expert's point of view, describing what occurs when, why, how, and under what conditions. This could be a separate document, but will act as the basis for identifying the Steps in Section 0.

1.5 Actor (Stakeholder) Roles

Describe all the people (their job), systems, 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. These groupings and the relevant roles that the actors play help one 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) [5, 6]		*Group Description* [7]
Actor Name [8]	*Actor Type (person, device, system etc.)* [9]	*Actor Description* [10]

Replicate this table for each logic group.

1.6 Information exchanged

Describe any information exchanged in this function. These information objects are corresponding to the "Name of Info Exchanged" column in Section 2.1.2 and 2.1.3.

Information Object Name [11]	*Information Object Description* [12]

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 [13]	*Activities/Services Provided* [14]

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 [15]	*Impact of Contract/Regulation on Function* [16]

Policy[17]	From Actor [18]	May [19]	Shall Not [20]	Shall [21]	Description (verb) [22]	To Actor [23]
ProvideEnergy	*ESP*			*X*	*Provide power on demand*	Customer

Constraint [24]	Type [25]	Description [26]	Applies to [27]

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 [28]	*Preconditions or Assumptions* [29]

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

# [30]	Event [31]	Primary Actor [32]	Name of Process/Activity [33]	Description of Process/Activity [34]	Information Producer [35]	Information Receiver [36]	Name of Info Exchanged [37]	Additional Notes [38]	Environment [39]
#	*Triggering event? Identify the name of the event.*[1]	*What other actors are primarily responsible for the Process/Activity? Actors are defined i section1.5.*	*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 o the step. "If …Then…Else" scenarios can be captured as multiple Actions o as separate steps.*	*What other actors are primarily responsible for Producing the information? Actors are defined in section1.5.*	*What other actors are primarily responsible for Receiving the information? Actors are defined in section1.5.* *(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

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

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

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 [40]	*Post-conditions Description and Results* [41]

2.2 Architectural Issues in Interactions[42]

Elaborate on all architectural issues in each of the steps outlined in each of the sequences above. Reference the Step by number. Double click on the embedded excel file – record the changes and save the excel file (this updates the embedded attachment).

The architectural issues are grouped into four categories, namely “configuration”, “quality of service”, “security” and “data management”.

Note: For the purposes of publication, the embedded excel workbook has been replaced with the set of architectural issues questions asked for each of the steps outlined above.

2.2.1 Communication Configuration Issues

1. Numbers of “end” entities or sources of data
    1. One
    2. Two to a few
    3. Few to a hundred
    4. Hundreds to thousands
    5. Thousands to millions
    6. Significantly varied in different implementations
    7. Changes frequently
    8. Other
2. Numbers of “central” entities or users of data
    1. One
    2. Few
    3. Hundreds
    4. Thousands
    5. Millions
    6. Significantly varied in different implementations
    7. Changes frequently
    8. Other
3. Distance between entities
    1. A few feet
    2. A few miles
    3. Many miles
    4. Many hundreds of miles
    5. Varies and/or is not relevant
4. Location of information producer (source of data)
    1. Operations center
    2. Corporate building
    3. Building
    4. Substation
    5. Field outside substation
    6. Customer site
    7. Another corporation
    8. Mobile
    9. Changes frequently
    10. Other
5. Location of information receiver (user of data)
    1. Operations center

2. Corporate building
3. Building
4. Substation
5. Field outside substation
6. Customer site
7. Another corporation
8. Mobile
9. Changes frequently
10. Other

6. Communications configuration
    1. WAN
    2. LAN
    3. One-on-one
    4. One-to-many
    5. Many-to-many
    6. Multi-drop
    7. Ad hoc
    8. Other
7. Communications media
    1. Any
    2. Landline preferred
    3. Wireless possible
    4. Wireless required
    5. Other
8. Communications ownership
    1. Any
    2. Utility-owned
    3. Jointly-owned
    4. Commercially provided
    5. Internet
    6. Other
9. Communication bandwidth
    1. < 2400 bps
    2. 2.4-56 kbps
    3. 10 Mbps-100Mbps
    4. 100Mbps - 1 Gbps
    5. >1 Gbps
    6. Other
10. Data exchange methods
    1. Any
    2. Master-slave
    3. Peer-to-peer
    4. Client-server
    5. Publish-subscribe
    6. Through database
    7. Ad hoc
    8. Other
11. Communication access services requirements
    1. Any or all
    2. Request-response
    3. Periodic reporting
    4. Report-by-exception
    5. Control command
    6. Select-before-operate
    7. Set parameter values
    8. Query for data by name

9. Subscribe
10. Broadcast
11. Multi-cast
12. Data discovery
13. Use of data sets
14. Query to find location of data
15. Query to determine what data is available (discovery)
16. Execute application
17. Establish and end association
18. Logging
19. Journaling
20. Remote restart
21. Remote reconfiguration
22. Remote diagnosis
23. Other

12. Data exchange pattern
    1. Data flow is <10% of bandwidth available
    2. Data flow >10% but less than 50% of bandwidth available
    3. Data flows patterns basically even
    4. Data flows include high volume bursts
    5. Other Low Latency required
13. Growth
    1. 2x number of participating devices - Over the next 5 years
    2. 10x number of participating devices - Over the next 5 years
    3. 100x number of participating devices - Over the next 5 years
14. Commonly used data exchange technologies
    1. Public Internet as communications media
    2. Internet-based protocols (e.g. HTML, XML)
    3. Computer Industry Component Technology Standards (e.g. Corba, EJB, .Net, Web Services)
    4. Transaction Technologies (e.g. Corba, EJB, .NET, Web Services)
    5. Database Access Services (SQL, OQL, object browsing)
    6. Methodologies for process management (e.g. EDI, ebXML)
    7. NAESB protocols (OASIS, E-tagging, RTO (TBD))
    8. IEC 61970 Common Information Model (CIM) Standard
    9. IEC 61970 Generic Interface Definition (GID) Standard
    10. IEC 61968 Interface Exchange Model (IEM) Message Definition Standards
    11. IEC 61850 (UCA) Standard
    12. IEC 60870-6 TASE.2 (ICCP)
    13. IEC 60870-5 and/or DNP
    14. Other legacy SCADA protocols
    15. Building Automation Protocols SSPC135
    16. Other Building Automation Protocols
    17. ANSI C12 SC 17 (IEC 62056-53/61/62) Metering Standard
    18. Graphics data exchange standards
    19. Through a database using proprietary database interfaces
    20. Flat files or CSV files
    21. Other standard technologies
    22. Other standard technologies
    23. Vendor proprietary technologies
    24. Other non-standard technologies
    25. None since interface has never been implemented
    26. None of the above/ not relevant/ don't know
15. Relative maturity of of current implementation
    1. Very mature and widely implemented
    2. Moderately mature

3. Fairly new
4. Future, no systems, no interactions

16. Existence of legacy systems
    1. Many legacy systems
    2. Some legacy systems
    3. Few legacy systems
    4. Extensive changes will be needed for full system functionality
    5. Moderate changes will be needed
    6. Few changes will be needed
    7. No changes will be needed
17. Configuration issues
    1. Communications access to “end” entities difficult and/or costly
    2. Bandwidth not typically able to handle the data traffic
    3. Media does not have adequate availability
    4. Media does not have adequate reliability
    5. Expense of communications channels is an issue
    6. None
    7. Other
18. Data exchange issues
    1. End devices are “compute-constrained” and limited ability to handle data exchanges
    2. Volume of data causes data handling problems
    3. Data types and formats change frequently over time at any one implementation
    4. Data types and formats vary significantly from implementation to implementation
    5. None
    6. Other
19. Protocol issues
    1. Standard protocols do not exist for this type of data exchange
    2. Standard protocols exist but are not usually implemented
    3. Too many standards exist without a consensus on which to use
    4. Pieces of standards exist, but these are often not implemented in interoperable means
    5. None
    6. Other
20. Ranking of issues of greatest concern
    1. Indicate issue of greatest concern Existing links not fast enough for executing this step
    2. Indicate 2nd issue of greatest concern Links between utilities exist rarely or not at all
    3. Indicate 3rd issue of greatest concern Generalized algorithms for these steps don't exist yet

2.2.2 Quality of Service Requirements

1. Elapsed time response requirements for exchanging data
    1. 1-4 milliseconds
    2. 4-10 milliseconds
    3. Less than 1 second
    4. 1-2 seconds
    5. 10 seconds
    6. More than 10 seconds
    7. No specific response requirements
    8. Other Must occur between trip and reclose
2. Contractual timeliness for exchanging data is required
    1. Within 1 second
    2. Within 1 minute
    3. Within 5 minute
    4. Within some longer time

5. No specific contractual timeliness is required
6. Other

3. Availability of information flows
    1. 99.9999% + availability ~ 1/2 second per year
    2. 99.999% + availability ~ 5 minutes per year
    3. 99.99% + availability ~ 1 hour per year
    4. 99.9% + availability ~ 9 hours per year
    5. 99% + availability ~ 3.5 days per year
    6. 90% + availability ~ 1 month per year
    7. Less than 90%
    8. Continuous availability not required so long as downtime is scheduled
    9. Continuous availability not required but must be available at specific times or under specific conditions
    10. No specific availability is required
    11. Other
4. Precision of data requirements (normally relevant only for conversions, e.g. analog to digital)
    1. 100% accurate
    2. >.5% variance
    3. >1%
    4. >5%
    5. Not relevant
    6. Other
5. Accuracy of data requirements
    1. Requires quality flag indicating at least normal and not normal
    2. Age of data needs to be knowable
    3. Time skew of data must be known
    4. Adequate accuracy can be assumed
    5. Accuracy of data not an issue
    6. Other
6. Frequency of data exchanges
    1. Essentially continuous
    2. Every few milliseconds
    3. Every few seconds
    4. Periodicity greater than a few seconds
    5. Upon event
    6. Upon request
    7. Random
    8. Sparse
    9. Other
7. Commonly used techniques for meeting quality of service requirements of this data exchange
    1. Failure detection
    2. Automatic restart
    3. Automatic failover to second source of data or function
    4. Automatic failover of communication channels to secondary channel
    5. Backup of data
    6. Transaction rollback
    7. QoS monitoring
    8. Alarming on QoS failure
    9. None
    10. Not needed or not relevant
    11. Other
8. Required response times
    1. Should be met, but the needed engineering is not available without highly customized approaches
    2. Should be met, but the available solutions imply costs that are not justifiable
    3. Should be met, but the available solutions are non-standard or proprietary

    4. Usually is met and is not really an issue
    5. Other
9. Contractual timeliness
    1. Should be met, but the needed engineering is not available without highly customized approaches
    2. Should be met, but the available solutions imply costs that are not justifiable
    3. Should be met, but the available solutions are non-standard or proprietary
    4. Usually is met and is not really an issue
    5. Other
10. Availability of information flows
    1. Should be met, but the needed engineering is not available without highly customized approaches
    2. Should be met, but the available solutions imply costs that are not justifiable
    3. Should be met, but the available solutions are non-standard or proprietary
    4. Usually is met and is not really an issue
    5. Other
11. Precision of data requirements
    1. Should be met, but the needed engineering is not available without highly customized approaches
    2. Should be met, but the available solutions imply costs that are not justifiable
    3. Should be met, but the available solutions are non-standard or proprietary
    4. Usually is met and is not really an issue
    5. Other
12. Accuracy of data requirements
    1. Should be met, but the needed engineering is not available without highly customized approaches
    2. Should be met, but the available solutions imply costs that are not justifiable
    3. Should be met, but the available solutions are non-standard or proprietary
    4. Usually is met and is not really an issue
    5. Other
13. Frequency of data exchanges
    1. Should be met, but the needed engineering is not available without highly customized approaches
    2. Should be met, but the available solutions imply costs that are not justifiable
    3. Should be met, but the available solutions are non-standard or proprietary
    4. Usually is met and is not really an issue
    5. Other
14. Ranking of issues of greatest concern
    1. Indicate issue of greatest concern existing systems not fast enough to do this with comms
    2. Indicate 2nd issue of greatest concern too costly to put relays at every switch
    3. Indicate 3rd issue of greatest concern

2.2.3 Security Requirements

1. Eavesdropping Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is
    1. Crucial
    2. Quite important
    3. Not particularly important
    4. Detection that a security violation was attempted is crucial
    5. Other
2. Information integrity violation Ensuring that data is not changed or destroyed is
    1. Crucial

2. Quite important
3. Not particularly important
4. Detection that a security violation was attempted is crucial
5. Other

3. Masquerade and/or spoofing Ensuring that data comes from the stated source is
    1. Crucial
    2. Quite important
    3. Not particularly important
    4. Detection that a security violation was attempted is crucial
    5. Other
4. Repudiation Ensuring that the source cannot deny sending the data or that the receiver cannot deny receiving the data is
    1. Crucial
    2. Quite important
    3. Not particularly important
    4. Detection that a security violation was attempted is crucial
    5. Other
5. Replay Ensuring that data cannot be resent by an unauthorized source is
    1. Crucial
    2. Quite important
    3. Not particularly important
    4. Detection that a security violation was attempted is crucial
6. Information theft Ensuring that data cannot be stolen or deleted by an unauthorized entity is
    1. Crucial
    2. Quite important
    3. Not particularly important
    4. Detection that a security violation was attempted is crucial
    5. Other The log of the events is crucial, not the data itself
7. Denial of Service Ensuring unimpeded access to data is
    1. Crucial
    2. Quite important
    3. Not particularly important
    4. Detection that a security violation was attempted is crucial
    5. Other
8. This data exchange has the following requirements with respect to proof of conformance and/or non-repudiation with contractual agreements
    1. Logging of all information exchanged during this interaction is required
    2. Logging of only key information is required
    3. Logging of the source, destination, requesting application, and requesting user of information exchanges is required, but not the data itself
    4. Logging is not required
    5. Other logging
9. Security measures commonly used with this data exchange
    1. Access control through passwords
    2. Access control through database security mechanisms
    3. Virtual Private Networks (VPNs)
    4. Private (secret) key encryption
    5. Public key encryption (e.g. SSL/TLS)
    6. Firewalls with Access Control Lists and/or proxy servers
    7. Dial-back modems
    8. Bilateral data access control tables
    9. Timestamping, logging, and data records
    10. Non-repudiation techniques
    11. Kerberos
    12. Network management such as SNMP or CMIP
    13. Physical isolation

14. Backup
15. Security policies with procedures to follow
16. Trusted parties so no cyber security needed
17. None, but needed
18. None, and not needed
19. Other proprietary security measures, I.e. encrypted radios

10. Security Prevention Issues, Concerns, and Problems
    1. Addition of security violation prevention solutions could impact the required performance
    2. Addition of security violation prevention solutions could be too costly
    3. Addition of security violation prevention solutions could be too difficult or burdensome for users
    4. Data exchanges go across organizational boundaries, making security difficult
    5. No standard solutions are available
    6. Addition of security solutions is not feasible
    7. Other security concern
11. Security Detection Issues, Concerns, and Problems
    1. Addition of security violation detection solutions could impact the required performance
    2. Addition of security violation detection solutions could be too costly
    3. Addition of security violation detection solutions could be too difficult or burdensome for users
    4. Data exchanges go across organizational boundaries, making security difficult
    5. No standard solutions are available
    6. Addition of security solutions is not feasible
    7. Other security concern
12. Security Contractual Proof Issues, Concerns, and Problems
    1. Addition of security contractual proof solutions could impact the required performance
    2. Addition of security contractual proof solutions could be too costly
    3. Addition of security contractual proof solutions could be too difficult or burdensome for users
    4. Data exchanges go across organizational boundaries, making security difficult
    5. No standard solutions are available
    6. Addition of security solutions is not feasible
    7. Other security concern
13. Ranking of issues of greatest concern
    1. Indicate issue of greatest concern little if any security deployed right now
    2. Indicate 2nd issue of greatest concern existing systems are mostly proprietary, although some stds exist
    3. Indicate 3rd issue of greatest concern large number of devices will make security deployment costly

2.2.4 Data Management Requirements

1. Type of source data
    1. Source data was directly measured
    2. Source data was previously automatically stored in a database
    3. Source data was previously manually entered in a database
    4. Source data was calculated or output by an application
    5. Other Human source
2. Correctness of source data
    1. Source data is always correct (e.g. by definition)
    2. Source data is usually correct
    3. Source data is often not correct (incorrectly entered, out of date, not available)
    4. Source data is rarely correct
    5. Correctness of source data is not relevant

6. Other

3. Up-to-date data management
    1. Received data must be up-to-date within seconds of source data changing
    2. Received data must be up-to-date within minutes of source data changing
    3. Received data must be up-to-date within hours of source data changing
    4. Received data does not need to be up-to-date if source data changes
    5. Other
4. Management of large volumes of data that are being exchanged
    1. Major part of step involves handling large volumes of data
    2. Some part of step involves handling large volumes of data
    3. No part of step involves handling large volumes of data
    4. Other
5. Data consistency and synchronization management across systems
    1. Second-by-second synchronization Data being exchanged must be kept consistent and synchronized with other systems within seconds
    2. Minute-by-minute synchronization Data being exchanged must be kept consistent and synchronized with other systems within minutes
    3. Day-by-day synchronization Data being exchanged must be kept consistent and synchronized with other systems within hours or days
    4. No synchronization Data being exchanged does not need to be kept consistent or synchronized with other systems
    5. Other
6. Management of timely access to data by multiple different users
    1. Contractual/required time windows for multiple access are less than one second
    2. Contractual/required time windows for multiple access are within seconds
    3. Contractual/required time windows for multiple access are within tens of seconds
    4. Contractual/required time windows for multiple access are within minutes
    5. Timely access by multiple users is not relevant
    6. Other
7. Validation of data exchanges
    1. All data must be validated on each data exchange
    2. Data must include quality codes to indicate its validity
    3. Data from different sources must be validated against each other
    4. Data mapping of data item names is required for data from different sources
    5. Data can be assumed as valid (or validity checking is handled elsewhere)
    6. Data is usually not validated
    7. Data cannot be validated
    8. Validity of data is not relevant
    9. Other
8. Management of accessing different types of data to be exchanged
    1. Each data exchange could entail different types of data (e.g. query a database)
    2. Numbers or types of data being exchanged are changed or updated every few minutes
    3. Numbers or types of data being exchanged are changed or updated every few hours
    4. Numbers or types of data being exchanged are changed or updated every few days or weeks
    5. Numbers or types of data being exchanged are rarely changed or updated
    6. Not relevant
    7. Other
9. Management of data across organizational boundaries
    1. Data exchanges go across corporate boundaries
    2. Data exchanges go across departmental boundaries
    3. Data exchanges go across boundaries between system developed by different vendors
    4. Data exchanges are within one vendor"s system
    5. Not relevant
    6. Other
10. Transaction integrity required (backup and rollback capability)

1. Data exchanges require the ability to rollback to previous data states
2. Data exchanges require full backup for immediate “failover” to a second source of data
3. Data exchanges require backup of crucial data for “cold” failover
4. Data exchanges do not require rollback or backup
5. Other Data exchanges must be logged for later analysis and verification

11. Data format requirements
    1. Standard computer formats (e.g. binary, integers and floating pt, files)
    2. Standard serial transfer formats (e.g. DNP, Modbus, LonTalk, BacNet)
    3. Graphics formats
    4. EDI
    5. HTML-based
    6. XML-based
    7. CSV
    8. Standardized data objects
    9. Exchange of unstructured or special-format data (e.g. text, documents, oscillographic data) must be supported
    10. Any formats are acceptable
    11. Other
12. Management of data formats in data exchanges
    1. The same data exchanged between different applications have different formats that need to be “converted”
    2. The same data exchanged between different applications have the same formats
    3. Conversion of data formats is automatically handled by each application
    4. Other
13. Naming of data items
    1. Names of data items are different in different applications and must be “mapped” to each other
    2. Meanings of data items are different in different applications and must be “converted”
    3. Other
14. Management across different implementations
    1. Types of data being exchanged can vary significantly in different implementations
    2. Types of data being exchanged vary very little in different implementations
    3. Not relevant
    4. Other
15. Data exchange maintenance in which a human changes or updates what is to be exchanged
    1. Data exchanges require maintenance every few hours
    2. Data exchanges require maintenance every few days
    3. Data exchanges require maintenance every few weeks or months
    4. Data exchanges rarely require maintenance
    5. Not relevant
    6. Other
16. Database maintenance in which a human changes or updates what is in the database
    1. Database requires maintenance every few hours
    2. Database requires maintenance every few days
    3. Database requires maintenance every few weeks or months
    4. Database rarely requires maintenance
    5. Not relevant
    6. Other
17. Data maintenance effort human versus automation
    1. Data maintenance involves significant human time and manual data entries
    2. Data maintenance is partially automated but involves some human time and manual data entries
    3. Data maintenance is mostly automated but requires occasional intervention
    4. Data maintenance is (or can be if so authorized) completely automated (e.g. Live Update of virus definitions or Microsoft updates)
    5. Not relevant

6. Other

18. Commonly used data formats and management techniques for this data
    1. Standard computer formats (e.g. integers and floating pt, files)
    2. Standard serial transfer formats (e.g. analog points, status points, control points, such as used in DNP, Modbus, LonTalk)
    3. Graphics formats
    4. EDI formats
    5. HTML-based formats
    6. XML-based formats
    7. Comma separated variables (CSV) in a file
    8. Proprietary data format
    9. Data updates are done manually by a database administrator or maintenance personnel
    10. Data is validated automatically
    11. Data objects have well-known names (e.g. CIM and IEC61850)
    12. Transaction and data exchanges "discovery" is handled automatically (e.g. ebXML)
    13. Mechanisms are in place to ensure consistency of data
    14. Transaction rollback capabilities are used
    15. Not relevant
    16. Other
19. Management of source data
    1. Correctness of source data is all too often a major problem
    2. Not relevant
    3. Other
20. Management of time-related aspects of data exchanges
    1. Updating of data in a timely manner can pose a design or performance problem
    2. Management of large volumes of data can pose a performance or data organization problem
    3. Data consistency and synchronization management across systems can pose a performance problem
    4. Management of timely access to data by multiple different users can pose a problem
    5. Not relevant
    6. Other
21. Validation of data exchanges
    1. Validity of data received can pose a problem
    2. Management of data across organizational boundaries can pose a problem
    3. Transaction integrity required (backup and rollback capability) can pose a problem
    4. Not relevant
    5. Other
22. Data formats and structures in data exchanges
    1. Management of accessing different types of data to be exchanged can pose a problem
    2. Management of data formats in data exchanges can pose a problem
    3. Management of special-format data can pose a problem
    4. Naming of data items can pose a problem
    5. Management across different implementations can pose a problem
    6. Not relevant
    7. Other
23. Management of data maintenance by maintenance personnel (human intervention)
    1. Data exchange maintenance in which a human changes or updates what is to be exchanged can pose a problem
    2. Database maintenance in which a human changes or updates what is in the database can pose a problem
    3. Data maintenance effort human versus automation can pose a problem
    4. Not relevant
    5. Other
24. Ranking of issues of greatest concern
    1. Indicate issue of greatest concern sending data across organizational boundaries

2. Indicate 2nd issue of greatest concern mapping point numbers is a tedious, error prone manual process
3. Indicate 3rd issue of greatest concern As distribution automation increases, volumes of data and management of databases will increase greatly

2.3 Diagram[43]

For clarification, draw (by hand, by Power Point, by UML diagram) the interactions, identifying the Steps where possible.

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 [44]	Reference or contact information [45]
[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 [46]	Status [47]
[1]		
[2]		

3.3 Revision History

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

No [48]	Date [49]	Author [50]	Description [51]
0.			

This page intentionally left blank.

Endnotes

[1] The [Template] Function Name corresponds to an [RMODP] Name and is modeled as the name attribute of a [UML] Use Case.

[2] The [Template] Function ID has no correspondence to [RMODP]. The Function ID is modeled as a [UML] Tagged Value having the attribute name equal to “id” and owned by the [UML] Use Case.

[3] The [Template] Function Description corresponds to the [RMODP] Enterprise Viewpoint and is modeled using the documentation attribute of a [UML] Use Case.

[4] The [Template] Narrative corresponds to the [RMODP] Enterprise Viewpoint and is modeled using the document attribute of a [UML] Artifact. Each subsection corresponds to a separate Artifact. The Artifact name is the Narrative section number and section name.

[5] The [Template] Community corresponds to an [RMODP] Community and is modeled as a [UML] Collaboration. (Note: This is not to be confused with a [UML] Collaboration Diagram.)

[6] The [UML] Collaboration representing the [RMODP] Community contains [UML] Collaboration Roles having a [UML] Base Classifier of the [UML] Actor belonging to the [RMODP] Community.

[7] The [Template] Community Description corresponds to an [RMODP] Community and is modeled using the documentation attribute of the [UML] Collaboration.

[8] The [Template] Actor Name corresponds to an [RMODP] Actor and is modeled as a [UML] Actor.

[9] The [Template] Actor Type has no correspondence to [RMODP] and is modeled using the [UML] <<stereotype>> assigned to the [UML] Actor.

[10] The [Template] Actor Description corresponds to an [RMODP] Actor and is modeled using the documentation attribute of a [UML] Actor.

[11] The [Template] Information Object Name corresponds to an [RMODP] Object Type and is modeled using the name attribute of a [UML] Classifier.

[12] The [Template] Information Object Description corresponds to an [RMODP] Object Type and is modeled by to the documentation attribute of a Classifier.

[13] The [Template] Service Name corresponds to the [RMODP] Enterprise Viewpoint and is modeled as a [UML] Use Case which is associated with the main domain template use case using the [UML] <<includes>> relationship.

[14] The [Template] Service Description corresponds to the [RMODP] Enterprise Viewpoint and is modeled as the documentation attribute of a [UML] Use Case.

[15] The [Template] Contract corresponds to an [RMODP] Contract and is modeled as a [UML] Classifier that aggregates owned [RMODP] Policy objects as [UML] Classifiers.

[16] The [Template] Contract Description corresponds to and [RMODP] Contract and is modeled using the documentation attribute of a [UML] Classifier.

[17] The [Template] Policy corresponds to an [RMODP] Policy and is modeled as a [UML] Classifier. A Policy Classifier is a [UML] Associated Classifier using the [UML] Permission association.

[18] The [Template] From Actor corresponds to an [RMODP] Actor and is modeled as a [UML] actor on the supplier side of the [UML] Association that relates the [Template] From Actor and [Template] To Actor

[19] The [Template] Permission corresponds to an [RMODP] Permission and is modeled as a [UML] Operation having the [UML] <<permission>> stereotype assigned. The [UML] Operation belongs to the [UML] Classifier modeling the [RMODP] Policy

[20] The [Template] Prohibition corresponds to an [RMODP] Prohibition and is modeled as a [UML] Operation having the [UML] << prohibition >> stereotype assigned. The [UML] Operation belongs to the [UML] Classifier modeling the [RMODP] Policy

[21] The [Template] Obligation corresponds to an [RMODP] Obligation and is modeled as a [UML] Operation having the [UML] << obligation >> stereotype assigned. The [UML] Operation belongs to the [UML] Classifier modeling the [RMODP] Policy.

[22] The Description of the [Template] Permission, [Template] Prohibition, or [Template] Obligation corresponds to the [RMODP] Permission, [RMODP] Prohibition or [RMODP] Obligation and is modeled using the documentation attribute of the [UML] Operation belonging to the [UML] Classifier modeling the [RMODP] Policy.

[23] The [Template] To Actor corresponds to an [RMODP] Actor and is modeled as a [UML] actor on the client side of the [UML] Association that relates the [Template] From Actor and [Template] To Actor

[24] The [Template] Constraint corresponds to an [RMODP] Environment Contract and is modeled as a [UML] Constraint that is applied to the [Template] named [UML] Actor or [UML] Classifier.

[25] The [Template] Constraint Type has no correspondence to [RMODP] and is modeled using the documentation attribute of the [UML] Constraint.

[26] The [Template] Constraint Description corresponds to an [RMODP] Environment Contract and is modeled using the documentation attribute of the [UML] Constraint.

[27] The [Template] Applies To corresponds to the named [RMODP] Actor, [RMODP] Object Type or [RMODP] Interface and is modeled using a [UML] Constraint applied to the corresponding [UML] Actor, [UML] Classifier or [UML] Interface.

[28] The [Template] Actor/System/Information/Contract corresponds to the named [RMODP] Actor, [RMODP] Object Type or [RMODP] Interface and is refers to an existing a [UML] Actor, [UML] Classifier or [UML] Interface.

[29] The [Template] Preconditions or Assumptions corresponds to an [RMODP] Precondition and is modeled using a [UML] Constraint applied to the corresponding [UML] Actor, [UML] Classifier or [UML] Interface.

[30] The [Template] Step Number corresponds an [RMODP] Step and is modeled multiple ways:

1. The [RMODP] Step may be may be modeled as a [UML] Message who's name attribute is partially defined by the step number. The Message may appear in either a [UML] Collaboration Diagram or a [UML] Sequence Diagram. Note due to the limitation of many Modeling Tools – The [Template] Step Number cannot directly map to the [UML] Message Number. Many of the commercial tools do not support letters in the [UML] Message Number, even though Rational's RUP process recommends the use of the letters to indicate parallel sequences of execution. As a result the [UML] Message Numbers are assigned sequentially – and the [Template] Step Number is assigned to the [UML] Message name attribute.
2. The [Template] Step Number also appears in a [UML] Activity Diagram and is part of the [UML] Transition name.

[31] The [Template] Triggering Event corresponds to [RMODP] Invariant Schema and is modeled using a [UML] Guard Condition on a [UML] Transition from a [UML] Action state or a [UML] Object Flow State.

[32] The [Template] Primary Actor corresponds to an [RMODP] Actor acting as the [RMODP] Initiating Object and refers to an existing [UML] Actor and may be modeled multiple ways:

1. The [Template] Primary Actor may be modeled using a [UML] Swim Lane
2. The [Template] Primary Actor may be modeled in an [UML] Collaboration Diagram as the Supplier side of a [UML] Message/Stimulus.

[33] The [Template] Name of Activity corresponds to and [RMODP] Action and is modeled multiple ways:

1. The [Template] Name of Activity may be modeled using a [UML] Call Action of a [UML] Message in the [UML] Collaboration Diagram.

2. The [Template] Name of Activity may be modeled using the name attribute of an [UML] Action State in the corresponding [UML] Activity Diagram.

[34] The [Template] Description of Activity corresponds to and [RMODP] Action and is modeled multiple ways:

1. The [Template] Description of Activity may be modeled using the documentation attribute of a [UML] Call Action of a [UML] Message in the [UML] Collaboration Diagram.
2. The [Template] Description of Activity may be modeled using the documentation attribute of a [UML] Action State in the corresponding [UML] Activity Diagram.

[35] The [Template] Information Receiver corresponds to an [RMODP] Actor behaving as an [RMODP] Consumer Object and is modeled using a [UML] Classifier Role with a base [UML] Classifier assigned to an existing [UML] Actor. The [UML] Classifier Role appears on the client side of the [UML] Message/Stimulus in a [UML] Collaboration Diagram or [UML] Sequence Diagram.

[36] The [Template] Information Producer corresponds to an [RMODP] Actor behaving as an [RMODP] Producer Object and is modeled using a [UML] Classifier Role with a base [UML] Classifier assigned to an existing [UML] Actor. The [UML] Classifier Role appears on the supplier side of the [UML] Message/Stimulus in a [UML] Collaboration Diagram or [UML] Sequence Diagram.

[37] The [Template] Name of Info Exchanged had multiple correspondences to [RMODP]

1. The [Template] Name of Info Exchanged corresponds to an [RMODP] Object Type and is modeled using a [UML] Classifier. The [UML] Classifier is a supplied [UML] Parameter to a [UML] Operation. The [UML] Operation is placed on the [UML] Actor corresponding to the [RMODP] Actor involved in the information exchange.
2. The [Template] Name of Info Exchanged corresponds to an [RMODP] Invariant Schema and is modeled using the he name attribute of an [UML] Object Flow State in the [UML] Activity Diagram

[38] The [Template] Additional Notes have a correspondence to the [RMODP] Computational Viewpoint and are modeled as additional details of the document attribute of a [UML] Message/Stimulus.

[39] The [Template] Environment corresponds to an [RMODP] Environment Object and is modeled using a [UML] Collaboration. Note the [UML] Collaboration is not to be confused with a [UML] Collaboration Diagram.

[40] The [Template] Actor/Activity corresponds to the named [RMODP] Actor, [RMODP] Object Type or [RMODP] Interface and is refers to an existing a [UML] Actor, [UML] Classifier or [UML] Interface.

[41] The [Template] Post-Conditions Descriptions and Results correspond to an [RMODP] Post-Condition and is modeled using a [UML] Constraint applied to the corresponding [UML] Actor, [UML] Classifier or [UML] Interface.

[42] The [Template] Architectural Significant Issues have multiple correspondences to [RMODP] based on the type of issue (not elaborated). The [Template] Architectural Significant Issues are modeled using [UML] Tagged Values and are owned by the corresponding [UML] Message/Stimulus in the [UML] Collaboration Diagram.

[43] The [Template] Diagram has corresponds with the [RMODP] Engineering Viewpoint, [RMODP] Enterprise Viewpoint and [RMODP] Computational Viewpoint depending on the contents of the diagrams supplied by the [Template] author. The [Template] Diagram has no [UML] correspondence but is modeled using a dummy stereotype where the diagram is treated as the icon of the stereotype.

[44] The [Template] Contact has no correspondence to [RMODP], yet is modeled using the documentation attribute of a [UML] Package owning the [UML] Artifacts stereotyped <<document>> that identify the different sections of the [Template].

[45] The [Template] Reference has no correspondence to [RMODP], yet is modeled using the documentation attribute of a [UML] Package owning the [UML] Artifacts stereotyped <<document>> that

identify the different sections of the [Template]. All modeling elements added to the model will utilize the "reference" [UML] Tagged Value to refer to the Artifact for traceability.

[46] No correspondence

[47] No correspondence

[48] No correspondence

[49] No correspondence

[50] No correspondence

[51] No correspondence