IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems

1547.3™

IEEE Standards Coordinating Committee 21

Sponsored by the
IEEE Standards Coordinating Committee 21 on
Fuel Cells, Photovoltaics, Dispersed Generation, and Energy Storage

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

16 November 2007

IEEE Std 1547.3™-2007

Recognized as an
American National Standard (ANSI)

IEEE Std 1547.3™-2007

IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems

Sponsor
IEEE Standards Coordinating Committee 21 on
Fuel Cells, Photovoltaics, Dispersed Generation, and Energy Storage

Approved 30 October 2007

American National Standards Institute

Approved 17 May 2007

IEEE-SA Standards Board

Abstract: This guide is intended to facilitate the interoperability of distributed resources (DR) and help DR project stakeholders implement monitoring, information exchange, and control (MIC) to support the technical and business operations of DR and transactions among the stakeholders. The focus is on MIC between DR controllers and stakeholder entities with direct communication interactions. This guide incorporates information modeling, use case approaches, and a pro-forma information exchange template and introduces the concept of an information exchange interface. The concepts and approaches are compatible with historical approaches to establishing and satisfying MIC needs. The IEEE 1547™ series of standards is cited in the U.S. Federal Energy Policy Act of 2005, and this guide is one document in the IEEE 1547 series.

This guide is primarily concerned with MIC between the DR unit controller and the outside world. However, the concepts and methods should also prove helpful to manufacturers and implementers of communications systems for loads, energy management systems, SCADA, electric power system and equipment protection, and revenue metering. The guide does not address the economic or technical viability of specific types of DR. It provides use case methodology and examples (e.g., examples of DR unit dispatch, scheduling, maintenance, ancillary services, and reactive supply). Market drivers will determine which DR applications become viable. This document provides guidelines rather than mandatory requirements or prioritized preferences.

Keywords: communications; control; data acquisition; diesel generators; dispersed generation; distributed energy resources; distributed generation; distributed power; distributed resources; distribution system; electric power system; electrical network; energy management; energy storage; fuel cells; grid; IED; information exchange; intelligent electronic devices; interconnection requirements and specifications; meter; microturbines; monitoring; photovoltaic power systems; public utility commission; regulations; rulemaking, federal, national, regional, SCADA; standards; state; substations; supervisory; telemetry; utility grid

---

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Print: ISBN 0-7381-5633-7 SH95697
PDF: ISBN 0-7381-5634-5 SS95697

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.
The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Introduction

This introduction is not part of IEEE Std 1547.3, IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems.

IEEE Std 1547.3 is one of a series of standards published by the IEEE or being developed by IEEE Standards Coordinating Committee 21 on Fuel Cells, Photovoltaics, Dispersed Generation, and Energy Storage concerning distributed resources interconnected with area electric power systems. IEEE Std 1547™ provides interconnection technical specifications and requirements as well as test specifications and requirements; IEEE Std 1547.1™ provides the test procedures for verifying conformance to IEEE Std 1547. The documents in the IEEE 1547 series are as follows:

- IEEE Std 1547™, IEEE Standard for Distributed Resources Interconnected with Electric Power Systems.
- IEEE Std 1547.1™, IEEE Standard for Conformance Test Procedures for Equipment Interconnecting Distributed Resources with Electric Power Systems.
- IEEE P1547.2™, Draft Application Guide for IEEE Std 1547 Standard for Interconnecting Distributed Resources with Electric Power Systems.[1]
- IEEE Std 1547.3™, IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems.
- IEEE P1547.4™, Draft Guide for Design, Operation, and Integration of Distributed Resource Island Systems with Electric Power Systems.
- IEEE P1547.5™, Draft Technical Guidelines for Interconnection of Electric Power Sources Greater Than 10 MVA to the Power Transmission Grid.
- IEEE P1547.6™, Draft Recommended Practice for Interconnecting Distributed Resources with Electric Power Systems Distribution Secondary Networks.

The IEEE 1547 series of standards is an outgrowth of the changes in the environment for the production and delivery of electricity and builds on prior IEEE standards, recommended practices, and guides developed by the IEEE Standards Coordinating Committee 21 on Fuel Cells, Photovoltaics, Dispersed Generation, and Energy Storage. In 2005, the United States Federal Energy Policy Act cited and required the IEEE 1547 series of standards for interconnection.

IEEE Std 1547.3 is intended to facilitate interoperability of distributed resources interconnected with an area electric power system. It is intended to help stakeholders in distributed resource installations implement optional approaches for monitoring, information exchange, and control to support the operation of their distributed resources and transactions among the stakeholders associated with the distributed resources. This guide describes functionality, parameters, and methodologies for monitoring, information exchange, and control related to distributed resources interconnected with an area electric power system. The focus is on monitoring, information exchange, and control data exchanges between distributed resource controllers and stakeholder entities with direct communication interactions. This guide incorporates information modeling and use case approaches, but it is also compatible with historical approaches to establishing and satisfying monitoring, information exchange, and control needs for distributed resources interconnected with an area electric power system.

The data exchanges between the distributed resource controller and equipment or entities internal to the local electric power system are not addressed in this guide. The many potential paths of data exchanges among individual stakeholders are also beyond the focus of this document. This guide does not establish requirements for interconnection, protection, safety, or local and area electric power system operation functions. Further, it is beyond the scope of this guide to mandate the business or tariff requirements associated with distributed resources interconnected with an electric power system. However, monitoring,

[1] Numbers preceded by P are IEEE authorized standards projects that were not approved by the IEEE-SA Standards Board at the time this publication went to press. For information about obtaining drafts, contact the IEEE.

information exchange, and control related to such issues and requirements may be ameliorated or satisfied by judicious use of this guide. Finally, specific hardware and software equipment, products, and services are not the subject of this guide.

Notice to users

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions are reasonable or non-discriminatory. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this guide was completed, SCC21 had the following membership:

Richard DeBlasio, *Chair*

Steve Chalmers, *Vice-chair*

Thomas S. Basso, *Secretary*

David Bassett
John J. Bzura
James M. Daley
Douglas C. Dawson
Frank Goodman
Kelvin Hecht
Gerald Johnson
Joseph L. Koepfinger
Benjamin Kroposki
Peter McNutt
Charles W. Rogers
Robert Saint
Mallur N. Satyanarayan
Timothy P. Zgonena

At the time this guide was completed, the Distributed Resources Monitoring, Information Exchange, and Control Working Group had the following membership:

Frank R. Goodman, Jr., *Chair*

Joseph L. Koepfinger, *Vice-chair*

Thomas S. Basso, *Secretary*

Richard Allison
Martin Baier
Arup Barat
David Bassett
Stephen G. Batsell
David Beach
David J.Bosack
Edward A. Brann
Gerard J. Burke
Jim Butler
John J. Bzura
Jim Calore
David Cartes
Frances M. Cleveland
David M. Costyk
Murray W. Davis
Paul A Dolloff
Kevin E. Donahoe
William E. Feero
Joseph F. Galdo
Andris Garsils
Daniel A. Goodrich
Tom Gordon
Erich W. Gunther
Raymond M. Hudson
C. Travis Johnson
Yuri Khersonsky
Brendan Kirby
Stanley Klein
Brenon Knaggs
Ljubomir A. Kojovic
Kevin Komara
John Kueck
Frank Lambert
Jim Lee
James W. Lemke
Jason Lin
Kevin P. Loving
Wayne W. Manges
Sylvain Martel
Paul Mattes
Anthony Mazy
Gary McNaughton
Arun Narang
Gary L. Olson
Barry Peirce
Robert Peterson
Charles Rogers
Steve Rosenstock
Robert Saint
William W. Saylor
Kent Sheldon
Herbert J. Sinnock
Andrew Skok
Sanjeev Srivastava
Wayne Stec
Dennis Tollefson
Amy Vaughn
John Vinod
Tim Wall
Simon Wall
Michael Wang
Randy West
Steve Widergren
Robert Wills
Thomas Yeh
Bob Yinger
Richard Zhang

The following members of the balloting committee voted on this guide. Balloters may have voted for approval, disapproval, or abstention.

William J. Ackerman
Satish K. Aggarwal
Steven C. Alexanderson
Ali Al Awazi
David L. Bassett
Thomas S. Basso
David C. Beach
Wallace B. Binder
Kenneth A. Birt
Stuart H. Bouchey
Steven R. Brockschink
John J. Bzura
James A. Calore
Danila Chernetsov
Frances M. Cleveland
Stephen P. Conrad
Terry L. Conrad
Tommy P. Cooper
Garth P. Corey
F. De La Rosa Costilla
Neal B. Dowling
Michael T. Doyle
Stephen E. Early
Gary Engmann
Manuel Gonzalez
Frank R. Goodman
Randall C. Groves
Ronald D. Hartzel
John F. Hawkins
Dennis Horwitz
R. Jackson
Mark J. Kempker
Yuri Khersonsky
Mark J. Knight
Joseph L. Koepfinger
Jim Kulchisky
Scott R. Lacy
Chung-Yiu Lam
Shawn M. Leard
G. Luri
Keith N. Malmedal
Mark F. McGranaghan
Peter F. McNutt
Joydeep Mitra
Travis Neale
Michael S. Newman
David K. Nichols
T. W. Olsen
Donald M. Parker
Iulian E. Profir
Charles W. Rogers
Bob Saint
Steven Sano
Gary W. Scott
Hyeong J. Sim
Herbert J. Sinnock
Cameron L. Smallwood
Jerry W. Smith
Roger J. Sowada
Sanjeev K. Srivastava
Charles R. Sufana
S. Thamilarasan
James R. Tomaseski
Simon R. Wall
Randall L. West
Charles M. Whitaker
Steven E. Widergren
James W. Wilson
Bernd Wirth
Theodore C. Zeiss
Ahmed F. Zobaa

When the IEEE-SA Standards Board approved this recommended practice on 17 May 2007, it had the following membership:

Steve M. Mills, *Chair*
Robert M. Grow, *Vice Chair*
Don Wright, *Past Chair*
Judith Gorman, *Secretary*

Richard DeBlasio
Alex Gelman
William R. Goldbach
Arnold M. Greenspan
Joanna N. Guenin
Julian Forster*
Kenneth S. Hanus
William B. Hopf
Richard H. Hulett
Hermann Koch
Joseph L. Koepfinger*
John Kulick
David J. Law
Glenn Parsons
Ronald C. Petersen
Tom A. Prevost
Narayanan Ramachandran
Greg Ratta
Robby Robson
Anne-Marie Sahazizian
Virginia C. Sulzberger*
Malcolm V. Thaden
Richard L. Townsend
Howard L. Wolfman

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Alan H. Cookson, *NIST Representativ*e

Michelle D. Turner
IEEE Standards Program Manager, Document Development

William Ash
IEEE Standards Program Manager, Technical Program Development

Contents

IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems

1. Overview

This overview is intended to provide a concise description of the scope, purpose, limitations, and application of this guide. Background information is provided in this clause, and detailed discussions of technical content are provided in the later clauses of this guide. The scope explains what is covered in the guide, the purpose explains why this guide's project is needed, and a subclause on limitations is presented that identifies certain monitoring, information exchange, and control (MIC) aspects not covered in this guide. In other words, the technical boundaries of the guide are discussed in these opening subclauses. Following that, background and introductory information are presented on understanding this guide's general application considerations.

1.1 Scope

This document provides guidelines for monitoring, information exchange, and control of distributed resources (DR) interconnected with electric power systems (EPSs).

1.2 Purpose

This document provides guidelines to facilitate the interoperability of one or more DR interconnected with EPSs. It describes functionality, parameters, and methodologies for MIC of DR interconnected with or associated with EPSs. DR technologies include fuel cells, photovoltaics, wind turbines, microturbines, and other distributed generators as well as distributed energy storage systems.

This guide documents alternatives for sound practice based on current practice and includes both legacy and new MIC systems.

1.3 Limitations

This guide is primarily concerned with MIC between DR units and the outside world. It is not intended for MIC within a device or among the components that make up a DR unit. The data exchanges between the distributed resource controller and equipment or entities internal to the local electric power system are not addressed in this guide. Refer to 1.7 for clarification. The many potential paths of data exchanges among individual stakeholders are also beyond the focus of this document. This guide does not establish requirements for interconnection, protection, safety, or local and area EPS operation functions.

This guide does not attempt to judge the economic or technical viability of specific types of DR, but rather presents guidelines for MIC for specific use cases of DR. Market drivers will determine which DR applications become viable in these use cases. Further, it is beyond the scope of this guide to mandate the business or tariff requirements associated with DR interconnected with an electric power system. However, monitoring, information exchange, and control related to such issues and requirements may be satisfied by judicious use of this guide.

The guide provides a description of the MIC characteristics that support DR installations. The guide is intended to aid DR-interested entities in the identification of MIC issues and solutions to support DR installations. This guide is not wholly comprehensive of the types of applications or the MIC desires of interested parties.

This guide does not address the MIC within the local EPS. (See Figure 1.) It does not address MIC for protection, and it does not address MIC requirements associated with revenue metering.

The guide is not part of any set of information exchange architecture standards for utility systems. Hence, conforming products to this guide does not guarantee they will be compatible with any utility system information exchange architecture.

Finally, specific hardware and software equipment, products, and services are not the subject of this guide.

1.4 Alternative approaches

This document provides guidelines rather than rigid requirements. This means alternative approaches to good practice are suggested but no clear-cut recommendations are made. This document states approaches relative to MIC for DR in EPSs. Example approaches are given, but there is more than one effective way to accomplish the desired results. One approach or another may be easier to implement in a specific user's DR installation, and it is recognized that the user has a choice.

1.5 Different levels of stakeholder needs

Stakeholder MIC needs vary with DR type, size, ownership, and location. In some situations, only minimal DR communications capabilities will be implemented. Additional capabilities may simply not be needed, or the functional benefit may not justify the expense. In other situations, a more comprehensive set of capabilities will be implemented to meet particular stakeholder needs or because the implementation cost is minimal. Although this document lists many potential MIC capabilities, it is important to remember that a wide range of stakeholder needs exists and that a corresponding range of MIC capabilities would be appropriate in these systems. In general, the size of the DR unit and the complexity of the application situation will help the user determine which MIC capabilities from the most relevant use case in this guide should be applied.

1.6 How to use this document

This guide is intended to help stakeholders in DR installations implement alternative approaches for MIC to support the operation of DR and transactions among stakeholders associated with DR. The reader should become familiar with the overall structure and intent of this guide, especially as discussed in Clause 1 and Clause 4.

Clause 1 provides an overview of the guide. Clause 2 presents references that are indispensable for the application of this guide. Clause 3 presents definitions and acronyms. Clause 4 introduces general technical content and application considerations of MIC of DR. Clause 5 contains basic MIC guidelines that focus on 4.16 of IEEE Std 1547™.[1] Clause 6 and Clause 7 present an in-depth treatment of MIC based on forward-looking approaches. In these clauses, guidelines are given for information modeling of DR interconnection applications. Clause 8 identifies example information technology protocol options and guidelines for protocols for MIC. Clause 9 provides guidelines for security issues for MIC in DR applications.

[1] Information on references can be found in Clause 2.

After these clauses, Annex A provides a bibliography. Annex B supports Clause 4 by presenting an annotated list of communications protocols, and Annex C supports this clause by providing additional information about open systems. Annex D is an introduction to business process concepts that supplements Clause 6 and Clause 8. Clause 6 is also supported by Annex E, which provides a use case template, and Annex F, which provides sample use cases. Annex G supplements Clause 7 with sample information exchange agreements (IEAs). Finally, Annex H supports Clause 9 by providing additional information security information.

1.7 IEEE 1547.3 reference diagram for information exchange

Figure 1 provides a reference overview of IEEE 1547.3 guidelines. Its emphasis is conceptual to focus the guidelines on the MIC that are relevant to DR interconnection. The diagram identifies the components that participate in processes of interest. These components are the subjects, or actors, of the process descriptions included in these guidelines. The components in this diagram are consistent with IEEE Std 1547. The new components of the diagram not defined in IEEE Std 1547 are defined in 1.7.1.

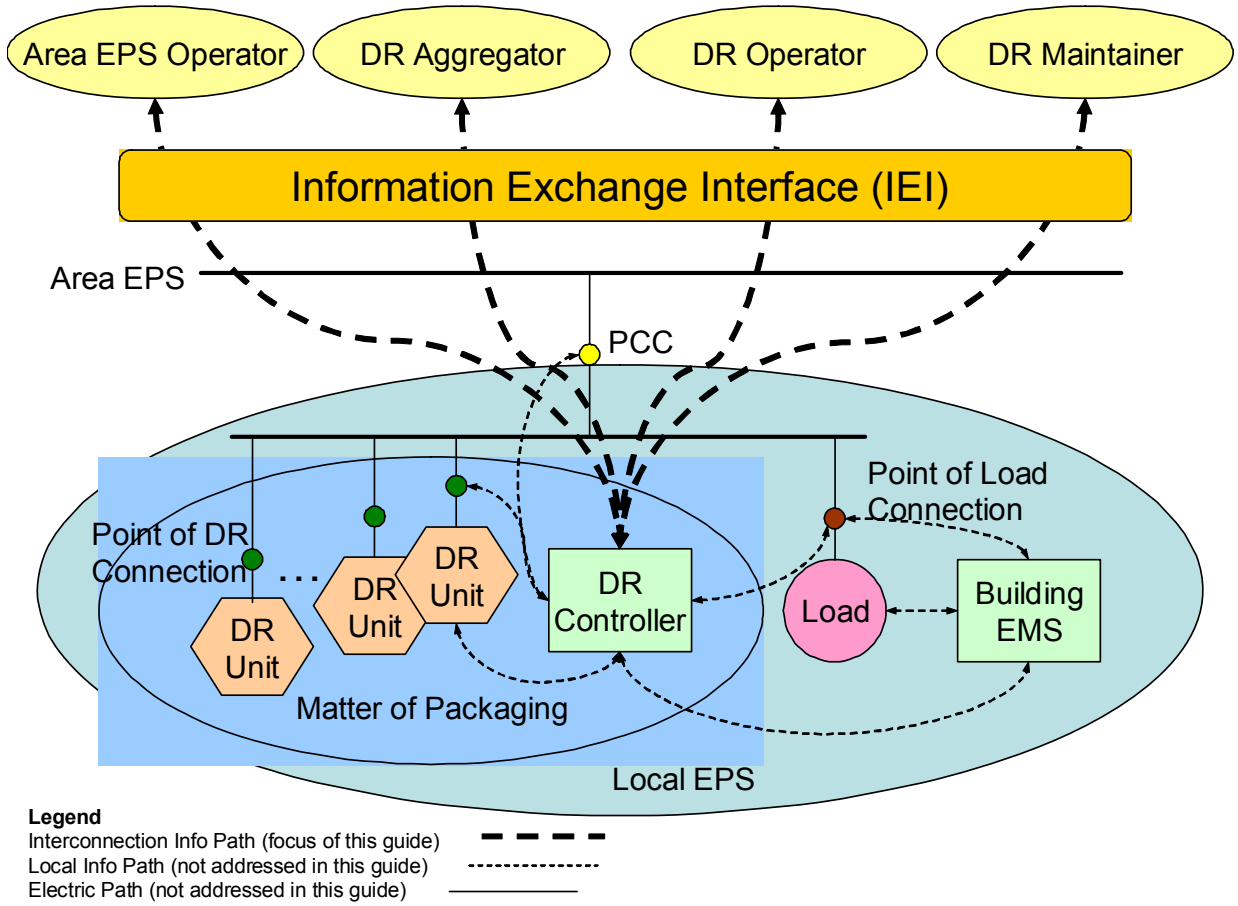


Figure 1— Reference diagram for information exchange

The upper ovals represent the roles of stakeholders who may need to exchange information with the DR system about its interconnection with the area EPS. Other stakeholders are acknowledged as important in the integration of these resources; however, those shown are the subject of the IEEE 1547.3 guidelines (see 1.7.1.2).

The DR units are represented by the hexagons. There may be one or many DR units at a site, but there will be at least one DR controller that performs a monitoring and control function. The DR controller has the intelligence with which to collaborate with stakeholders and site equipment. Note that the DR controller may communicate with these other entities through a communication gateway component; however, for the purposes of the reference diagram, the DR controller subsumes this function. The DR units and controllers can be installed in a variety of configurations. DR units and DR controllers may be packaged together or separately, depending on the business strategy of the manufacturers and the requirements of the clients.

The large circle represents a load. Some loads may be facilities with facility energy management system (EMS) controllers to optimize their operations. A building facility controller is represented as a rectangle and labeled building EMS. Because the focus of the guidelines is on the DR interconnection, coordination of the DR with specific loads on the local EPS may be needed. The building EMS represents the intelligent component for collaboration with the DR controller to enable such interactions as may be needed for combined heat and power applications. The building EMS operator and the DR operator would need to collaborate to ensure appropriate interaction between the DR controller and building EMS for this purpose.

Connections of interest are presented as lines in Figure 1. Solid lines represent electrical connections, and dashed lines represent communication paths. The communication paths are further sub-divided into those that are relevant to the guidelines and those that are acknowledged as important in an installation but are not the focus of this work. Note that communications exist among the stakeholders; however, these are not the subject of these guidelines and, for simplicity, are not shown in the diagram. The heavy dashed lines between stakeholders and the DR controller indicate the focus of these guidelines. The lighter dashed lines are generally required for local monitoring and control of internal device parameters or connection points in the local EPS. They are addressed through various mechanisms (such as standards, de facto standards, and custom implementations) that are generally within the control of the DR site integrator and, therefore, are less relevant to the interconnection with the area EPS and interaction with the DR stakeholders. As noted in 1.3, limitations, local sensing, and control are not the concern of this guide. In addition, the light dashed line between the DR controller and building EMS is included in the diagram to acknowledge that these systems may be integrated at a site to coordinate capabilities such as combined heat and power, but the details of this interaction are not the concern of this guide.

This guide can be thought of in terms of an information exchange interface for the DR device to communicate with remote parties. The information exchange interface could be an actual single point of interface for all remote information flows to and from the device, or it could be an abstraction that represents information flows by multiple, but coordinated, physical media. In either case, this document provides guidance for the information content (e.g., parameters, data, and data rates) that needs to be available at the information exchange interface. The information exchange interface is the information exchange counterpart of the point of common coupling (PCC) in the electrical system.

1.7.1 Diagram terminology

To clarify the terms and concepts in the reference diagram, definitions of the equipment and stakeholder roles follow. The term “role” represents that component of an organization that performs a certain job and interacts with other components in its duties. Organizations can be structured to contain different mixes of roles (e.g., a distribution system company may include area EPS operator (AEPSO), DR operator, and DR maintainer roles). By distinguishing among roles, the information exchange described by these guidelines can be applied to organizations with different combinations of roles. The same holds true for the combinations of equipment components in an installation and the roles they assume.

1.7.1.1 Equipment roles

— **Building EMS:** A system that supervises the scheduling and interaction among all building subsystems (e.g., chillers, boilers, and air-handling units) to meet facility needs with appropriate operator input. Building EMSs are also used to optimize building operations, start/stop, and demand control. Other names for these systems include building supervisory control systems, building automation systems, or facility management systems. Building EMSs may need to share information with the DR controller to coordinate supply and demand within a local EPS.

— **DR controller:** A device that manages the moment-by-moment operation of the DR device. These functions include fuel control, machine safety, and electrical protection as well as other functions that need tightly coupled monitoring and control. The DR controller has an interface that handles the slower communications requirements of the stakeholders and coordination with a building EMS. The DR controller can be incorporated into a DR device, or one DR controller may control several DR devices. The DR controller includes the functions of system control, electrical protection, and steady-state control, as described in the Definitions clause of IEEE Std 1547.1™.

— **DR unit:** Per IEEE Std 1547, the DR unit is a source of electric power that is not directly connected to a bulk power transmission system. DR units include both generators and energy storage technologies.

— **Load:** A point of delivery for end-use electrical consumption in the electric system. The load is usually made up of a combination of appliances (e.g., heating, ventilation, and air conditioning; refrigerators; lights; and other electric equipment) that is fed through a single point in the local EPS.

1.7.1.2 Stakeholder roles

The stakeholders with an interest in DR interconnection are people and organizations with complex groupings of responsibilities. Each organization is marked by its particular business strategies and structures, which have the capacity to evolve over time. The predominant roles that stakeholders assume are defined in this subclause. Any stakeholder organization may be composed of one or more of these roles.

The stakeholder roles are distinguished into two categories based on their need for direct interaction with DR systems, as illustrated in Figure 2. Note that many paths of information exchange exist among these roles, but these are beyond the focus of this document.

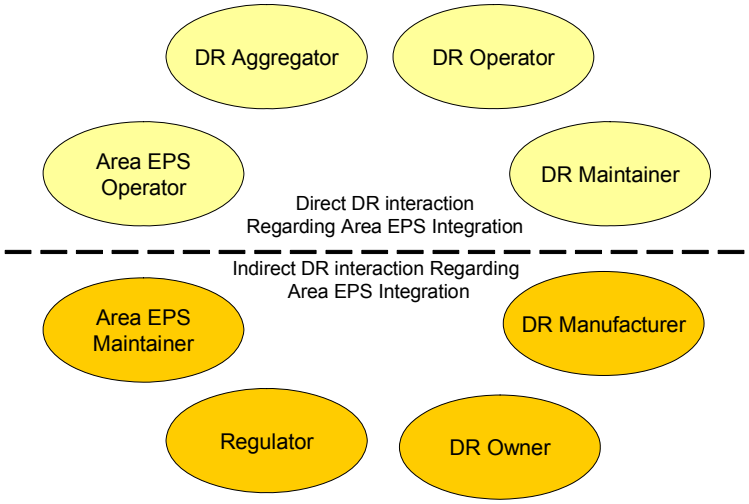


Figure 2—Stakeholder roles relevant to DR interconnection

1.7.1.2.1 Roles with direct interaction

The following stakeholder roles may have direct communications interactions with DR systems about their interconnection with the area EPS:

- **Area electric power system operator (AEPSO):** Responsible for the operations of the area EPS with which the DR is interconnected through the PCC. This operator is concerned with the safe and reliable operation of the distribution system and ensures that any misoperation of the DR will not affect other customers connected to the EPS. The AEPSO may need to interact with the DR unit to monitor its state or ensure its removal from the EPS to protect the safe and reliable operation of the EPS. In some cases, the AEPSO may also own and operate the DR.
- **DR aggregator:** Manages distributed electric energy resources that consist of more than one supply source (e.g., for the purpose of marketing energy and ancillary services to clients via the area EPS). The DR aggregator may interact with DR controllers to exchange economic or control information as well as information for contract settlement.
- **DR maintainer:** Maintains a DR unit for safe, reliable operation. The DR maintainer may interact with the DR unit to monitor its behavior, receive reports of problems involving maintenance, or otherwise review its health.
- **DR operator:** Controls the DR operation through local or remote means. It interacts with the DR unit to monitor its status and supervise its control.

1.7.1.2.2 Acknowledged roles without direct interaction

The following roles are acknowledged to play an important part of the successful integration of DR technology with the distribution system. They are distinguished from the roles with direct information exchange interaction because they gather their information needs visually or through others that have information exchange roles with the DR controller.

- **Area EPS maintainer:** Responsible for maintaining the EPS equipment on the area EPS side of the PCC. To safely maintain this equipment, the area EPS maintainer will need to know the operational state of the DR unit from the AEPSO and have visual assurances of important operational characteristics (such as de-energized state).
- **DR manufacturer:** Manufactures, produces, or integrates components that make up all or part of the system referred to as the DR. This includes producers of DR controllers. The DR manufacturer may get diagnostic information from the DR controller through its own diagnostic communication mechanisms or through others, such as the DR maintainer or DR operator, that have information exchange. Manufacturer interfaces may be highly specialized and business-sensitive and thus are beyond the focus of these guidelines.
- **DR owner:** Owns in part or whole a DR unit. The DR owner may have no connection with the location or operation of the DR. It interacts with other stakeholder roles (e.g., the DR operator) to verify operations and maintenance aspects performed by the other roles.
- **Regulator:** Monitors agreed-upon aspects of DR and distribution system operations for proper behavior against established rules. The regulator gathers information through visual means and the records kept by those performing the other stakeholder roles.

2. Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 1547, IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems.[2, 3]

IEEE Std 1547.1, IEEE Standard for Conformance Tests Procedures for Equipment Interconnecting Distributed Resources with Electric Power Systems.

3. Definitions and acronyms

For the purposes of this guide, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards, Seventh Edition* [B33][4] should be referenced for terms not defined in this clause.

3.1 Definitions

3.1.1 **actor:** Term used in Unified Modeling Language (UML) to designate the role a human, an application, or a system plays in the function being modeled.

3.1.2 **aggregation:** A special form of association that specifies a whole-part relationship between the aggregate (whole) and a component part.

3.1.3 **alarm:** Change-of-state information that is important enough to warrant notifying a person or system.

3.1.4 **area electric power system (EPS):** An EPS that serves local EPSs.

3.1.5 **association:** The semantic relationship between two or more classifiers that specifies connections among their instances.

3.1.6 **authorization:** The process of verifying that a user or process has permission to use a resource in the manner requested. To assure security, the user or process also needs to be authenticated before access is granted.

3.1.7 **class:** A description of a set of objects that share the same attributes, operations, methods, relationships, and semantics. A class may use a set of interfaces to specify collections of operations it provides to its environment.

3.1.8 **class diagram:** A diagram that shows a collection of declarative (static) model elements such as classes and types and their contents and relationships.

3.1.9 **collaboration:** The specification of how an operation or classifier, such as a use case, is realized by a set of classifiers and associations playing specific roles used in a specific way. The collaboration defines an interaction.

[2] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).
[3] The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.
[4] The numbers in brackets correspond to those of the bibliography in Annex A.

3.1.10 collaboration diagram: A diagram that shows interactions organized around the structure of a model by using either classifiers and associations or instances and links. Unlike a sequence diagram, a collaboration diagram shows the relationships among the instances. Sequence diagrams and collaboration diagrams express similar information but show it in different ways.

3.1.11 command: Controllable point used to change system behavior (enable/disable).

3.1.12 communication security: Protective measures for information transmitted between system components, over telecommunication links, and through networks to provide data confidentiality, integrity, and authenticity.

3.1.13 communications security: The use of administrative, technical, or physical measures to deny unauthorized persons information from a computer or a communications network and ensure the authenticity and integrity of such communications.

3.1.14 compromise: A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred.

3.1.15 control: Operational function used to change and modify, intervene, switch, set parameters, and optimize generation.

3.1.16 data integrity: (A) The degree to which a collection of data is complete, consistent, and accurate. (B) The condition or state in which data has not been altered or destroyed in an unauthorized manner.

3.1.17 distributed energy resource: *See:* **distributed resources.**

3.1.18 distributed generation or distributed generator: Electric generation facility connected with an area EPS through a PCC; a sub-set of DR.

3.1.19 distributed resources (DR): Sources of electric power that are not directly connected with a bulk power transmission system. DR include both generation and energy storage technologies.

NOTE—DR devices are also widely known as "distributed energy sources" and "distributed energy resources." Both the terms DR and DER are used in other contexts to have a broader meaning than in this guide. [5]

3.1.20 distributed resource aggregator: Manages distributed electric energy resources that consist of more than one supply source for the purpose of marketing energy and ancillary services to clients via the area EPS. The DR aggregator may interact with DR controllers to exchange economic or control information as well as information for contract settlement.

3.1.21 distributed resource controller: A device that manages the moment-by-moment operation of the DR device. These functions include fuel control, machine safety, and electrical protection as well as other functions that need tightly coupled monitoring and control.

3.1.22 distributed resource maintainer: Maintains a DR unit for safe, reliable operation. The DR maintainer may interact with the DR unit to monitor its behavior, receive reports of problems involving maintenance, or otherwise review its health.

3.1.23 distributed resource operator: Controls the DR operation through local or remote means. It interacts with the DR unit to monitor its status and supervise its control.

[5] Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

3.1.24 distributed resource owner: Owns in part or whole a DR unit. The DR owner may have no connection with the location or operation of the DR. It interacts with other stakeholder roles (e.g., the DR operator) to verify operations and maintenance aspects performed by the other roles.

3.1.25 distributed resource unit: Per IEEE Std 1547, the DR unit is a source of electric power that is not directly connected to a bulk power transmission system. DR units include both generators and energy storage technologies.

3.1.26 distributed storage: An electric storage facility connected with an area electric power system through a PCC; a subset of distributed resources.

3.1.27 domain: An area of knowledge or activity characterized by a set of concepts and terminology understood by practitioners in that area.

3.1.28 electric power system (EPS): Facilities that deliver electric power to a load.

3.1.29 electric power system, area: *See:* **area electric power system (EPS)**.

3.1.30 electric power system, local: *See:* **local electric power system (EPS)**.

3.1.31 enumeration: A list of named values used as the range of a particular attribute type. For example, RGB Color = {red, green, blue}. Boolean is a predefined enumeration with values from the set {false, true}.

3.1.32 event: The specification of a significant occurrence that has a location in time and space. In the context of state diagrams, an event is an occurrence that can trigger a transition.

3.1.33 extensible markup language: A specification developed by the World Wide Web Consortium, or W3C (a consortium of organizations that promotes interoperability on the Internet). Extensible Markup Language (XML) is a pared-down version of SGML designed especially for Web documents. It allows designers to create customized tags (data types), which enables the definition, transmission, validation, and interpretation of data among applications and among organizations.

3.1.34 function: A task, usually automated but with possible actions by human users, that is performed in the control center or distributed resource system.

3.1.35 generalization: A taxonomic relationship between a more general element and a more specific element. The more specific element is fully consistent with the more general element and contains additional information. An instance of the more specific element may be used where the more general element is allowed.

3.1.36 information: Content of communication; data and metadata describing data. The material basis is raw data, which is processed into relevant information. distributed resource device information categories include source information (e.g., analogue and state information) and derived information (e.g., statistical and historical information).

3.1.37 information exchange: Communication process between two systems, such as component and actor, with the goal to provide and get relevant information. Requires specific communication functions (services).

3.1.38 interaction: A specification of how stimuli are sent between instances to perform a specific task. The interaction is defined in the context of a collaboration.

3.1.39 interaction diagram: A generic term that applies to several types of diagrams that emphasize object interactions. These include collaboration diagrams and sequence diagrams.

3.1.40 interconnection: The result of adding a distributed resource unit to an area electric power system.

3.1.41 interconnection system: The collection of all interconnection equipment and functions, taken as a group, used to interconnect a distributed resource unit with an area electric power system.

3.1.42 island: A condition in which a portion of an area electric power system is energized solely by one or more local electric power systems through the associated point of common couplings while that portion of the area electric power system is electrically separated from the rest of the area electric power system.

3.1.43 islanding: The process whereby a power system is split into two or more segments, each with its own generation. Islanding is a deliberate emergency measure, the result of automatic protection or control action, or the result of human error.

3.1.44 local electric power system (EPS): An EPS contained entirely within a single premise or group of premises.

3.1.45 measured value: A sample of an analog quantity over a specific time period.

3.1.46 message: A specification of the conveyance of information from one instance to another, with the expectation that activity will ensue. A message may specify the raising of a signal or the call of an operation.

3.1.47 monitoring: An operational function used for local or remote observing of the status and changes of states.

3.1.48 object: An entity with a well-defined boundary and identity that encapsulates state and behavior. State is represented by attributes and relationships; behavior is represented by operations, methods, and state machines. An object is an instance of a class.

3.1.49 ontology: In the field of information technology, an ontology defines the common words and concepts (the meaning) used to describe and represent an area of knowledge. It is an engineering product that consists of a specific vocabulary used to describe a part of reality, plus a set of explicit assumptions regarding the intended meaning of that vocabulary—in other words, the specification of a conceptualization.

3.1.50 operational function: Used by actors for the normal daily operation of devices to obtain information about devices and send instructions to them. Types include monitoring, logging and reporting, data retrieval, and control.

3.1.51 package: A general-purpose mechanism for organizing elements into groups. Packages may be nested within other packages.

3.1.52 parallel operation: (A) The operation of interconnected power systems in synchronism. (B) The operation of network components—such as lines, transformers, and generators—connected in parallel.

3.1.53 personnel security: Procedures to ensure that personnel with access to sensitive information and critical services have the appropriate authorizations and training.

3.1.54 physical security: The protection of system resources from physical access, tampering, and destruction through the use of barriers, locks, seals, and intrusion detection systems.

3.1.55 point of common coupling: The point at which a local electric power system is connected with an area electric power system.

NOTE—See Figure 1 of IEEE Std 1547.

3.1.56 protocol: A set of semantic and syntactic rules that determines the behavior of functional units in achieving meaningful communication.

3.1.57 relationship: A semantic connection among model elements. Examples of relationships include associations and generalizations.

3.1.58 report: Historical information; event-driven or periodical notification of information comprising also statistical information and total performance.

NOTE—The term "report" (or "reporting") is also used for the communication service to send spontaneous data from a server to a client.

3.1.59 role: The named specific behavior of an entity participating in a particular context. A role may be static (e.g., an association end) or dynamic (e.g., a collaboration role).

3.1.60 scenario: A specific sequence of actions that illustrates behaviors. A scenario may be used to illustrate an interaction or the execution of a use case instance.

3.1.61 scheduled operation: Operation of a selected generation set at constant power or on successive steps of power, the values of which are previously specified within a given period of time.

3.1.62 security: The protection of hardware and software from accidental or malicious access, use, modification, destruction, or disclosure. Security also pertains to personnel, data, communications, and the physical protection of computer installations.

3.1.63 security policy: The objectives and mandates for protecting information, services, and other resources in a system and the philosophy of protection for meeting those objectives.

3.1.64 sequence diagram: A diagram that shows object interactions arranged in time sequence. In particular, it shows the objects participating in the interaction and the sequence of messages exchanged. Unlike a collaboration diagram, a sequence diagram includes time sequences but does not include object relationships. A sequence diagram can exist in a generic form (i.e., describes all possible scenarios) and in an instance form (i.e., describes one actual scenario). Sequence diagrams and collaboration diagrams express similar information but show it in different ways.

3.1.65 set point: Controllable target (demanded) value for a process quantity.

3.1.66 stakeholder: A person or group of people who has a share in something (an asset or a concept) and in the effect of its creation, alteration, or removal.

3.1.67 state diagram: A labeled directed graph that consists of circles to represent states and directed line segments to represent transitions between states.

3.1.68 subclass: In a generalization relationship, the specialization of another class; the superclass.

3.1.69 superclass: In a generalization relationship, the generalization of another class; the subclass.

3.1.70 system failure: Malfunctions in the hardware and software that could compromise the security of the system (for example, non-security-related failures and design flaws are not considered). The malfunctions include both intentional and inadvertent design or implementation flaws (including malicious hardware and software) and component failures. For intentional attacks, this threat area assumes that an intruder has access to the design or implementation processes of the system or to the operational system in such a way as to be able to cause a failure in a component. For inadvertent attacks, there may not be a specific intruder.

3.1.71 Unified Modeling Language (UML): Language for specifying, visualizing, constructing, and documenting the artifacts of software systems as well as for business modeling and other non-software systems. The UML represents a collection of the best engineering practices that have proved successful in the modeling of large and complex systems.

3.1.72 use case: The specification of a sequence of actions, including variants, that a system (or other entity) can perform while interacting with actors of the system.

3.1.73 use case diagram: A diagram that shows the relationships among actors and use cases within a system.

3.2 Acronyms

AE	alarms and events
AEPSO	area electric power system operator
AGA	American Gas Association
CAN	controller area network
CIM	Common Information Model
COM	Component Object Model
CORBA	Common Object Request Broker Architecture
DA	data access
DCOM	Distributed Component Object Model
DDE	Dynamic Data Exchange
DNP	Distributed Network Protocol
DNP3	Distributed Network Protocol 3
DR	distributed resource(s)
DX	data exchange
ebXML	Electronic Business Extensible Markup Language
EMS	energy management system
EPS	electric power system
GPL	General Public License
HDA	historic data access
HTTP	Hyper Text Transfer Protocol
ICCP	Inter-Control Center Communications Protocol
IEA	information exchange agreement
IEC	International Electrotechnical Commission
IECSA	Integrated Energy and Communication Systems Architecture
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	local area network
MIC	monitoring, information exchange, and control
OPC	open connectivity
OSI	Open Systems Interconnection
PCC	point of common coupling
PPP	Point-to-Point Protocol
RADIUS	remote authentication dial-in user service
RFC	request for comments
SOAP	Simple Object Access Protocol
TASE	Telecontrol Application Service Elements
TCP	Transmission Control Protocol
TLS	transport layer security
UDP	User Datagram Protocol
UML	Unified Modeling Language
UTC	Coordinated Universal Time
VPN	virtual private network
W3C	World Wide Web Consortium
WAN	wide area network
WG	working group
WINA	Wireless Industrial Networking Alliance
XML	Extensible Markup Language

4. General information about monitoring, information exchange, and control

This clause presents high-level background on MIC. DR can be used by, owned by, operated by, and maintained by, as well as provide services to, a multitude of stakeholders. The possible combinations of stakeholders and use cases are endless. However, a cross-section of specific use cases covers what are believed to be the most common scenarios in the foreseeable future. Such a cross-section is used as a basis for the MIC guidelines presented in this guide.

Any monitoring and information exchange system for DR must meet the stakeholder requirements for data exchange, performance, and security for the application.

MIC for DR systems should support interoperability between the DR devices and the area EPS. Interoperability is the ability of two or more devices to exchange information and work together in a system. This is achieved by using published object and data definitions, standard commands, and standard protocols. There are various levels of interoperability—a limited set of capabilities may be standard and available in a multi-vendor system, while extended capabilities may require proprietary commands.

Other desirable capabilities are self-description and automatic (MIC) system configuration. These features should reduce costs by eliminating the need for data translation, equipment customization, and manual configuration. They would increase reliability by eliminating data and command translation errors.

A further desirable capability is extensibility. Use cases and stakeholder needs are bound to further evolve. For this reason, all aspects of MIC systems should be extensible. For example, information models should be capable of extension to allow for new data items or device capabilities, and protocols should be capable of modification to support new physical media or application functions. It is recommended that open architecture standards be used as a path to the goal of interoperability.

All engineered technologies go through a life cycle of creation, deployment, maintenance, and retirement. This is particularly apparent in software information systems in which changes can be made relatively easily and product life cycles can be relatively short. Legacy systems refer to the deployed parts of the system, which may no longer be the state of the art in the industry but continue to contribute valuable functions to system operations. Mature communication protocols and related specifications and standards can transition to legacy status when newer approaches begin to be deployed. The power system should accommodate the continual integration of new equipment and communication technologies if current technology is not adequate for operational needs. Because of the large installed base of existing legacy technology, integration approaches need to consider how new ideas and technology can be integrated.

These guidelines look to the current trends in industrial communications and their improved aspects with the perspective that they should be able to be integrated with legacy components of the system. In addition, the trends of today will become the legacy components of the system tomorrow. More modern approaches should consider aspects that will ease their integration with the next generation of technology.

4.1 Interoperability

Interoperability is the ability of two or more devices to exchange information and work together in a system. This is normally achieved using published object and data definitions, standard commands, and standard protocols. Interoperability also requires some level of automatic system configuration.

Interoperability may be cost-effective if it eliminates the need for manual configuration, equipment customization, or data translation. It increases reliability by eliminating data and command translation errors.

There are various levels of interoperability. For example, a limited set of capabilities may be available in a multi-vendor system, extended capabilities may be proprietary, or significant manual configuration may be required to achieve interoperability. A well-recognized model for organizing communications concepts is the ISO (International Organization for Standardization) Open Systems Interconnection (OSI) seven-layer model, which is detailed in

Annex C. Agreement between interacting parties at specific layers of this model allows for interoperation at those layers. Greater interoperability of products has occurred because of standards agreements reached at various layers of this model.

4.2 Performance

Communication systems implemented to meet the needs specified in this guide exhibit certain performance characteristics. This subclause describes how performance in communication systems is specified and how the end user can interpret the specifications to determine applicability to various DR applications. The parameters all interact, so the end user must determine how each parameter interacts with the others and the appropriate balance. Four critical performance parameters—throughput, latency, reliability, and security—can be used to characterize communication network performance.

4.2.1 Throughput

Throughput measures the amount of user information that can be sent through the communication network continuously. It is expressed as kilobits per second (Kbs). It can be expressed as a maximum, minimum, or nominal value for the network. This should be specified from the end-user perspective and not from the raw-bit-rate perspective. The protocol overhead should be accounted for in this parameter. Any repeated transmissions because of errors must be accounted for as well. A critical design parameter is trading off the bit error rate and forward error correction with throughput because uncorrected errors in a packet will trigger re-transmission of the entire packet and thus affect realizable throughput.

4.2.2 Latency

Latency is the time that elapses between the issuance of a request and the performance of the requested operation. It can be expressed as a minimum, maximum, or nominal value. The units are usually seconds. For example, a command to close a breaker sent to the field (from an arbitrary remote site) requires a finite amount of time before the breaker actually closes.

NOTE—The communication required for confirmation of the action is not included in the measure of latency.

4.2.3 Reliability

The mean time between failures for a communications network is an index of its reliability. This is the time (in seconds or years) that can be expected between communication failures—i.e., when a request sent fails to arrive or one of the other attributes fails to deliver in the expected (or required) range.

This parameter includes what is normally referred to as the reliability, availability, and maintainability of the communications system. This measure takes into account failures caused by hardware or software malfunction, unavailability because of maintenance (e.g., for battery replacement), or downtime to reconfigure the communications network when new nodes are added or removed. It is a measure of the likelihood (or mean time between failure) that, if a command is issued to open a breaker at some arbitrary time, that breaker will actually respond within the timeframe allotted.

4.2.4 Security

Security is the ability to protect against unauthorized access while providing authorized access. The measure is how rigorous the candidate system is with respect to this attribute. The unit can be time-based (e.g., how many years it would take for someone to invade the system), probability-based (e.g., the probability that an attacker is successful in the attack), or cost-based (e.g., the investment per event to protect against an attack versus the investment per access for authorized entities). An attack can be defined as intervention by an unauthorized entity that could destroy information, intercept information, degrade the integrity of information, or deny access to the information to authorized entities. An authorized entity can become an attacker, perhaps inadvertently, if the security system fails to provide adequate protection against inadvertent actions that could destroy or degrade information or intercept

information for which the entity has no authorization. An example is an operator who floods a network beyond capacity when he/she downloads his/her retirement data to his/her console.

The cost of security is more than the cost of the procurement and installation of the hardware and software. Another critical cost parameter is the cost impact of the operation of the security system. For example, how much does it cost (in dollars) every time a display times out and requires password re-entry at a critical time in process operations? The ideal security system would prevent all unauthorized access and permit all authorized access without any cost impact.

4.3 Open systems approach

It is not necessary to use open architecture standards, but this guide attempts to avoid inconsistency with expectations for future open communication architecture to make it easy to migrate to open communication architecture standards as they become available. It is impossible for the guide to assure compatibility with all the proprietary architectures in use, and no attempt to do so has been made.

Open architecture standards

- Use non-proprietary methods and techniques.
- Have no license fees or royalties for their use or distribution.
- Are not limited with respect to areas of use, types of user, or particular products and technologies.
- Are (ideally) available and adopted as international standards.

Annex C details what “open” means with respect to this guide.

4.4 Extensibility

Use cases and stakeholder needs are bound to evolve. For this reason, all aspects of MIC systems should be extensible. For example, information models should be capable of extension to allow new data items and device capabilities, and protocols should be capable of modification to support new physical media or application functions.

4.5 Automatic configuration management

Manual configuration of MIC systems and DR equipment is expensive and prone to error. It is important that DR devices simplify and automate this task as much as possible. At the power system level, work is being done on configuration languages that can describe and control the configuration process and on other activities to improve the automation of power systems.

4.5.1 Self-description

One requirement for automatic configuration is self-description (also called interrogation). This is the ability of a device to describe itself in a standard way upon request by other DR devices or a central controller.

4.6 Information modeling

Information modeling is used to describe systems whose components interact by exchanging information. The requirements definition and design process for software systems falls into this category. As software and communications technology penetrates coordination and control schemes in systems of physical devices, the same information modeling approaches apply. The description of DR monitoring and information exchange is an appropriate application of information modeling techniques. Applying the commonly understood techniques of information modeling to a monitoring and information exchange situation enhances the ability of system designers and implementers to clearly understand this guide.

To unambiguously understand the meaning of information communicated in an interaction between parties, a rigorous, systematic approach is needed. The definition of the common words and concepts used to describe and represent an area of knowledge (such as the integrated operation of a DR with an area EPS) is known in information modeling as an "ontology." An ontology is an engineering product that consists of a specific vocabulary to describe a part of reality, plus a set of explicit assumptions regarding the intended meaning of that vocabulary—in other words, the specification of a conceptualization (The Semantic Web [B2]). By specifying an ontology for DR information exchange, a common language for communication between parties (devices as well as humans) can be systematically established.

Although a common vocabulary is an important component of an information model, interoperability between parties requires an understanding of the pre-conditions, the allowable sequence of interactions, and the expected conditions at the conclusion of an interaction. Information technologists refer to this interaction as the business process between parties. Business processes are best derived through the description of specific real-life scenarios that describe the system in action. A formalized description of a business process is a "use case." Use cases that describe typical scenarios of DR interactions with a DR operator, AEPSO, DR aggregator, and DR maintainer reveal the information that needs to be exchange, the sequence of messages, and the expected pre-conditions and post-conditions for proper operation.

The generally accepted format for describing information models is the UML. UML is the standard language for visualizing, specifying, constructing, and documenting the artifacts of a software-intensive system. It can be used with all processes, throughout the development life cycle, and across implementation technologies. UML is based on object-oriented principles and supports methodologies that combine generally accepted good practices in the modeling of large and complex systems. This includes information modeling concepts such as business modeling (work flow and business functions), object modeling, and software component modeling.

The UML modeling methodology is very powerful. It can be used from the highest overview level to actual software implementation. The key benefit of UML is that it provides consistent, well-defined concepts, terminology, and diagrams for visualizing the complex interactions that are implemented in the virtual cyber world.

UML helps describe the viewpoints that are appropriate to the modeling aspects of this guide—the business processes, the information models, and the computational or interaction models. These viewpoints can be elaborated on as follows:

- The business process viewpoint describes the purpose, scope, and policies of the system under consideration. It describes the system and the environment with which the system interacts. It not only covers the human user roles, devices, and systems involved to accomplish a set of activities, but also it describes the contracts, regulations, and constraints applied on the system. The primary UML tool for describing business processes is called a uses case. Use cases describe typical scenarios that exercise the system and reveal the actors (types of people involved), the relevant subsystems, and their interactions.
- The information viewpoint specifies the ontology: types of things (classes), data attributes, relationships to other classes, and behavior. UML defines class diagrams for describing this type of information.
- The computational viewpoint describes the interactions among the components of the system, as described through their interfaces. It specifies the sequence and type of information exchanged. UML provides collaboration and sequence diagrams for this purpose.

Clause 6 and Clause 7 provide the details of the processes and information models for DR MIC applicable to this guide.

4.7 Protocols

Protocols implemented in any communication system can be viewed as implementing one or more layers of the ISO OSI model. Details of the ISO OSI seven-layer model are included in Annex C. Details of that model and of how that model can be applied to issues associated with this guide are included in Clause 8.

5. Data exchange guidelines based on 4.16 of IEEE Std 1547 (*Monitoring provisions)*

This clause addresses IEEE Std 1547, 4.1.6. There is a brief discussion of DR conversion technologies. All other requirements within IEEE Std 1547 that require data exchange are not addressed in this clause.

Three classes are defined in Table 1 based on the rating of the DR installation. It is recognized that these class size breakdowns can be modified to accommodate local regulations and practices. More importantly, it is also recognized that the MIC guidance within each class may have to be altered to meet local regulations.

5.1 Overview

In IEEE Std 1547, text in 4.1.6 states, "Each DR unit of 250 kVA or more or DR aggregate of 250 kVA or more at a single PCC shall have provisions for monitoring its connection status, real power output, reactive power output, and voltage at the point of DR connection."

The requirements of IEEE Std 1547 apply at the PCC unless otherwise noted, and 4.1.6 of IEEE Std 1547 states that the provisions for monitoring be provided at the point of DR connection, which may or may not be the PCC.

For DR units or DR aggregate of 250 kVA or greater, the stakeholders may then choose whether to make use of those provisions to monitor the operation of the DR unit. The method to achieve the monitoring is not defined by IEEE Std 1547 and is left open to the stakeholders. This clause provides guidance for when these parameters should be monitored.

Aggregate installations, by definition, are composed of multiple units, of which each may be rated at less than 250 kVA. When the combined output of all of the DR units in an aggregate configuration exceeds 250 kVA at a single PCC, then 4.1.6 of IEEE Std 1547 applies. IEEE Std 1547, 4.1.6, may be met by a single provision for monitoring these parameters. However, the DR manufacturer, local EPS maintainer, or local EPS operator or owner may wish to have each DR unit monitored for his or her own needs, such as for performance troubleshooting. Frequently, there is a single point where the aggregated system connects within a local EPS. It is at this single point of aggregate DR connection where monitoring provisions of 4.1.6 of IEEE Std 1547 apply such that connection status, total real power output, total reactive power output, and voltage at that single point are required to be made available. This point of aggregate DR connection may or may not be the PCC. Further, 4.1.6 of IEEE Std 1547 does not address communication details, such as sending information to the area EPS via a communication system. However, those details are significant and may be established by mutual agreement, such as through an IEA.

The monitoring parameters may be available at various locations such as at a separate DR controller, at a remote terminal unit, or at another communication device. In addition, DR controllers are often integrated within the DR unit. These provisions meet the MIC guidance for aggregate installations.

The monitoring provisions are intended to allow stakeholders to monitor a DR's performance. If the monitoring is interfaced with the area EPS via SCADA, the DR operator needs to consider the scan rate and the communication protocol used by the AEPSO. Clause 4, Clause 6, Clause 7, and Clause 8 of this guide discuss these issues in more detail.

IEEE Std 1547, 4.1.6, is not for revenue metering purposes. The AEPSO is likely to have specific revenue metering requirements.

To maintain a reliable distribution system, the AEPSO, may need to control connected DR systems as established by connection agreements. To maintain system voltage within required American National Standards Institute ranges, it may be necessary for the AEPSO to control reactive power. During peak load situations, the AEPSO may need every DR to operate at full power. All such examples will require a secure, two-way communication system and appropriate interfaces between the AEPSO and the DR installations.

5.1.1 Connection status

In this guide, "connection status," as used in 4.1.6 of IEEE Std 1547, means an indication of whether or not an individual DR is connected.

An AEPSO is interested in the open/closed status of the sectionalizing device at the PCC. However, it is recognized that the PCC and the point of DR connection could be a considerable distance apart. For such installations, "connection status" can be interpreted as the open/closed status of the sectionalizing device at the point of DR connection.

Connection status should not be confused with an indication of whether or not the DR is energizing the area EPS, available, or running.

5.1.2 Real power

The monitoring provision for real power requires that each DR unit provide the ability for an external device to connect and monitor the real power output, at the point of DR connection of the DR unit. Real power may be measured (metered) for revenue purposes. Measuring a unit's real power output can also be used to indicate when the unit is operating.

5.1.3 Reactive power

The monitoring provision for reactive power requires that each DR unit provide the ability for an external device to connect and monitor the reactive power output, measured in kVAR, at the point of DR connection of the DR unit. Depending on the DR's generating technology, the DR unit may be able to provide reactive energy, which may be measured (metered) for revenue purposes.

5.1.4 Voltage

The monitoring provision for voltage requires that each DR unit provide the ability for an external device to connect and monitor the voltage, measured in volts, on the DR unit side of the point of DR connection to the local EPS. Monitoring of the DR voltage is often required for synchronism.

5.2 DR conversion technologies

This subclause summarizes some of the key characteristics of the major types of DR conversion technologies. These characteristics are the partial basis for the MIC guidance given in this clause.

5.2.1 Inverters

Inverters listed and labeled in compliance with UL 1741 [B61] include verification that they pass a non-islanding test in conformance with IEEE Std 1547.1. If the local EPS de-energizes, this type of inverter will cease to energize the local and area EPS. This type of inverter needs to sense the voltage and frequency so the DR will promptly cease to energize the area EPS during an outage and re-synchronize when power is restored in compliance with IEEE Std 1547.1.

5.2.2 Induction generator

An induction generator requires reactive power, generally from the area EPS, to produce real power. If the area EPS de-energizes, an induction generator will not continue to produce real power unless an alternate source of reactive power is available. The protection package for this generator will need to sense voltage and frequency from the area EPS to disconnect for an area EPS fault or abnormal operating condition. Normal area EPS voltage and frequency are also required before the DR unit can reconnect to the area EPS.

5.2.3 Synchronous generator

A DR system that contains a synchronous generator requires monitoring of the area EPS voltage and current to maintain proper operation while in parallel with the area EPS. The protection package for this generator will need to sense voltage and frequency from the area EPS to disconnect for an area EPS fault or abnormal operation condition. Normal area EPS voltage and frequency are also required before the DR unit can re-synchronize to the area EPS.

5.3 DR installation rating class definitions

This guide defines three classes based on the rating of the DR installation (see Table 1). It is recognized that these class size breakdowns can be modified to accommodate local regulations and practices. For DR aggregate installations behind a PCC, the total combined rating of all DR within the aggregate defines the class to which the aggregate installation belongs.

Table 1—DR installation classes

Class	DR rating
Class 1	0 < DR rating < 250 kVA[1]
Class 2	250 <= DR rating < 1500 kVA[1]
Class 3	1.5 <= DR rating <= 10 MVA[1]
NOTE 1— The 250 kVA and 10 MVA demarcations are established in IEEE Std 1547, 4.1.6. NOTE 2— The upper limit for this class may vary.	

MIC recommendations have been made for each class, but modifications within each class may have to be altered to meet local regulations.

5.3.1 Class 1

Class 1 includes DR units less than 250 kVA. DR systems that are likely to be encountered in this class include the following:

- Small (residential) photovoltaic systems
- Small wind turbines
- Microhydro systems
- Combined heat and power co-generation
- Microturbines
- Small fuel cells
- Energy storage devices
- Electric drive vehicle.

IEEE Std 1547, 4.1.6, states that units in this class are not required to provide monitoring provisions; however, it may be desirable in some cases to monitor these and other parameters.

Because installations in this class are relatively small, it is unlikely that the AEPSO will require monitoring. In rare instances, the AEPSO may want to know the connection status of the DR unit. In some instances, the DR owner may want to monitor the kilowatt-hour output of the DR in a billing cycle. Research and beta test projects may require additional MIC that may have to be met with additional monitoring equipment.

Units in this class may qualify for net metering tariffs, which may be available from the AEPSO. By definition, net metering installations require nothing more than the use of a revenue meter.

5.3.2 Class 2

Class 2 includes DR units between 250 kVA and 1.5 MVA. IEEE Std 1547, 4.1.6, states that DR units in this class shall provide monitoring provisions. Class 2 installations could be an aggregate of smaller DR units.

The display resolution of a typical area EPS EMS is 1 MW; therefore, the AEPSO may require the energy output of a Class 2 DR installation to be monitored by the EMS. It is highly unlikely that units in this class will be included in automatic generation control algorithms or be a part of the area EPS economic dispatch.

As DR installations approach output levels of 1 MW, the DR owner may be required to communicate the DR's connection status and output to the AEPSO. A Class 2 DR installation of 1 MW may need to communicate its status and output to an independent system operator. The independent system operator is likely to request the total megawatt-hour production on a daily basis.

Class 2 DR installations are unlikely to impact system voltage at the PCC. Therefore, it is highly unlikely that the AEPSO will require voltage monitoring. Additionally, Class 2 DR installations are unlikely to be contracted to provide voltage regulation.

5.3.3 Class 3

Class 3 includes DR units between 1.5 MVA and 10 MVA. IEEE Std 1547, 4.1.6, states that DR units in this class shall provide monitoring provisions.

DR installations in this class could have a significant impact on the area EPS system to which it is connected. As a minimum for most DR installations of this class, the AEPSO is likely to require status of the DR. Commonly, the DR's real and reactive power will be monitored and telemetered to the AEPSO. In such a case, the AEPSO's SCADA system may be used. This interfacing of the DR with the area EPS SCADA system may require integration with the scan rate and the protocol currently in use by the AEPSO.

6. Business and operations processes

A standard information technology approach should be used to capture the MIC interactions and information exchange necessary to accomplish the many functions involving interconnected DR sites. These functions cover operational requests for dispatch as well as monitoring of the operational aspects of DR. In the information technology community, these processes are termed "business processes." They describe the scenarios of various parties and equipment accomplishing business objectives. Business process modeling reveals the requirements embedded in these interactions and identifies commonalities of interaction and information exchange in different processes. A popular language for modeling these processes and the information involved is UML.

For background on business process concepts and the use of UML, see Annex D.

This clause describes the organization of the many processes relevant to the scope of monitoring and information exchange in this guide. It begins with a summary of the aspects of UML that will be used to model these processes, interactions, and information. Next, it organizes the business and operations processes in a rational way to describe the range of usage and ensure that the major areas of MIC functionality are addressed. UML defines the mechanism to describe a business process as a use case. By using the use case methodology, one can identify the information to be exchanged and constraints on the sequence of operation for DR MIC. The attributes of a use case pertinent to this guide are presented next. This clause ends with representative samples of business processes. Because the business processes captured in use cases are numerous, the full uses cases are documented in the Annex F. Besides identifying general DR interconnection scenarios, these sample use cases serve as examples of how individual MIC interaction requirements can be captured.

6.1 Developing business processes using UML

Object-oriented methodologies for information modeling often use UML concepts and conventions. The approach for using UML to develop business-process use cases is as follows:

a) Select a business process (e.g., basic dispatch of a DR unit for energy).

b) Describe the business process in narrative form.

c) Determine all the actors (e.g., DR operator and AEPSO).

d) Determine the use case systems involved (e.g., the DR controller).

e) Describe all performance requirements, pre- and post-conditions, and other assumptions (e.g., a response to a request for status information shall be within 30 s, and the post-condition is that the DR unit is shut down and ready for dispatch in the future).

f) Draw and describe the interactions between the actors and use cases, including the information exchanged, the sequences of steps, and the decisions affecting information flows (e.g., sequences for starting a DR unit). These can be documented in activity diagrams, sequence diagrams, collaboration diagrams, and state diagrams, along with text to clarify the interactions.

6.2 How business processes are addressed

As mentioned earlier, use cases capture the MIC interactions between the users of DR and the DR. The categories of information to capture in a use case are included in Annex E. These items include the following:

— The name of the use case.

— A brief description.

— A narrative that describes the usage scenario that is about to be described. (This is a less formal account of the interactions that allows the reader to more easily understand the capability that is being exercised.)

— The actors involved in the use case.

— The systems that are participating in the use case.

— Any assumptions and design considerations of the use case. This can include limitations, constraints, or variations that may affect the use case including:

  — Regulations, policies, and financial considerations
  — Performance and timing requirements
  — Frequency of use or wait periods between use
  — Sizing, configuration of equipment and systems, numbers of devices, and volume characteristics
  — Quality of service
  — Information security and privacy issues
  — Physical operations security issues (e.g., stability and voltage control)

— The pre-conditions assumed at the initiation of the use case.

— The normal sequence of steps that describe the interactions between actors and the system and the information being exchanged at each step. This represents the main part of the use case.

— Any alternative or exception sequences. Separating the alternative sequences helps keep the normal sequence clear and as simple as possible.

— The post-conditions assumed at the conclusion of the normal sequence.

— Any references to other use cases or relevant documentation.

— A list of the outstanding issues associated with the use case.

— A revision history indicating the versions of the use case, what was done in each version, and who did it.

— Any diagrams that help clarify the use case. These are expected to follow the UML diagram conventions.

6.3 Representative business processes

Information exchanges are determined by the MIC functions required for monitoring, controlling, maintaining, and managing DR devices and installations. There are many business processes to consider when exploring relevant functionality to these guidelines. Rather than present details on all of them, a small number of representative use cases are developed to present the breadth of common MIC interactions related to interconnected DR operation. These use cases were selected to demonstrate patterns of interactions for MIC and may not represent the most common operations.

In particular, much of the information to be exchanged is the same for many use cases, and the availability of different types of information will be determined by the equipment capabilities, the installation choices, and the degree of precision that the business processes necessitate. A few representative business processes that cover key information exchange requirements have been identified. These selected business processes can be assessed in detail to determine the minimum information exchange needs as well as the optional information exchange needs that may typically be encountered. In addition, aspects of multiple use cases can be combined to create new use cases that may span multiple interactions between parties. Table 2 contains examples of use cases.

Table 2—Example use cases

Use case	Description
DR unit dispatch	The DR operator dispatches a single DR unit for parallel operation with the area EPS and coordinates with the AEPSO for economic energy (no ancillary services) for shaving peak. This is a diesel generating unit that requires environmental monitoring.
DR unit dispatch for energy export	The DR operator of a single-unit 1.1-MW wind turbine intends to operate as an independent power producer. The DR operator will dispatch his DR unit with the intention of selling energy back to the owner of the area EPS.
DR unit scheduling	A DR operator creates, edits, and deletes schedules to dispatch commands to a DR unit. The DR operator's system communicates the scheduled operation to the DR controller, who invokes commands to the DR unit at appropriate times and notifies the DR operator of status.
DR aggregation	The DR operator dispatches multiple DR units during peak periods of energy usage per information (e.g., real-time pricing, dispatch request, and interruptible rate) provided by the DR aggregator and coordinated with the AEPSO. The DR aggregator monitors net metering information from the site.
DR maintenance	A DR owner contracts with a DR maintainer to periodically service a DR unit and perform emergency repairs. The DR maintainer monitors key performance indicators and coordinates with the DR operator when service is required.
DR ancillary services	The DR may be utilized to provide any or all of the following ancillary services: load regulation, energy losses, spinning and non-spinning reserve, reactive supply.
DR providing reactive supply	The DR unit may provide reactive supply by absorbing VARs or producing VARs by changing the field current to match a pre-established schedule. Alternatively, a stated power factor on the high side of the interconnection transformer or PCC can be established.

See Annex F for the use cases cited in Table 2. The following list summarizes the nature (stakeholders and DR technology) of the use cases found in the annex:

— The DR unit dispatch use case provides the basic information exchange interactions between a DR operator and a DR site and the coordination with an AEPSO. The use case assumes that the DR site does not back feed energy into the area EPS. It also presumes a fossil-based prime mover so that environmental information exchange can also be explored.

— The aggregation of energy use case presents a situation in which a DR aggregator is involved to coordinate several DR sites in packaging a significant amount of energy for the marketplace or area EPS needs. Net metering issues are also introduced in this use case.

— The DR unit scheduling use case explores the possibility of a DR operator configuring a DR controller with operation schedules to be executed at a future time. Coordination with an AEPSO is also in this case.

— The DR maintenance use case considers the needs of a maintenance provider to be able to remotely monitor and access information concerning a DR unit's performance.

— The DR unit dispatch for energy export use case looks at a wind farm installation in which energy can flow back into the area EPS.

— The DR ancillary services and DR reactive supply use cases explore DR uses to supply ancillary services to the area EPS.

7. Information exchange model

Suppose two parties, Party A and Party B (e.g., a DR controller and an AEPSO), decide to collaborate on an activity. Once they agree on what information is required to support their application, they need to agree on the method they will use to get this information to flow between them. The framework for discussing this is called an information exchange model. The information exchange model defines general concepts that can be used in specific designs that become implemented with real DR units, real protocols, and real communication channels.

This clause does not prescribe specific designs or implementations but provides a conceptual framework from which commonly held ideas and vocabulary can be applied to DR MIC. Rather than being "plug and play," a shared information exchange model facilitates the mapping to specific implementations. Implementations can be based on industry standards or proprietary solutions, or because there are many levels for agreement to achieve interoperation, an implementation can be a combination of these. The information exchange model does not rule out any of these approaches or the creation of new standards and solutions.

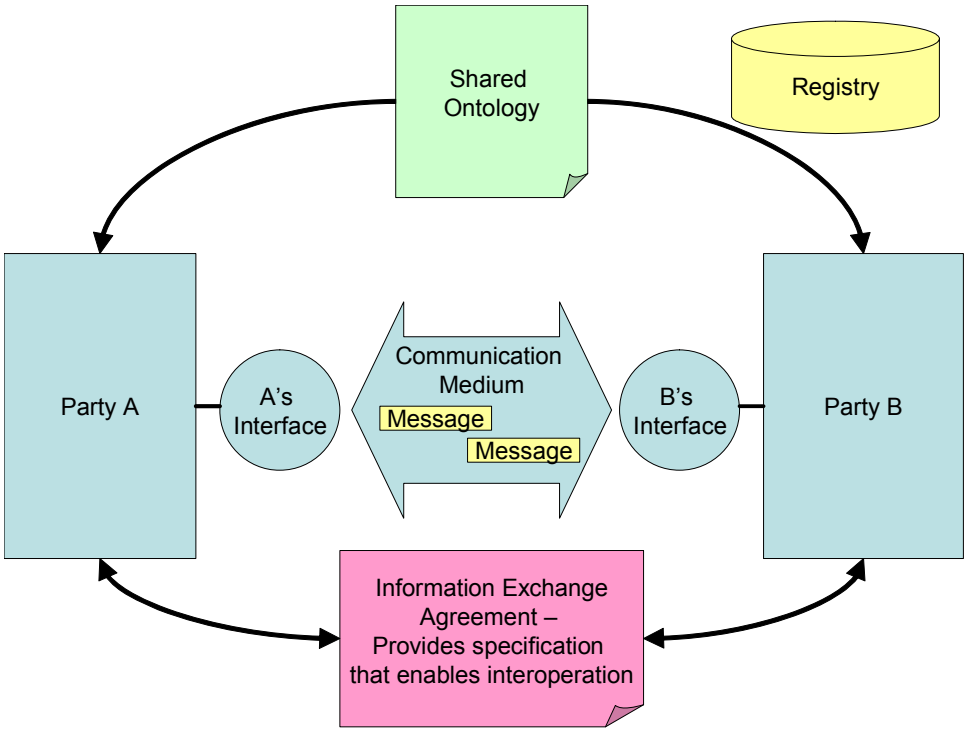


Figure 3—Information exchange model elements

7.1 Information exchange model elements

As shown in Figure 3, for any interaction to succeed, the parties involved must agree on several elements of communication. The elements of an information exchange model are described in an information exchange (or collaboration) agreement. This agreement specifies the interface that each party exposes to the outside world. The interfaces send or receive messages that contain information in a certain form and understandable content. The data exchanged can be specified in an agreed-upon structured vocabulary that is common or shared between the two parties. This shared vocabulary is referred to as the DR MIC ontology.

Ontologies are constructed, shared, and standardized throughout enterprises and trade organizations as a way to develop consistency of nomenclature and relationships within a topic community (or "domain"). For example, if the topic is "cinema," then an ontology might include concepts such as cinema, genre, movie, and musicals. Properties of these things include actor, actress, cinema name, director, duration, music director, producer, and so on.

Though the information exchange model elements are provided to provide context, the focus of this guide is on the ontology for DR MIC and a template for specifying the important components in an IEA.

7.1.1 Information exchange agreement

The information exchange agreement (IEA) describes the roles and capabilities of the parties to achieve a shared outcome. It specifies the interface, message definition, and message content supported between two transacting parties. In some sense, it is similar to a protocol; however, beyond the form of handshaking, the IEA explains what actions (or services) its interface can perform, what format it expects in the message being communicated, what approach of securing the interaction is used, and what things that are contained in the message mean (the ontology).

7.1.2 Interface

An interface is the point of contact that a software component has with its interacting partners. The interface describes the services that a party agrees to support. Some interfaces are defined by the protocol they support [e.g., Distributed Network Protocol 3 (DNP3) or open connectivity (OPC)], which in turn, define a generic set of services (e.g., read, write, publish, subscribe). In some approaches, the designer has the flexibility to define services (e.g., a Web services approach). In this case, the services must be described and shared with the transacting parties so they know what is available and how to use them. Interfaces also specify the proper sequencing of information needed to affect an outcome. For example, before a switch can be opened, it must be selected for operation in a previous message exchange.

Loosely coupled networked systems, usually built on Internet-based technologies, are becoming popular in electronic business systems and are being applied for integrating DR MIC. A service-oriented architecture is a collection of services that communicate. The services are self-contained and do not depend on the context or state of the other service. They work within a distributed systems architecture. A service-oriented architecture environment has development and integration tools that allow interfaces to services to be defined and help the system integrator assemble solutions from these components. Web Services and Electronic Business XML, or ebXML, standards contribute to the support of the service-oriented architecture concept.

7.1.3 Message

The message is the quantum of information that is communicated between parties. Protocols specify the format of the message and can have several layers of communication-related information. Here, the focus is on the action or service requested and the message content related to the business at hand, such as a DR unit parameter.

7.1.4 Resource registration and discovery

Modern information exchange technology includes methods to interrogate what an interface has to offer, including the services it supports, the information able to be exchanged (including type of DR device and size), and the identity (unique identifier and human-readable names) of the objects (things) that form the content supported by the

interface. The support of an interrogation (discovery) service allows a service requestor to find out which specific set of objects is involved in the communication.

To help system engineers integrate devices involved in the information exchange, the resource discovery interface can be used to browse (look up) the objects at a site and configure the collaboration. Although unique identifiers are needed to unambiguously identify an object, human-readable names are easier for an integrator to use. For this reason, naming rules are instituted so that ambiguity is diminished as integrators traverse commonly used paths through the information. These rules are specified in namespaces. For example, a discovery service at a DR site could be used to find all the DR units managed by a DR controller. For each DR unit, the discovery service might provide information about its name and model number. The namespace may require uniqueness of names for the DR units managed by a DR controller so that people using the service can unambiguously reference each DR unit.

In addition, implementations may make use of the concept of a registry. A registry is a separate set of software that stores information about the components involved in an information exchange as well as aspects of the IEA itself. A registry is a separate repository that is shared by a community of interested parties. It is much like a telephone book, though the community can decide to strictly control access to the registry. Parties can register their devices and interfaces with the registry. One can query the registry's repository to find information about transacting parties and the communication mechanisms they support. For example, documents that contain the standard IEA that a party supports could be stored in a registry. Those wishing to conduct business electronically with this party could be directed to the registry, where (with permission) they can download a copy of the standard IEA.

Because a registry is a service for a community of players, third parties may exist with the purpose of maintaining proper operation of the registry service. The concept of a registry could be applied to a limited, closed implementation integrates DR, or it could be open to a larger community. Registries can be automated for machine-to-machine coordination, or they can be applied to support human look-up capabilities.

7.1.5 Ontology—shared vocabulary

The ontology unambiguously defines the real-world concepts that are referenced in an information exchange. It provides a common language (shared meaning) about these things and their relationship to one another. Interacting parties commit to the ontology so that they can communicate about DR without necessarily committing to a globally shared theory of operation. Different information exchange implementations involving different approaches and protocols may call these things different names, but the ontology serves as a common point for interpretation. The terminology used in the ontology is derived from the information identified in the use cases described earlier.

In database terms, an ontology is similar to a database schema; however, whereas a schema is implementation-oriented, an ontology is more conceptual and can be used to derive different schemas depending on the way a designer wishes to map these concepts into data structures. Intelligent agents and other programs make use of shared ontologies to facilitate interoperation, and they are an important foundation for enabling the trends in the Internet community toward the Semantic Web.

The maturation of ontologies has grown to the point that there are now standards for capturing and registering ontologies. For example, Web Ontology Language includes an XML-based language for writing ontologies based on Resource Definition Framework/Schema. A series of tools with graphic visualization support for capturing an ontology are based on UML (see Clause 6). These tools allow those specifying the ontology the ability to create a visual map that graphically shows the classes of interest and the relationships among them. Report tools also allow the user to list descriptions and associated parameters in a document format.

7.2 DR MIC ontology

Establishing an ontology for DR MIC can significantly facilitate integration. By getting commonly accepted terms, definitions, and allowable relationships for DR MIC information, a user community can more quickly understand complex concepts, avoid re-inventing terms, and form the basis of something that can be improved in a controlled manner over time.

The bulk of this subclause focuses on an ontology for DR MIC.

7.2.1 UML approach to documenting the DR MIC ontology

UML provides a widely accepted information modeling framework for representing an ontology. In the power system area, IEC 61970 [B26] has developed the Common Information Model (CIM) as an ontology for EMS integration and extended it for distribution systems and utility enterprise integration. The CIM contains classes (object types) such as substations, breakers, and work orders as well as other data typically found in an EMS, SCADA, distribution management system, or work and asset management system. The CIM is defined in UML and contains many basic modeling concepts (such as attribute units and resource naming) that can be borrowed for DR MIC. (See the IEC 61970-300 series [B27] for the CIM.)

An ontology rendered in UML documents real-world things in terms of classes, attributes, and associations (i.e., relationships) and provides unique names and definitions to each object.

7.2.2 DR MIC ontology example

This subclause describes an example of a DR MIC ontology. It is inspired from the relevant CIM classes of IEC 61970-300 [B27] and extends them with classes and relationships proposed by recent work in this area. The following UML class diagram (Figure 4) graphically shows the classes (things) whose information is relevant to the content of DR MIC messages. The shaded boxes in the diagram indicate classes that already exist in the CIM.

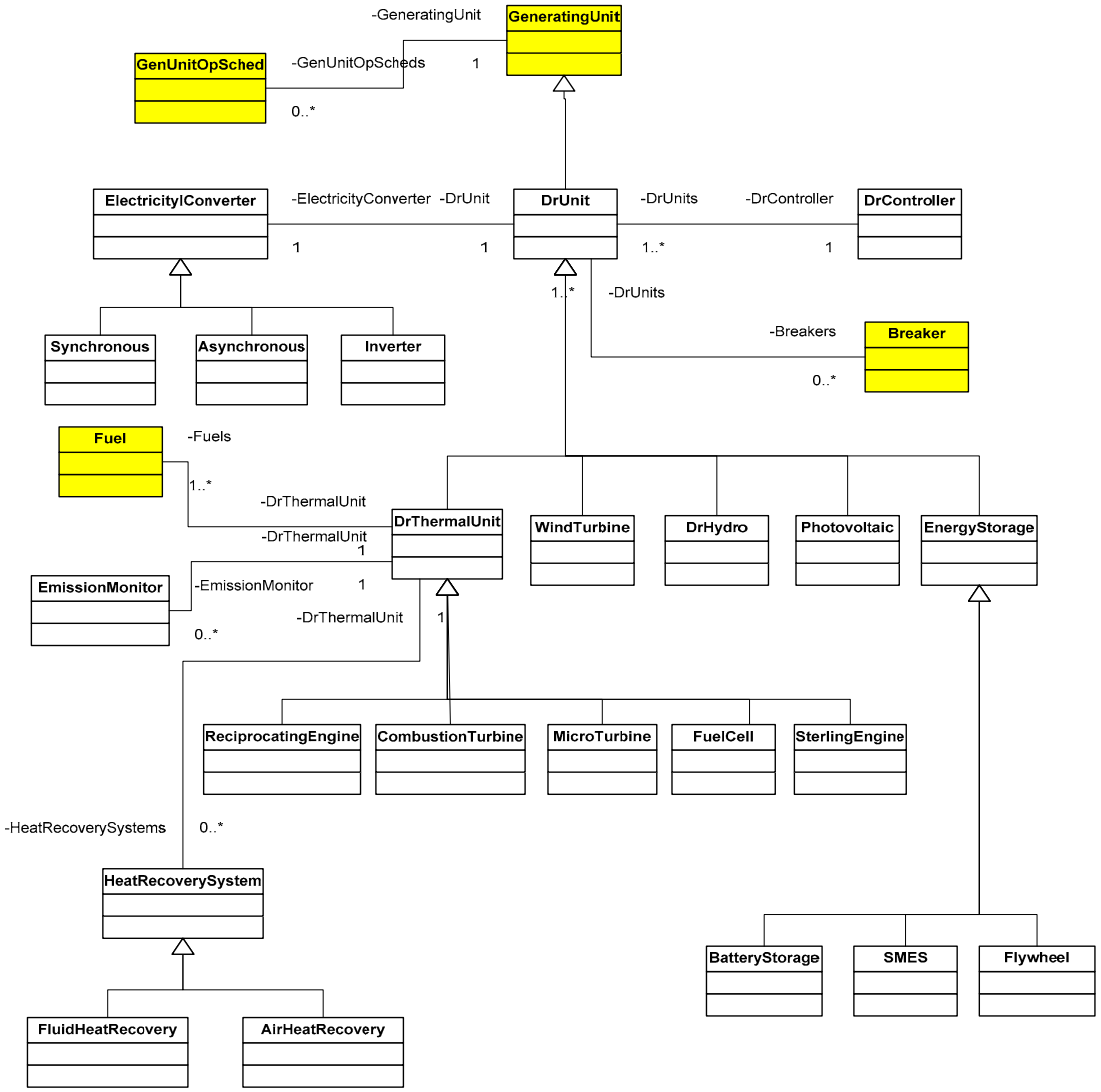


Figure 4—UML class diagram of DR MIC ontology

Note that in Figure 4 the DR unit class inherits from the GeneratingUnit. The contents of this diagram can also be produced in tabular form that identifies each class, its attributes, and its associations, including those it inherits from other classes (IEC 61970-300 [B27]).

Attributes exist for each of the classes in the ontology. The following is an abridged list of attributes for the DrUnit class that are identified in the use cases of Annex F. The use cases identify the information exchange needs for accomplishing real-world interactions. The names and concepts also need to be reviewed against similar attributes in the CIM to enhance consistency and completeness. Many attributes will be “inherited” from parent classes (e.g., DrUnit inherits the attributes from the CIM GeneratingUnit class). Attributes relevant to a specific type of DrUnit, such as engine temperature in ReciprocatingEngine, would be found under the specialized classes that inherit from the DrUnit class.

In the following example, the classes DrUnit and Breaker are described. DrUnit is shown to inherit some attributes and an association from the GeneratingUnit Class, while the remaining attributes and the association with the Breaker class are native. "Native" means that the attributes and associations are defined directly with the class in question.

Example of Breaker DrUnit classes with attributes and associations

Breaker
A mechanical switching device capable of making, carrying, and breaking currents under normal circuit conditions and also making, carrying for a specified time, and breaking currents under specified abnormal circuit conditions (e.g., those of short circuit). The typeName is the type of breaker (e.g., oil, air blast, vacuum, or SF6).

Breaker attributes
Native attributes

Name	Units	Definition
Naming.aliasName	(String)	Free text name of the object or instance
ampRating	Amperes	Continuous rating in amperes
intRating	Amperes	Fault interrupting rating in amperes
inTransitTime	Seconds	The transition time from open to close, in seconds
normalOpenSwitch	Boolean	Set if the switching device is normally open

Breaker associations
Native roles

Association name	Related class	Definition
IsolatesDrUnit	DrUnit	A DrUnit may be isolated by a circuit breaker

DrUnit

The DR unit is a source of electric power that is not directly connected to a bulk power transmission system. DR units include both generators and energy storage technologies.

DrUnit Attributes

Native attributes

Name	Units	Definition
WattOutput	Watts	Real power output at DrUnit connection
VarOutput	VAR	Reactive power output at DrUnit connection
Voltage	Volts	Voltage at point of DrUnit connection
OnOffStatus	Enumeration	Unit is on or off
OperationalState	Enumeration	Starting, stopping, ramping
ConnectionType	Enumeration	Three-phase or single-phase, delta, wye
VoltageRating	Volts	Voltage rating of the unit
AmpRating	Amps	Current rating of the unit
NominalFrequency	Hertz	Nameplate frequency
VoltAmpRating	Volt-Amps	Power rating
MaximumWattRating	Watts	Maximum real power rating
VarRating	VAR	Reactive power rating
Synchronized	Enumeration	Unit synchronized to EPS or not
OperationalTime	Seconds	Time unit has been operating since started
TotalWatthours	Watthours	Total energy delivered since started

Attributes inherited from GeneratingUnit

Name	Units	Definition
Name	String	Free text name of the object or instance
Identifier	Binary	Unique identifier (machine-readable)
Location	Global positioning system coordinates	Global positioning system location of device

DrUnit Associations

Native roles

Association name	Related class	Definition
IsolatingBreaker	Breaker	A Breaker may isolate a DrUnit for protection and maintenance
ControlledByDrController	DrController	A DrUnit is controller by a DrController
GeneratesByElectricityConverter	ElectricityConverter	To produce electricity, the DrUnit has an associated converter

Associations inherited from GeneratingUnit

Association name	Related class	Definition
UsesGenUnitOpSchedule	GenUnitOpSchedule	A generating unit may have an operating schedule, indicating the planned operation of the unit

7.3 Information exchange agreement template

The following template for an IEA provides a framework to capture the specification of technology and processes needed to support interoperable interactions between parties in the use of a DR unit.

1. Introduction
2. Theory of Operation Overview
3. Shared Ontology
4. Message Structure
5. Interface Services and Collaboration Agreements
   - 5.1. Business (Workflow) Message Definitions
   - 5.2. Choreography Rules (order/sequence of messages in a transaction)
   - 5.3. Transaction Services
   - 5.4. Resource Identification
   - 5.5. Resource Registration and Discovery
   - 5.6. Data and Time Formats
   - 5.7. Time Synchronization
   - 5.8. Security Agreements
   - 5.9. Expected Standalone Behavior
6. Performance Requirements and Constraints
7. Communication Protocol Profile
8. Version Compatibility
9. Miscellaneous
10. Example Usage

The subsequent subclauses describe the contents of each of these headings. Annex G provides an example of an IEA. Other approaches for MIC of DR units can use this example to help clarify how the various sections of the IEA template can be used to document particular implementations or other popular DR MIC implementations.

7.3.1 Introduction

Introduce the IEA and its typical applications. If the technology and interaction processes are already described in other specification documents, such as standards, then reference the overriding work that forms the basis for the agreement.

7.3.2 Theory of operation overview

Describe the approach to interaction with the DR site and between parties of the information exchange. For example, some approaches may be command and control-oriented, while others offer information that allow the interacting party to decide the appropriate response based on local conditions and knowledge.

7.3.3 Shared ontology

To understand the message content, the meaning of the terms and their relationships used in the messages are captured in an ontology. Reference any standard or proprietary ontologies used, or document the special ontology used in this case. Mapping terms to the DR ontology provided in this guide can facilitate the understanding of terms among parties. In addition, semantic mapping tools (inference engines) can help automate the process of associating message content to a party's local view of information.

7.3.4 Message structure

Describe the message structure used primarily at the application layer of communications (i.e., the information associated with the application of the DR unit and its interaction with the other parties). Typically, this structure includes the envelope (the format of what goes around the message to package it), the header (the leading information that provides context for the main content of the message), and the payload (the main content of the message). The format of the information contained in this structure is important to describe. For example, the message payload may use XML. As another example, referencing Simple Object Access Protocol (SOAP) describes a complete message format with envelope, header, and payload structure.

7.3.5 Interface services and collaboration agreements

An interface is the point of contact that a software component has with its interacting partners. An interface service provides clearly specified actions at an interface, such as establishing a connection, initiating transactions, and exchanging information models. Different types of interfaces are used for different types of devices and different installations. These interfaces may conform to different specifications (open or proprietary). Different generic services are supported by interfaces that follow various interoperation specifications (e.g., Web Services, ebXML, IEC 61850 [B14], OPC, BACnet, LonWorks®, ModBus®). This document does not define generic services or special services but states that they need to be specified as part of the IEA.

7.3.5.1 Business message definitions

Define the messages for accomplishing the work at hand (i.e., implementing a business process use case). Some approaches use generic messages such as the commands Get, Set, Report by Exception, or Query) and are qualified by reference to specific information items. Others may be more application-specific, such as Request Status, which may expect a fixed or variable response about the state of an isolation breaker, the real and reactive power output of a DR unit, and a time stamp.

7.3.5.2 Choreography rules

The order or sequence of messages in a transaction is important to understand for interoperation. For example, a Select-Before-Operate sequence may require acknowledgement as a part of the message exchange before subsequent messages will be issued. Interaction diagrams, such as used to describe use cases, can be used to depict choreography rules.

7.3.5.3 Transaction services

Transaction services provide options for message exchange between parties. These services can include the following:

- Reliable delivery
- Message delivery prioritization
- Synchronous/asynchronous communication
- Non-repudiation (log or audit trail)
- Exchanges of the ontological message structures
- Connection establishment and disconnection
- Security services
- Network management services
- Error and failure management services

7.3.5.4 Resource identification

Real-world objects are realized as instances of the conceptual classes specified in the ontology. To reference objects and distinguish among them, a resource identification system is needed. This subclause describes the approach that the interacting parties agree to regarding resource identification. Although all objects inherit a name attribute, there is a need for a unique identifier to preserve identity through equipment movement and modeling changes. This can also support the need for one or more human-readable names associated with an object, particularly because different users of the equipment may use different names.

7.3.5.5 Resource registration and discovery

This subclause describes the resource registration and discovery methods used among parties as appropriate. These methods could include completely manual methods (e.g., paper exchanges and subsequent data entry) or more automated methods.

Information about resources or IEAs themselves can be made available through a registry. Describe such a facility as applicable to the agreement.

7.3.5.6 Data and time formats

Describe the format for data (such as the way integer, real, and text information is represented in a message). Also describe the format for time and date information, including what time zone is being used and how daylight savings time is handled, that is exchanged between parties.

7.3.5.7 Time synchronization

Interoperability generally requires time coordination between the transacting parties. The needs in this area depend on the application enabled between parties. Time synchronization can be handled by many mechanisms, ranging from manual entry of time to constant time updates from global positioning system sources. Describe the requirements for the degree of accuracy, the approach for coordinating time, and the expected response to failures in time synchronization.

7.3.5.8 Security agreements

Describe the security agreements that are required for all interactions among the parties. These security agreements should cover both the broad security policies that include information handling by the parties involved and the actual security services that will be implemented for the electronic interactions.

The security agreements should include the following:

- Security policy on information handling
- Agreements on the requirements for confidentiality, integrity, availability, non-repudiation, and accountability for each type of message exchange
- Specific requirements for access control, including role-based access structure, passwords (management and updates), other access control policies, and methods of enforcement
- Specific requirements for the authentication procedures and technologies
- Specific requirements for the authorization of end users and software applications
- Specific requirements for encryption and key management, including encryption algorithms, certificates (e.g., management, updates, revocation, and identification of certificate authorities if public key infrastructure is used for key management), and other methods of key management, if used
- Specific requirements for the logging and audit trails
- Agreements on intrusion detection and management, as well as intrusion recovery and forensics

7.3.5.9 Expected standalone behavior

Describe the expected operation of each party involved in an interaction in the event that communication is lost.

When successful communication is compromised, system components need to move to operating positions that respect safety and overall system health. For a DR site, this may mean opening the electrical link to the area EPS depending on the situation, or it may mean leaving the link closed. All parties involved need to agree to the expected actions to take when communication is lost.

7.3.6 Performance requirements and constraints

Describe the performance expectations for successful interaction. Aspects of performance include the following:

- Availability of each information flow
- Accuracy of data (i.e., data quality identification requirements)
- Information flow timing (e.g., start times, time windows)
- Error/failure recovery contractual time requirements
- Information retention
- Update/change management requirements

7.3.7 Communication protocol profile

Describe the allowable communication protocol profiles that can be used by parties. The descriptions of the protocols should include all parameters and settings that are needed to ensure interoperability.

The messages are transported on a communication profile that specifies one or more protocols to cover the various ISO layers. Some protocols specify all the communications layers (see the OSI model in Clause 8). Others may only specify some of the levels. This section of the agreement needs to discuss the communication profile of one or more protocols that are needed for interoperation.

7.3.8 Version compatibility

Describe which versions of ontology, services, messages, protocols, and security will be supported while still maintaining interoperability.

7.3.9 Miscellaneous

Provide a section to cover aspects of the agreement that do not fit in the other sections.

7.3.10 Example usage

Provide examples of interaction sequences that exercise the IEA to illustrate the interoperation supported by the agreement.

8. Protocol issues

8.1 Purpose

Clause 7 defined the information exchange models and standard interfaces that can be used in the DR MIC. The realization of those standard interfaces will depend on the protocols. Many protocols are used for various aspects of DR MIC (refer to Annex B). The protocols vary across a wide spectrum, from completely propriety and used only by the company that developed it to standardized and used across several industries. Protocols also span several stages of life cycles; some are new and employ the latest technology advancements, while others are quite old and primitive in their implementation. Therefore, it is beyond the scope of this document to pick and choose a set of protocols to be used in DR MIC. The document lays out several basic guidelines for protocol selection.

8.2 Desirable categories of protocols

A protocol is a formal description of message formats and rules that two or more devices follow to communicate across a network. Before selecting a protocol, one should understand the categorization of protocols. One common way to partition various protocols is the ISO OSI seven-layer reference model, namely, “application,” “presentation,” “session,” “transport,” “network,” “data link,” and “physical” layer. A protocol typically spans several layers. Protocols can be grouped into profiles. A protocol profile is an agree-upon sub-set and interpretation of the OSI model. In Annex B, various protocols are grouped into three profiles to provide a simplified view of the protocol space. The A profile (A stands for application) spans the upper three layers. The T profile (T stands for transport) spans the middle two layers and the L profile (L stands for data link) spans the lower two layer. For example, OPC is an A profile data exchange protocol, which is built upon Microsoft .Net technology. It has also been extended to include XML technology so that a greater level of interoperability can be achieved. Another example is Transmission Control Protocol (TCP)/IP, which is a T profile protocol, which is widely used. An L profile protocol example is EIA RS-232 [B3], which specifies signal voltages, signal timing, signal function, mechanical connectors, and data exchange formats.

Another way to categorize protocols is based on the concept of common services. A common service is a commonly defined functionality derived by identifying the cross-cutting distributed information requirements. For example, networks time synchronization is a common service, and NTP is a standard network time synchronization protocol to achieve this functionality. Another example is network management common service. The corresponding protocols are Simple Network Management Protocol and CMIP. A third example is security management.

8.3 Evaluation criteria

To meet information exchange requirements, a set of protocols—or, using more formal information technology terminology, a "profile" of protocols, is needed. For the data exchange requirements, one can consider the protocol selection based on the seven-layer model, or more coarsely, the A, T, and L profiles. Besides that, one should also decide how to achieve the common services such as network management, time synchronization, and security management, which have their own protocols. One can use several criteria to select a protocol "profile" to be used in DR MIC as follows:.

— *Platform Independence:* Having the ability to interface/share information with several platforms such as Microsoft Windows®, Linux®, UNIX®, and various embedded/real-time operating systems. An example of a protocol that does this very well is TCP/IP.[6] Computers and computing devices can use TCP/IP no matter what operating system or platform they are running.

— *Openness:* Having published concepts, rules, and implementations with non-restrictive use. In other words, standardized protocols will better serve the needs of DR MIC. One example is the well-known Hyper Text Transfer Protocol (HTTP). It is built on top of TCP/IP and has well-published rules. Therefore, anyone can implement it as long as the rules are obeyed.

— *Self-Describing:* Being able to investigate the contents of protocol messages and understand their intent, the data contained, and the structure in which the data are being transferred. XML-based protocols are great examples of self-describing protocols because XML tags describe the data they represent in plain text.

For more information about performance criteria, refer to Clause 4.

Other criteria include deterministic, security, expandability, and upgradeability.

8.4 Mapping data into protocols

Mapping data from DR sites into protocols can be difficult. Data from measuring devices must be fit into an acceptable form to be transmitted via the site communications protocol. Software data types are often used to make this mapping. This can result in problems because the data might not map into the data types of the protocol correctly. Data can be truncated or lost if the data type does not match the "real" world data correctly. Another issue with mapping data at DR sites is that data can come in several forms. Site devices transmit critical data over several media via several protocols. Mapping that data to provide a useful culmination of information from a DR site can be difficult because, unless there is a uniform protocol at the site, each protocol must be translated into a common format.

This issue can be solved by clear definition of the IEA and wise selection of underlying protocols. From the protocol aspect, the general guideline is to choose open, standardized, and widely accepted protocols. One example is XML-based protocols. The transport of XML can be based on SOAP, which, in turn, is built on HTTP. Therefore, it is platform-independent, and it is supported by Microsoft, Linux, and UNIX environments. Hence, mapping data to XML and then transporting that through SOAP could be a good way to handle information exchange for DR MIC.

[6] This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same results.

8.5 Protocol selection guidelines

Hundreds of protocols have been developed, and many more are under development. Within the lifetime of this guide, it is assured a universal standard protocol will not be agreed upon. However, the following guidance is presented to assist stakeholders in addressing how to approach the problem of such a large number of protocols from which to choose. What can be employed is a separation of the message content (payload) from the protocol into a common meaning of information content (semantics) that can be used by any present or future industry. Devices at the information-gathering level made by hundreds of manufactures do a great job of pulling the information and making the data available. An alternative approach to transmitting data over several protocols in an ad-hoc fashion at the site is to pull all the data together into an XML format and then use the communications protocol to transfer the XML-based information to whatever entity might need the data. XML makes sense because it is not a protocol-dependent format, it is interoperable, and it is self-describing. XML has also gained momentum across most industries as a popular means of data exchange, so if the data from a DR site needs to be exchanged with other systems in different industries chances are the XML format will be easily accepted. Besides message content, the actions (services) invoked or requested by a message and the sequencing rules for an action still need to be described by the information model, which includes the choices of protocols agreed to for interoperation.

9. Security guidelines for DR implementations

9.1 Introduction

9.1.1 Security challenges for MIC associated with DR

The security of individual DR units, and possibly the whole area EPS, could be threatened by inadvertent actions, malfunctions, or deliberate manipulations of a DR remote monitoring and control system. Where DR monitoring and control is a part of the critical infrastructure of the interconnected electric power system, appropriate security measures are essential. An effective security strategy requires an ongoing, top-down management commitment. If MIC systems of a DR system are integrated with those of the stakeholders, it can be said that security issues really have no boundary. Even though the scope of this document is limited to DR, the issue of security is much more encompassing.

DR monitoring and control systems face many security challenges. These include the following:

- The need to communicate with a wide range of stakeholders
- The increasing use of open infrastructures such as the Internet
- The need for integration of legacy systems
- The growing complexity in protocols and distributed computing
- The growing threats from and sophistication of hostile entities

9.1.2 Scope of security guidelines: information security

Security for DR systems can be divided into the following four main areas:

a) Information security for the MIC system covers cyber security, including communications links, databases, and interfaces among software applications.

b) Physical security of the DR plant, DR communication links, and area EPS control systems influence information security but is outside the scope of these guidelines.

c) The effect of the communications system performance on the reliability of the DR unit itself and that of the interconnected electric power system is also outside the scope of these guidelines.

d) Personnel security for the users of the DR plant, communications, and area EPS facilities is important to information security but is also outside the scope of these guidelines.

This clause focuses primarily on information security because the scope of this guide is MIC of DR. Information security encompasses the following four requirements:

1) Confidentiality of information
2) Integrity of information
3) Availability of information
4) Accountability (non-repudiation) related to actions

These concepts, and how they affect DR implementations, are discussed in the rest of this clause.

Different DR installations will require different degrees of security. One size does not fit all. Therefore, an assessment of security requirements will be needed on a case-by-case basis and should be related to the criticality of the assets and the cost of security measures and their effect on operations.

The severity of various risks should be balanced with the difficulty and cost of their prevention. This is best accomplished via a formal process of security risk assessment and development of a security policy. These issues are covered briefly in Annex E, but there are many documents that provide a more detailed framework for this process (e.g., ISO/IEC 17799 [B50], NIST 800-12 [B54]).

Security policies should continually evolve to address changing infrastructure while staying ahead of potential attacks from hostile entities. Constant vigilance (security monitoring and auditing) is needed, as is continuous adaptation to changes in the overall power system environment. There will always be residual risks that should be taken into account and managed, so DR systems need to be fault-tolerant and capable of appropriate autonomous operation. It is the very distributed and autonomous nature of DR that gives it the beneficial potential to increase the overall reliability of the entire power system.

These guidelines discuss the security issues that should be taken into account and that may affect DR installations. They cannot provide a specific set of recommendations because security needs vary widely, as do the types of security measures available and their associated costs. Actual security measures for a specific DR implementation need to be determined on a case-by-case basis.

9.1.3 Key security references

Security is an area of technology that is being addressed by many industries, and it is by no means specific to DR. Therefore, the following references should be viewed as key sources of additional detailed information:

- ISO/IEC 17799 [B50]
- NIST 800-12 [B54]
- IETF RFC 2196 [B41]
- IETF RFC 2401 [B43]
- AGA 12 [B1], which provides “bump in the wire” security solutions
- NIST SP 500-166 [B55]
- EPRI 100174 [B4]
- EPRI 100898 [B5]
- OASIS Security Assertion Markup Language (SAML) V2.0 [B57].

— EPRI 1012160, [B7], which contains a discussion of security issues and a comprehensive reference list.

— IEC 62351 series [B28] through [B32], which are the security standards for some key protocols, including DNP3, IEC 61850 [B14], and Inter-Control Center Communications Protocol (ICCP).

— FIPS Pub 140-2 [B8]. FIPS 140-2 is a standard that describes U.S. federal government requirements that information technology products should meet for sensitive but unclassified use.

— ISA–The Instrumentation, Systems, and Automation Society SP100 [B49], the proposed standard for wireless industrial automation

9.2 Security issues specifically related to DR

The security issues specifically related to DR include (but are not limited to) the items detailed in 9.2.1 through 9.2.3.

9.2.1 Security issues of importance to DR implementations

The following security issues are of particular importance to DR implementations:

— In multi-vendor environments, DR equipment and systems are provided by different vendors within one installation.

— Multi-company ownership raises security issues related to proprietary information versus public information, what information one company may or may not see, and what controls each is able to manage and is responsible for.

— Requirements for very rapid response and very high availability in protection relaying are needed.

— Requirements for rapid response for DR and area EPS operations are needed.

— There may be financial repercussions because of market operations, which could affect the owner or be more significant if the DR is needed in area control.

— Market fragmentation increases the need for interoperable security solutions across multiple vendors and multiple customers.

— In terms of temporal and spatial diversity, DR units have very different response time frames and can be widely distributed, which makes security measures more difficult to implement consistently.

— New power system configurations may use DR units as a resource to ameliorate disturbances rather than implement the current practice of shutting off DR units during disturbances. This may entail increased vulnerabilities to security threats and increased sensitivity to the effects of security attacks.

— The costs of implementing security measures need to be minimized because of the relatively low cost of DR implementations (compared with other power system facilities).

— Safety of personnel and equipment in the power system environment requires highly reliable systems.

— Security risk assessment for DR implementations may reflect both the criticality of the DR system to the owner and the importance of the DR system to the utility that relies on the power.

— Measuring security solutions, breaches, and effects allows quantifiable metric analysis of the costs associated with implementing security as well as the costs associated with different security breaches.

— Securing legacy systems is key to the overall security of DR implementations.

— Both internal and external threats need to be addressed.

— The security risks associated with accidental actions by authorized users need to be addressed.

9.2.2 Security measures of importance to DR implementations

The following security measures are of particular importance to DR implementations:

- Security policies that cover all aspects of security, including assessing security needs, creating procedures, determining technologies, training, auditing, and re-assessing security needs
- Individual and role-based access control, which includes methods for determining access needs and restrictions for individuals and the roles they play within the DR environment as well as techniques (procedures and technologies) for enforcing these access rules
- Multiple layers of security to improve defense against inadvertent careless actions, equipment failures and malfunctions, and deliberate attacks
- Passwords, certificates, smart cards, biometrics, and other methods for authenticating access
- Physical and cyber intrusion detection to detect and alarm unauthorized activities
- Intrusion mitigation methods and technologies to minimize damage from intrusions, whether detected or not
- Access control lists in router firewalls, which are common and effective for limiting access to authorized Internet Protocol (IP) addresses (although they should not be considered infallible because of the difficulty of maintenance)
- Public key infrastructure, key management, transport layer security (TLS), virtual private networks (VPNs), and other typical cyber security solutions for communications, particularly across organizational boundaries
- AGA Cryptographic Protection of SCADA Communications [B1]: Basic recommendations can provide one relatively simple method for adding some level of security for legacy systems
- IEC 62351 series [B28] through [B32] security standards for DNP3, IEC 61850 [B14], and ICCP, which provides security for these commonly used protocols.

9.2.3 Examples of security measures for different levels of DR criticality

Table 3 illustrates how some security measures could be associated with different levels of DR criticality. This table is an example only and should not be viewed as definitive.

Table 3—Examples of security measures for different levels of DR criticality

Security measure	High criticality of DR	Medium criticality of DR	Low criticality of DR
Security policy	✓	✓	✓
Individual and role-based access control	✓	✓	✓
Multiple layers of security	✓	✓	
Passwords	✓	✓	✓
Certificates or smart cards	✓	✓	
Intrusion detection	✓	✓	
Intrusion mitigation techniques	✓		
Access control lists in firewalls	✓	✓	
Public key infrastructure, TLS, VPNs, etc.	✓		
Bump-in-the-wire encryption		✓	
IEC 62351 [B28]–[B32] security standards	✓	✓	

9.3 Potential security threats to DR systems

There are many potential information security threats to DR operation, including the following:

- Disgruntled employees
- Industrial espionage
- Competitors
- Carelessness
- Bypassed security mechanisms
- Equipment failures
- Inadequate training
- Terrorism

These threats can use the following methods to attack a system.

9.3.1 Spoofing

Spoofing is the imitation by an illegitimate entity of a legitimate entity to obtain unauthorized access, issue improper controls, or modify data.

9.3.2 Replay attacks

Replay is the capturing and resending of prior legitimate messages to cause improper actions.

9.3.3 Man-in-the-middle attacks

“Man in the middle” is a hostile entity configured to intercept information, potentially modify it, and then resend it to a recipient without the knowledge of either the original sender or the receiver.

9.3.4 Data manipulation

Data manipulation includes the following:

- The supply of false data to manipulate markets or equipment dispatch
- Falsified outage data
- Modification of time stamps

9.3.5 Viruses and worms

Viruses and worms can modify system operation or cause malfunction and loss of data.

9.3.6 Loss of privacy

Loss of privacy is the release of private data at the personal or corporate level.

9.3.7 Key management

Key management problems may include the following:

- Exposure of keys during distribution or through social engineering

— Exposure of algorithms (which is not a problem with current open standards because security is provided by the key, not the algorithm)

9.3.8 Network issues

A network issue is the interference with network hardware and software (e.g., routers, gateways, and domain name servers) using any of the attacks in this subclause. Mesh networks are ad hoc networks that have no fixed routing, so unauthorized joining or disruption can be more troublesome.

9.3.9 Time stamp issues

Time stamp issues involve the following:

— Falsified time servers

— Possible control, authentication, or auditing implications

9.3.10 Denial of service

There are several classes of denial of service. They are as follows:

— Overload of communications services

— Resource exhaustion (e.g., file names or storage space)

— Exploitation of improper coding (e.g., buffer overflow and undocumented commands)

— Exploitation of protocol oversights (e.g., deadlocked states)

Practices to minimize the threat of denial of service attacks are as follows:

— Monitoring inter-domain communications for excess traffic

— Implementing timeouts and connection limits

— Testing for coding errors and protocol oversights

— Testing for vulnerabilities with publicly available tools

— Providing fail-safe operation upon loss of communications

— Allowing suitable levels of autonomy so DR can perform limited functions without communications

9.4 Network security considerations

The following subclauses discuss security considerations related to common communications media, protocol, networking, and application interactions. This list is representative of the communications systems used for DR implementations, but it is not exhaustive.

9.4.1 Media security considerations

The following subclauses deal with the physical layer of the ISO OSI seven-layer model for network communications.

9.4.1.1 Dial-up access

Dial-up access is routinely used for remote maintenance. It should be implemented through the use of RADIUS (IETF RFC 2865 [B46] IETF and RFC 2869 [B47]) when feasible. It is important to implement so denial of service is mitigated (e.g., time-outs are applied for inactivity or invalid activity and only valid protocol and application messages are allowed). For instance, vendors sometimes implement auto-answer equipment, which opens a security hole in the network.

9.4.1.2 Dedicated serial communications

If the path of the serial link or the protocol does not provide adequate confidentiality, particularly if it extends outside a physical or electronic security perimeter, then either encryption or external hardware should be applied.

9.4.1.3 Telecommunication providers

Because telecommunication providers implement their own security measures, which may not be visible to users of their services, service level agreements should be used to contract with telecommunication providers to require exact levels of availability, throughput, timeliness, confidentiality, and other performance requirements.

9.4.1.4 Fiber optic cables

Fiber optic cables provide immunity to electromagnetic noise and eavesdropping through electromagnetic coupling. They are not immune, however, to other forms of attack.

9.4.1.5 Wireless media technologies

Current offerings are based on the older narrow-band or the newer spread spectrum radios. Spread spectrum is offered only in the newer, unlicensed (i.e., industrial, scientific, medical) bands. For example, in the United States, licensed radios are protected by the Federal Communications Commission (FCC) from interference, while the unlicensed band radios are forced to “tolerate” interference from other sources. In reality, the protection offered by the FCC for licensed radio frequencies results in only slightly better protection; the effectiveness of security is related to the degree of its enforcement. Newer bands have been authorized for other services such as implantable and bedside medical devices and other special applications.

The security issues surrounding wireless include both real and perceived shortcomings. The current commercially available products offer security in much the same way as wired networks—through encryption and key management such as described in IEEE Std 802.11i™ [B34]. Other techniques can make the wireless link harder to detect and intercept, but no commercial products are currently available. In the United States, standards for government communication security now include wireless under FIPS 140-2 [B8]. Only a few suppliers offer wireless products that meet this standard, but more are expected as customers demand this protection.

Available spread spectrum technologies include direct sequence spread spectrum and frequency-hopping spread spectrum. The Wireless Industrial Networking Alliance (www.wina.org) is a consortium of end users, suppliers, academics, and technology experts chartered to help sort through the alternatives and end user requirements to make decisions less onerous.

Other technologies (such as orthogonal frequency division multiplexing) are being commercialized, but these are not truly spread spectrum. Their security advantages are yet to be demonstrated. New spread-spectrum technologies, such as hybrid spread spectrum and ultra-wide band, may offer some advantages in overcoming security issues associated with wireless connectivity, but there are no commercially available systems.

In theory, wireless can offer security advantages over existing wired connectivity, but no commercial products have emerged. These technologies—which include low probability of detect and low probability of intercept—are being tested in laboratories. Issues such as cost, complexity, and user demand have thwarted attempts to bring commercial products to the marketplace.

Some examples of available wireless technologies are as follows:

- Digital microwave radio
- Satellite leased channels
- Very small aperture terminal for satellite systems
- Spread-spectrum radio
- Wi-Fi, based on IEEE Std 802.11 b/g/i/n [B34]
- Bluetooth™, based on IEEE Std 802.15.1 [B35][7]
- ZigBee™, based on IEEE Std 802.15.4 [B37][8]
- WiMAX™, based on IEEE Std 802.16 [B38][9]
- Cell phones, including general packet radio service and global system for mobile communications

9.4.1.6 Communication path selection

Additional security (increase availability) can be obtained by having alternate paths available in case of failure of the primary path. In many cases, it is possible to choose a communications path so encryption is not required. An example is inter-unit communication in a physically secure environment.

9.4.2 Protocols and network security considerations

9.4.2.1 Virtual private networks

Virtual private networks (VPN) technology can be used to improve security when the communication path is not secure. However, VPN does not provide security between applications; it only provides security for the communications channel.

9.4.2.2 IP security and IPSec

Currently available routers typically have firewall capabilities, which include the ability to monitor and filter IP addresses through access control lists. These access control lists should be kept up to date. A few simple rules are better than a long list of special-purpose rules. IPSec (specified in IETF RFC 2401 [B43]) was developed by the Internet Engineering Task Force Security Area to provide interoperable, cryptographically-based network layer security for IPv4 and IPv6. The set of security services, provided at the IP layer, includes access control, connectionless integrity, data origin authentication, protection against replays, confidentiality (encryption), and limited traffic flow confidentiality.

9.4.2.3 Transport layer security to secure TCP/IP

Transport layer security (TLS) is the security technology used over the Internet for TCP/IP security. (When TLS is being used, most browsers show a little lock or other security symbol.) TLS can provide transport-level authentication, integrity, and confidentiality for all communication systems using TCP/IP.

[7] Bluetooth is a trademark owned by Bluetooth SIG, Inc.
[8] ZigBee is a trademark owned by Zigbee Alliance.
[9] WiMAX is a trademark owned by the WiMAX Forum®.

9.4.2.4 Security for ModBus

This is a de facto standard protocol that is in wide deployment. It can be used in a serial- or network-based deployment (TCP-based). There are no provisions in the basic ModBus protocol for security, and no authentication extensions are known to be in development. Security can be added through "bump in the wire" technologies such as AGA 12 [B1], or through the use of IEC 62351-3 TS [B29] if ModBus is run over TCP.

9.4.2.5 Security for DNP3

Security for DNP3 is being standardized by the DNP Users Group based on IEC 62351-5 [B31] security standard for IEC 60870-5 [B10].

9.4.2.6 Security for IEC 61850

Security for IEC 61850 [B14] is being standardized in IEC 62351-6 [B32], which also requires TLS if it is run over TCP.

9.4.2.7 Security for ICCP (IEC 60870-5 TASE.2)

Security for ICCP is being standardized in IEC 62351-4 [B30], which requires TLS and secure Manufacturing Message Specification.

9.4.3 System security considerations

9.4.3.1 Passwords, certificates, and other authentication tools

Passwords are the most common method for authenticating human users, but they can be breached by many mechanisms. For instance, most people write down their passwords so they do not forget them. An attacker can find these passwords in a drawer, shoved under a mouse pad, or even stuck on the monitor. Passwords can also be guessed (e.g., a pet's name or a husband's birthday), the keyboard can be "sniffed" by devices or software that capture all key strokes, and poorly designed systems can send a password "in the clear" over an insecure network, where a hacker can eavesdrop.

Certificates can be seen as the software application's equivalent to passwords. A "trusted" entity issues certificates to applications or systems, which can then be used by security mechanisms such as the public key infrastructure to ensure that these entities are who they say they are and that data transferred between them is secured.

9.4.3.2 Security for Web services

Web services could be used for many DR transactions. Security for Web services is being developed by the W3C and the Organization for the Advancement of Structured Information Standards. See the W3C Web site at http://www.w3.org and the Organization for the Advancement of Structured Information Standards Web site at http://www.oasis-open.org.

9.4.3.3 Malicious activities

Examples of malicious activities include the following:

- Viruses and worms
- Spyware
- Trojan horses
- Malicious use of communication maintenance tools
- Insecure memory stick transfers

Annex A

(informative)

Bibliography

[B1] AGA 12, Cryptographically Protected SCADA Communications: Basic recommendations.[10]

[B2] Daconta et al, *The Semantic Web*, Wiley Publishing, 2003.

[B3] EIA RS-232-C, Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Data Interchange.[11]

[B4] EPRI 100174, Communication Security Assessment for the United States Electric Utility Infrastructure.[12]

[B5] EPRI 100898, Scoping Study on Security Processes and Impacts, Final Report, June 2003.

[B6] EPRI 1012160, *IntelliGrid Architecture Report: Volume 1, IntelliGrid User Guidelines and Recommendations*, December 2005.[13]

[B7] EPRI 1012160, *IntelliGrid Architecture Report: Volume IV—Appendix A—Security*.

[B8] FIPS Pub 140-2, 1994 January 11, Security Requirements for Cryptographic Modules.[14]

[B9] Fowler, M. and Scott, K., *UML Distilled: Applying the Standard Object Modeling Language*, Addison-Wesley, 2003.

[B10] IEC 60870-5, Telecontrol Equipment and Systems—Part 5: Transmission Protocols.[15]

[B11] IEC 60870-6, Telecontrol Equipment and Systems—Part 6: Telecontrol Protocols Compatible With ISO Standards and ITU-T Recommendations.

[B12] IEC 61158, Digital Data Communication for Measurement and Control—Fieldbus for use in Industrial Control Systems.

[B13] IEC 61784, Digital Data Communications for Measurement and Control—Part 1: Profile Sets for Continuous and Discrete Manufacturing Relative to Fieldbus Use in Industrial Control Systems.

[B14] IEC 61850, Communication Networks and Systems in Substations.

[B15] IEC 61850-1, Communication Networks and Systems in Substations—Part 1: Introduction and Overview.

[10] AGA 12 is available at http://www.gastechnology.org/webroot/app/xn/xd.aspx?it=enweb&xd=10AbstractPage/050142.xml.

[11] EIA publications are available from Global Engineering Documents, 15 Inverness Way East, Englewood, Colorado 80112, USA (http://global.ihs.com/).

[12] EPRI documents are available from the Electric Power Research Institute, 3420 Hillview Ave, Palo Alto, California 94304, USA (http://www.epri.com/).

[13] The IntelliGrid publications can be accessed via the IntelliGrid website at http://www.IntelliGrid.info.

[14] FIPS publications are available from the National Technical Information Service (NTIS), U. S. Dept. of Commerce, 5285 Port Royal Rd., Springfield, VA 22161 (http://www.ntis.org/).

[15] IEC publications are available from the Sales Department of the International Electrotechnical Commission, Case Postale 131, 3, rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iec.ch/). IEC publications are also available in the United States from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

[B16] IEC 61850-2, Communication Networks and Systems in Substations—Part 2: Glossary.

[B17] IEC 61850-3, Communication Networks and Systems in Substations—Part 3: General Requirements.

[B18] IEC 61850-4, Communication Networks and Systems in Substations—Part 4: System and Project Management.

[B19] IEC 61850-5, Communication Networks and Systems in Substations—Part 5: Communication Requirements for Functions and Device Models.

[B20] IEC 61850-6, Communication Networks and Systems in Substations—Part 6: Configuration Description Language for Communication in Electrical Substations Related to IEDs.

[B21] IEC 61850-7-1, Communication Networks and Systems in Substations—Part 7.1: Basic Communication Structure for Substation and Feeder Equipment—Principles and Models.

[B22] IEC 61850-7-2, Communication Networks and Systems in Substations—Part 7.2: Basic Communication Structure for Substation and Feeder Equipment—Abstract Communication Service Interface.

[B23] IEC 61850-7-3, Communication Networks and Systems in Substations—Part 7.3: Basic Communication Structure for Substation and Feeder Equipment—Common Data Classes

[B24] IEC 61850-7-4, Communication Networks and Systems in Substations—Part 7.4: Basic Communication Structure for Substation and Feeder Equipment—Compatible Logical Node Classes and Data Classes Testing.

[B25] IEC 61850-8, Communication Networks and Systems in Substations—Part 8: Protocol Mapping.

[B26] IEC 61970, Energy Management System Application Program Interface.

[B27] IEC 61970-301, Energy Management System Application Program Interface (EMS-API)—Part 301: Common Information Model (CIM) Base.

[B28] IEC 62351-1, Data and Communication Security—Part 1: Introduction and Overview.

[B29] IEC 62351-3, Data and Communication Security—Part 3: Profiles Including TCP/IP.

[B30] IEC 62351-4, Data and Communication Security—Part 4: Profiles Including MMS.

[B31] IEC 62351-5, Data and Communication Security—Part 5: Security for IEC 60870-5 and Derivatives.

[B32] IEC 62351-6, Data and Communication Security—Part 6: Security for IEC 61850 Profiles.

[B33] IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition, New York, Institute of Electrical and Electronics Engineers Inc.[16]

[B34] IEEE Std 802.11, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area network—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

NOTE—IEEE Std 802.11b, IEEE Std 802.11g, and IEEE Std 802.11i have been incorporated into IEEE Std 802.11.

[16] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08855 USA (http://standards.ieee.org/).

[B35] IEEE P802.11n, Draft Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area network—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 4: Enhancements for Higher Throughput.[17]

[B36] IEEE Std 802.15.1, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs).

[B37] IEEE Std 802.15.4, IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).

[B38] IEEE Std 802.16, IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems.

[B39] IETF RFC 1826, IP Authentication Header.[18]

[B40] IETF RFC 1827, IP Encapsulating Security Payload.

[B41] IETF RFC 2196, Site Security Handbook.

[B42] IETF RFC 2313, PKCS #1: RSA Encryption Version 1.5.

[B43] IETF RFC 2401, Security Architecture for the Internet Protocol.

[B44] IETF RFC 2406, IP Encapsulating Security Payload.

[B45] IETF RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

[B46] IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS).

[B47] IETF RFC 2869, Remote Authentication Dial In User Service Extensions.

[B48] IETF RFC 3268, Advanced Encryption Standard Ciphersuites for Transport Layer Security.

[B49] ISA—The Instrumentation, Systems, and Automation Society SP100, Wireless Systems for Automation.

[B50] ISO/IEC 17799, Information Technology—Security Techniques—Code of Practice for Information Security Management.[19]

[B51] ISO/IEC 18014-1, Information Technology—Security Techniques—Time-Stamping Services—Part 1: Framework.

[B52] ISO 7816 series, Identification cards—Integrated circuit(s) cards with contacts.[20]

[17] Numbers preceded by P are IEEE authorized standards projects that were not approved by the IEEE-SA Standards Board at the time this publication went to press. For information about obtaining drafts, contact the IEEE.
[18] All RFCs are available at http://www.ietf.org/.
[19] ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iso.ch/). ISO/IEC publications are also available in the United States from Global Engineering Documents, 15 Inverness Way East, Englewood, Colorado 80112, USA (http://global.ihs.com/). Electronic copies are available in the United States from the American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).

[B53] ISO 11898 series, Road Vehicles—Controller Area Network (CAN).

[B54] NIST SP 800-12—An Introduction to Computer Security: The NIST Handbook.

[B55] NIST/ITL SP 500-166 Computer Viruses and Related Threats: A Management Guide.

[B56] North American Electric Reliability Council (NERC) CIP 002-009, Cyber Security Standard.

[B57] Organization for the Advancement of Structured Information Standards (OASIS), Security Assertion Markup Language (SAML) V 2.0.[21]

[B58] Quatrani, T., "Visual Modeling with Rational Rose and UML," Addison-Wesley, 1998.

[B59] Rosen, L., *Open Source Licensing*, Prentice Hall, 2005.

[B60] TIA/EIA-485, Electrical Characteristics of Generators and Receivers for Use In Balanced Digital Multipoint Systems.

[B61] UL 1741, Inverters, Converters, Controllers, and Interconnection System Equipment for Use With Distributed Energy Resources. [22]

[20] ISO publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iso.ch/). ISO publications are also available in the United States from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).

[21] This publication is accessible via http://www.oasis-open.org.

[22] UL standards are available from Global Engineering Documents, 15 Inverness Way East, Englewood, Colorado 80112, USA (http://global.ihs.com/).

Annex B

(informative)

Annotated list of protocols

This annex provides a list of protocols, communication media, and power system devices applicable to the MIC of DR.

There have been hundreds, if not thousands, of communications protocols used in and around DR locations. Typically, the communications can be broken into the following categories:

- Local DR equipment intercommunication and monitoring
- DR communication to the facility supported by the DR
- DR communication to external, off-site entities

In most cases, the sophistication of the communication protocols and the ability to use different physical transport (ISO OSI Layer 1) mechanisms increase as one progresses from local DR equipment intercommunication to DR communication to external entities. This means many of the protocols suitable for external communication are also applicable to local intercommunication, but most of the protocols used strictly for equipment intercommunication are not suited for external communication. When hard, predictable, real-time response is necessary, some of the external communication protocols may not work for equipment intercommunication.

Local DR equipment intercommunication and monitoring tends to have the most proprietary protocols of the three categories. Also, because of the longevity of the DR equipment and an “if it isn’t broken, don’t fix it” attitude, many original device intercommunication protocols are still in use. The many protocols in use include the following:

- Pneumatic
- 4–20 ma
- 0–10 V
- 0,12 V discrete (on/off)
- ModBus
- LonWorks
- Caterpillar Data Highway
- Controller area network (CAN)
- DeviceNet
- Many proprietary EIA RS-232- [B3] and TIA/EIA-485-based [B60] protocols
- Many proprietary power line communications protocols

Communicating DR information within the facility hosting and maintaining the DR equipment requires the ability to transport and interpret the data into more business and less industrial communication protocols. Typically these protocols are routable and implement layers 2 through 7 of the ISO OSI model to allow the ability to propagate across multiple physical transport architectures and applications.

The many protocols in use include the following:

- Ethernet
- TCP/IP
- Dynamic Data Exchange (DDE, which is being replaced by OPC in many places)
- Component Object Model /Distributed Component Object Model (COM/DCOM)
- OPC [data access (DA), HD, and alarms and events (AE)]
- LonWorks

To communicate externally requires many of the same features needed to bring the DR information to the host facility but typically requires more attention to security and concerns the ability to convert the data to a protocol acceptable for the available external physical communication connections.

The many protocols in use include the following:

- Ethernet
- TCP/IP
- User Datagram Protocol (UDP)
- DDE (which is being replaced by OPC in many places)
- COM/DCOM
- Common Object Request Broker Architecture (CORBA)
- Remote Method Invocation
- OPC (DA, HD, and AE)
- OPC-DX (data exchange)
- LonWorks
- Modem connection (proprietary)
- Modem connection TCP/IP via point-to-point protocol (PPP)
- Publish/Subscribe protocol

In some instances, communicating to a device externally may not require a routable protocol if obtaining information from a single device is all that is necessary and a modem interface is available. The protocol of the data coming across the modem may be proprietary as well. Because of its wide availability, inexpensive installation, and recurring costs, a simple modem connection using TCP/IP via PPP is very popular. With a device, such as a personal computer, onsite that can gather all of the equipment data into one format, such as OPC, the data can be sent over the modem PPP channel to the external entity. As data throughput requirements increase, broadband connections such as T1, cable, and high-speed satellite become more common. The broadband connections may have the advantage of always being connected over modem connections, which require significant handshaking any time a connection is initiated.

According to the ISO OSI reference model, the communication protocols are organized by seven layers: application, presentation, session, transport, network, data link, and physical (from the top to the bottom). Common usage defines a selection of a protocol at each layer as a "complete" profile. For convenience, pieces of a complete profile have been categorized into three sub-profiles by combining some of the following seven layers:

- A profile—spanning the upper three layers
- T profile—spanning the middle two layers
- L profile—spanning the lower two layers

The protocols in Table B.1 are grouped based on their specified profile types and the type of communications environment for which they are most appropriate (or in which they are commonly used).

Table B.1—Protocols

No.	Typical applications	Profile	Technology	Description	Source	URL
1	Enterprise level—Business-to-business	A Profile	J2EE/EJB	J2EE technology and its component-based model simplify enterprise development and deployment. The J2EE platform manages the infrastructure and supports the Web services to enable development of secure, robust, and interoperable business applications. The J2EE platform is the foundation technology of the Sun ONE platform and Sun's Web services strategy.	Sun	http://java.sun.com/j2ee/
2	Enterprise level—Business-to-business	A Profile	ebXML	ebXML is an eCommerce business-to-business-specific standard that seeks to create a bridge between electronic data interchange and XML. Major parts of ebXML include the Collaboration Protocol Profile and Agreement, messaging, and registry.	United Nations Centre for Trade Facilitation and Electronic Business and Organization for the Advancement of Structured Information Standards	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-iic
3	Enterprise level—Business-to-Business	A Profile	Web Services	A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically Web Service Definition Language). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.	W3C and others	http://www.w3.org/TR/ws-arch/

No.	Typical applications	Profile	Technology	Description	Source	URL
4	Control center to control center	A Profile	IEC 60870-6 [B11] (ICCP)	Also known as TASE.1 and TASE.2, the Telecontrol Application Service Elements 1 and 2 protocols allow for data exchange over wide area networks (WANs) between a utility control center and other control centers, other utilities, power plants, and substations.	IEC TC57 WG7	http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=1186
5	Control center—EMS	A Profile	IEC 61970—Generic Interface Definition [B26]	IEC 61970 [B26] provides standard interface specifications for "plug in" applications for an electric utility power control center EMS or other system performing the same or similar functions. A "plug in" application is defined as software that may be installed on a system with minimal effort and no modification of source code. This standard facilitates installation of the same application program on different platforms by reducing the efforts currently required.	IEC TC57 WG13	http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=1634
6	Control center	A Profile	MultiSpeak	MultiSpeak is a specification for the exchange of data among software applications commonly applied in small electric utilities, such as electric cooperatives. Software providers may use the specification to write interfaces that will enable the interchange of information with other software that supports MultiSpeak. The MultiSpeak Initiative is a collaborative effort of the National Rural Electric Cooperative Association and more than 120 software providers and consultants that serve electric utilities. The initiative was formed to foster the development of cost-effective, interoperable software products for electric utilities.	National Rural Electric Cooperative Association-sponsored	http://www.multispeak.org
7	Remote/external/SCADA	A Profile	COM/DCOM	DCOM is a protocol that enables software components to communicate directly over a network in a reliable, secure, and efficient manner. DCOM is designed for use across multiple network transports, including Internet protocols	Microsoft	http://www.microsoft.com/com/tech/DCOM.asp

No.	Typical applications	Profile	Technology	Description	Source	URL
				such as HTTP. DCOM is based on the Open Software Foundation's Distributed Computing Environment-Remote Procedure Call spec and will work with both Java applets and ActiveX components through its use of the COM.		
8	Remote/external/SCADA	A Profile	CORBA	CORBA is an architecture and specification for creating, distributing, and managing distributed program objects in a network. It allows programs at different locations and developed by different vendors to communicate in a network through an "interface broker." CORBA was developed under the auspices of the Object Management Group and has been sanctioned by both ISO and X/Open as the standard architecture for distributed objects (also known as components). Recently, the Object Management Group added real-time CORBA extensions and the minimum CORBA profile for embedded systems.	Object Management Group	http://www.omg.org/technology/documents/formal/corba_iiop.htm
9	Remote/external/SCADA	A Profile	Remote Method Invocation	Remote Method Invocation is a set of protocols that enable Java objects to communicate remotely with other Java objects. Remote Method Invocation is a relatively simple protocol. But unlike more complex protocols such as CORBA and DCOM, it works only with Java objects. CORBA and DCOM are designed to support objects created in any language.	Sun	http://java.sun.com/products/jdk/rmi/
10	Remote/external/SCADA COM/DCOM-based	A Profile	OPC [DA, historic data access (HDA), and AE]	OPC is open connectivity in industrial automation and the enterprise systems that support industry. Interoperability is assured through the creation and maintenance of open standards specifications. There are currently seven standards specifications completed or in development. Earlier versions of OPC specifications such as DA (data access), HDA and AE are based on the Microsoft	OPC Foundation	http://www.opcfoundation.org

No.	Typical applications	Profile	Technology	Description	Source	URL
				COM/DCOM platform. The newer release of OPC incorporated XML technology.		
11	Remote/external/SCADA XML-based	A Profile	OPC-DX	OPC-DX provides server-to-server communications across Ethernet fieldbus networks. It also adds remote configuration, diagnostic, monitoring, and management capabilities.	OPC Foundation	http://www.opcfoundation.org
12	Remote/external/SCADA older and not currently supported by MS	A Profile	DDE	DDE is an inter-process communication technology. DDE enables two running applications to share the same data. Although the DDE mechanism is still used by many applications, it is being supplanted by Object Linking and Embedding, which provides greater control over shared data.	Microsoft	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ipc/base/interprocess_communications.asp
13	Remote/external/SCADA	T Profile	TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP), originally developed by the Defense Advanced Research Projects Agency, is a suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. TCP/IP protocols map to a four-layer conceptual model known as the Defense Advanced Research Projects Agency model. The four layers of the model are: application, transport, internet, and network interface. Each layer in the model corresponds to one or more layers of the seven-layer OSI model.	Defense Advanced Research Projects Agency	http://www.faqs.org/rfcs/rfc768.html
14	Remote/external/SCADA	T Profile	UDP/IP	UDP is a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over	W3C/American National Standards Institute	

No.	Typical applications	Profile	Technology	Description	Source	URL
				a network.		
15	Monitoring and control to and within substations	A Profile	IEC 61850 [B14] (Utility Communications Architecture v2)	IEC TC57 Working Group 10 focuses on communications. The initial specifications focused on a "top down" approach, characterizing the interactions between substation components at a requirements level: · 61850-1 Introduction and Overview [B15] · 61850-2 Glossary [B16] · 61850-3 General Requirements [B17] · 61850-4 System and Product Management [B18] · 61850-5 Communications Requirements [B19]. WG 10 also has within its scope the task of developing a standard file format for exchanging information between proprietary configuration tools for substation devices. This standard is based on (XML) and draws on the data modeling concepts found in the other parts of IEC 61850 and the capability of the IEC 61850 protocols to "self-describe" the data to be reported by a particular device. IE C 61850-6 Substation Configuration Language [B20]: At about the time when the requirements parts of the work were approaching completion, WGs 10–12 became aware of the work that the Electrical Power Research Institute and the Utility Communications Architecture Forum had completed on Utility Communications Architecture, especially on a standard set of services and data models for intra-substation communications. This work was incorporated into IEC 61850 [B14] with some significant modifications in the following specifications:	IEC TC57 WG 10–12	http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=dirwg.p&ctnum=1188

No.	Typical applications	Profile	Technology	Description	Source	URL
				· 61850-7-1 Principles and Models [B21] · 61850-7-2 Abstract Communications Service Interface [B22] · 61850-7-3 Common Data Classes (Object Models) [B23] · 61850-7-4 Compatible Logical Node Classes and Data Classes (Object Models) [B24] Most of the IEC 61850 specifications describe the protocol in a very abstract manner, and only the last parts of the standard describe "specific communication service mapping" onto a particular set of protocols. The initial protocol profiles for IEC 61850 [B14] are using the Manufacturing Message Specification and both Internet and OSI protocol stacks. These are mainly full seven-layer profiles, but there are also high-speed profiles used directly over Ethernet (IEEE 802.x) local area networks (LANs) for "process bus" and protection tripping. The profiles are described in IEC 61850-8 [B25] Protocol Mapping. The initial intent was that IEC 61850 [B14] would be a superset of Utility Communications Architecture 2.0 and that devices implementing the two protocol suites could interoperate. Another significant contribution of IEC 61850 [B14] is a high-speed Ethernet-based protocol to be used for communications between "smart transformers" and higher-level devices to permit several different devices to simultaneously receive sampled waveform values from a given transformer in real-time:		

No.	Typical applications	Profile	Technology	Description	Source	URL
				· 61850-9 Sampled Measured Values Parts 7.1, 7.2, 7.3, 7.4, and 9.1 of IEC 61850 have become International Standards with the remaining protocol pieces reaching International Standard status in 2003 to early 2004. The final work in IEC 61850 will be to develop test procedures for verifying conformance to the protocol: · 61850-10 Certification Test Procedures		
16	Monitoring and control to and within substations	A Profile	DNP3	DNP was developed as a three-layer asynchronous protocol suitable for use on slow serial links and radios, so like IEC 60870-5 [B10]], it is strongly focused on compactness, data integrity, and reliability in noisy environments. It incorporates the best features of the many proprietary protocols that preceded it, such as select-before-operate and direct controls, accurately time-stamped data, broadcasting, freezing accumulators, scan groups, and report-by-exception. It also supports features that were very advanced for the time it was created, including spontaneous reporting, multiple masters, peer-to-peer communications, floating-point data, wild-card requests, file transfer, limited self-description, and vendor-extension. In 2000, the DNP Technical Committee defined a specification for carrying DNP3 over TCP/IP and UDP/IP. Because the WAN/LAN version is essentially the serial DNP3 encapsulated, this makes it possible to connect serial DNP3 devices to WAN/LAN DNP3 devices using terminal servers, IP packet radios, cellular digital packet data modems, and other networking technologies without requiring the access devices to have knowledge of DNP3. DNP3 is often	DNP Users Group	http://www.dnp.org/

No.	Typical applications	Profile	Technology	Description	Source	URL
				referred to as a SCADA protocol, but it was intended for use in all areas of utility communications. The DNP Technical Committee continues to add features to the protocol, with a mandate of maintaining backward compatibility with existing devices. Recent additions include double-bit status inputs and "attribute" objects that aid in self-description of the device. The committee is working on an XML schema for description of a DNP3 implementation and network security features for authentication and encryption. DNP3 Serial may use the same security technologies as those being developed by IEC TC57 WG15 for IEC 60870-5 Part 101 [B10]. DNP3 WAN/LAN may use the same security technologies as those being developed by IEC TC57 WG15 for IEC 60870-5 Part 104 [B10].		
17	Monitoring and control to and within substations	A Profile	IEC 60870-5 [B10]	IEC 60870-5 Part 101—Serial Telecontrol Protocol [B10] was developed by IEC TC57 in WG03 as a three-layer communications protocol standard for use by utilities for SCADA. It was designed primarily to meet the needs of real-time exchange of data between compute-constrained devices over media-constrained communication channels (typically less than 1200 bps). This protocol is widely used in Europe and other countries but is not typically used within the United States or Canada. In these two counties, a variation of IEC 60870-5 Part 101 [B10] was developed, called DNP. IEC 60870-5 Part 104—Telecontrol	IEC TC57 WG3	http://trianglemicroworks.com/mailman/listinfo/iec60870-5_trianglemicroworks.com

No.	Typical applications	Profile	Technology	Description	Source	URL
				Protocol over TCP/IP [B10] was developed by IEC TC57 in WG03 as an international standard, by placing IEC 60870-5 Part 101 [B10] over the TCP/IP Protocol stack. This permits networking of the communications for monitoring and controlling field devices through SCADA. This has made it less useful for compute-constrained devices and media-constrained communications but has made it significantly more useful for less constrained environments. It is equivalent to DNP when it runs over the TCP/IP.		
18	Local facility—within substation	A Profile	ModBus	ModBus protocol is a messaging structure developed by Modicon in 1979 that is used to establish master-slave/client-server communication between intelligent devices. It is a de facto standard and a widely used network protocol in the industrial manufacturing environment. It is implemented by hundreds of vendors on thousands of devices to transfer discrete/analog I/O and register data between control devices. In the power industry, it is used predominantly within substations. Modbus TCP/IP is an open specification developed in 1999 to provide a networking version of ModBus. ModBus Plus is a protocol that uses a Token Ring network topology with a physical access based on a transmission speed to 1 Mb/s. The Modbus Plus protocol uses ModBus messaging for the application layer and the High Level Data Link Control protocol for the network layer.	Modicon	http://www.modbus.org/default.htm
19	Local facility - within substation	L Profile	ProfiBus	The non-profit PROFIBUS User Organization, as a part of the worldwide organization PROFIBUS International, promotes and maintains a set of extremely popular specifications for local-area “bus” communications in	Siemens	http://www.profibus.org/

No.	Typical applications	Profile	Technology	Description	Source	URL
				industrial and process automation. PROFIBUS is also frequently used in power systems devices. The current PROFIBUS is actually PROFIBUS Decentralized Periphery, which replaces an earlier PROFIBUS Fieldbus Message Specification. PROFIBUS Fieldbus Message Specification resembled the current IEC 61850 [B14] profile, while DP is a more compact protocol suite. The core of PROFIBUS Decentralized Periphery is a data link layer that is simultaneously token-passing (between master devices) and polled (from masters to slaves), enabling deterministic bus access with high bandwidth utilization. The data link layer comes in several options and operates over a variety of physical layers. It is usually implemented in hardware. The approved physical media include RS485 [B60], RS485-IS, Manchester-Coded Bus Powered, and fiber optics, at rates from 9600 bps to 12 Mbps. To aid in interoperability, the PROFIBUS User Organization has defined several application layer profiles dedicated to specific uses such as factory automation, process automation, and motion control. PROFIBUS is listed among several "field buses" conforming to IEC 61158 [B12]: "Digital Data Communication for Measurement and Control—Fieldbus for use in Industrial Control Systems" and IEC 61784 [B13]: "Profile Sets for Continuous and Discrete Manufacturing Relative to Fieldbus Use in Industrial Control Systems." Access to PROFIBUS networks and data from IP-based Ethernet networks is achieved through PROFInet gateways,		

No.	Typical applications	Profile	Technology	Description	Source	URL
				which use an object-oriented application layer using DCOM and XML over TCP/IP.		
20	Local facility—Power line communications	L Profile	Ethernet Global Data		General Electric Company	
21	Local facility—Process control	L Profile	FieldBus	The non-profit Fieldbus Foundation promotes and maintains a popular local-area "bus" communications specification for use in industrial automation, particularly in instrumentation and control. This specification is known as "Foundation Fieldbus" and is distinguished from the generic term "fieldbus," which may apply to several different technologies. Foundation Fieldbus is a three-layer protocol suite plus object model specifications, known as "function blocks," defined above the application layer. It includes self-description in the form of "device description" files that use a standard (non-XML) language specific to Foundation Fieldbus. The data link layer is listed among several technologies complying to IEC 61158 [B12]: Digital Data Communication for Measurement and Control—Fieldbus for Use in Industrial Control Systems. The data link layer uses a "deterministic bus scheduler" to control access to the bus using token passing. The application layer, the Fieldbus Message Specification uses a publish/subscribe model and resembles the Manufacturing Message Specification that is the core of IEC 61850 [B14]]. The standard Foundation Fieldbus physical layer is a multi-drop 31.25-Kbps, "intrinsically safe" physical layer	FieldBus Foundation	http://www.fieldbus.org/

No.	Typical applications	Profile	Technology	Description	Source	URL
				known as H1. H1 networks may be accessed from Ethernet networks through a "linking device" using a "high-speed Ethernet" profile that includes TCP/IP, UDP/IP and Simple Network Management Protocol, or devices may support only high-speed Ethernet. The high-speed Ethernet specification pays special attention to redundancy in Ethernet LANs.		
22	Local facility — out of use but might still be seen	L Profile	DECnet		DEC	
23	Local equipment	L Profile	CAN	CAN is a ubiquitous protocol devised for monitoring and control in automotive applications. However, because of its small footprint and other technical attributes, it has found applications in many areas requiring interaction between sensors and controls. Virtually every manufacturer of embedded micro controllers provides devices with built-in CAN interfaces. In this regard, it is probably only second in commonality to a universal asynchronous receiver-transmitter and I2C as a means of device communications. CAN has also been standardized as ISO 11898 [B53].	CAN-CIA	http://www.can-cia.de/can/
24	Local equipment—CAN-based	L Profile	DeviceNet	DeviceNet is similar to CAN. It is a simple, networking solution for factory automation devices and provides interchangeability of "like" components from multiple vendors. DeviceNet specifications have been developed by the Open DeviceNet Vendor Association and are internationally standardized.	Open DeviceNet Vendor Association	http://www.odva.org/index.htm
25	Local equipment monitoring		Harley LTC-Map			
26	Local equipment		Caterpillar Data Highway		Caterpillar	
27	Building automation	A Profile	BacNet		BACnet Manufacturer	

No.	Typical applications	Profile	Technology	Description	Source	URL
					s Association	
28	Building automation	A Profile	CEBus		Consumer Electronics Association	
29	Building automation—Other	A Profile	LonWorks		Echelon	
30	Gas industry	A Profile	AGA Gas Flow		AGA	
31	Cross domains—Network management	A Profile	Simple Network Management Protocol		Internet Engineering Task Force	
32	Cross domains—Network management	A Profile	CMIP		ISO	
33	Cross domains—Time synchronization	L Profile	IRIG-B			
34	Cross domains—Time synchronization	L Profile	Rugby Clock			

Annex C

(informative)

Open systems

C.1 Open systems

a) Open systems are based on open standards and open formats.

b) Open standards are standards published under terms and conditions that allow anyone who acquires a copy to use or implement the standard without limitation or further obligation to the originator of the standard. The major exception involves conditions intended to protect the integrity of the standard and ensure conformance by claimed implementations. Open standards are often produced by voluntary consensus standards-developing organizations. IEEE is an example of a standards-developing organization whose processes conform to voluntary consensus requirements. Sometimes, open standards are developed and their provisions controlled under proprietary conditions, but they are openly published and their originator allows unlimited implementation. An example is the portable document format. Many open standards are sold for the cost of translation, publication, and other services provided by the standards-developing organization with provisions of copyright law being enforced the same as for printed books and periodicals. Many others are freely downloadable and redistributable over the Internet, with provisions of copyright law being enforced primarily to maintain integrity of the content. Many open standards also are accompanied by reference implementations licensed under open source terms. Some standards-developing organizations require a reference implementation to accompany the text of a standard to help resolve uncertainties in provisions and provide a basis for conformance tests. (Actually, development of the reference implementation often precedes the text of the standard and effectively serves to formally specify performance of the reference implementation. This has been a common historic practice in Internet standards and a major contribution to the success of the Internet.)

c) Open formats are open standards covering file and other data exchange formats. These can be freely implemented in open source or proprietary implementations and foster interoperable exchange of files and data between those implementations.

C.1.1 History

The ISO looked to create a simple model for networking, the OSI model. It took the approach of defining layers that rest in a stack formation, one layer upon the other. Each layer would have a specific function and deal with a specific task. Much time was spent to create the model, called The ISO OSI Seven-Layer Model for Networking. The model has seven layers, and each layer has a special and specific function. Current network communication standards evolved from these first efforts. Figure C.1 is a graphical representation of the ISO OSI seven-layer model for network communications.

Ethernet is an implementation for the physical and data link layers of the OSI model. EIA RS 232 [B3] and similar wiring standards are examples of physical layer standards. Some vendors have tried to defeat the purpose of the standard over the years because they believed that supplying proprietary solutions might result in higher performance, higher profits, or improved security. The current ubiquity of the Internet owes much of its success to these early models.

The move to “open source” as the model for openness came out of the UNIX community and defines a new benchmark. Many do not consider any standard as truly open unless all the sources are open and available without royalty. The Open Source Foundation works to maintain this level of open standards for UNIX.

C.1.2 Problem

End users today look to standards to solve a number of problems that translate into real or perceived cost, complexity, performance, or timeliness differences. Users look to standards to improve interoperability (so they do not get locked into a single vendor) and extensibility (so they can grow their solution as their application grows), competition (so they can control costs) and to mitigate consequences of obsolescence by allowing a migration path over time. These goals require that the solutions implemented adhere to the standard in quite rigorous ways, or the unintended consequences may outweigh the anticipated benefits.

Understanding the seven-layer model immediately begs the question "What does 'open' mean?" Some alternatives may be open at one of the seven layers but fully proprietary at the other six. Is that open? Only the end user can decide at what layer he or she requires "open."

C.1.3 Issues

Standards can be either de facto or de jure. De facto standards emerge from the marketplace and may be endorsed by an accredited standards body. Examples of de facto standards include Ethernet, Bluetooth, and Adobe Portable Document Format. De jure standards are defined with rigor by an accredited standards body and are usually available, for a nominal fee, from that body. They can be implemented by anyone and may have a certification procedure available.

The marketplace does not always ensure that the "best" technology becomes standard in any particular application. The argument about which is "better" misses the point of why standards are developed.

The frustration with the time it takes to get a standard approved by an accredited standards body has caused many organizations to pursue their own approaches with hopes that theirs will become the accepted standard eventually. This can be a big risk, but it also has a potentially high payoff.

C.1.4 Alternatives

Most currently available communications products adhere to the ISO OSI seven-layer model at one or more of the layer interfaces but not at all of them. The key to determining the appropriate solution for an application today hinges on where the application needs the extensibility, interoperability, competition, and protection against obsolescence. Once the layer where standardization is required is identified, the user can peruse the available solutions that meet the standards at the layer (or layers) required. Ideally, a standard solution would provide an open interface between each of the seven layers. Then alternate vendor solutions would plug and play at any one of the layers.

Most vendors claim open solutions if they are open at the physical layer (Ethernet) or perhaps the data link or network layers (TCP/IP). Application layer standards (XML) are also available, but the user cannot replace the modules underneath without extensive modification to the existing infrastructure. The key is to find products that define open interfaces in as many layers (of the seven) as possible while still meeting the other requirements for performance and cost.

C.1.5 Metrics

Metrics used to measure the degree of "openness" include initial cost, cost to extend/expand, time to extend/expand, perceived complexity, and market share. A standard that has little or no market share has little potential to make an impact. Some major companies are finding that they can provide open solutions to the marketplace more competitively than proprietary solutions because their own employees are now more productive. This could improve the landscape for open solutions in the marketplace.

C.1.6 Solution

Solutions available today are limited by perceived profitability by the suppliers. Many are convinced that proprietary products are cheaper, faster, and better. End users "voting with their feet" and moving toward open solutions will cause suppliers to rethink their positions. If open solutions are unavailable for a particular application, the end user can isolate that part of the solution and plan to upgrade to standards-based solutions when they become available. Future implementations, based on open standards, are becoming more cost-effective as Moore's Law begins to affect the measurement and control markets. Open standards permit the volumes of production necessary to begin seeing the economies of scale necessary for true Moore's Law solutions to emerge.

Many alternatives available today contain traps because no migration path is available once begun. Such solutions may look attractive at first, but without a path to an open architecture solution, options become cost-prohibitive and competitiveness with other suppliers becomes more difficult. The future in communications will play out along the ISO OSI seven-layer model (see Figure C.1). Open systems will provide the ubiquity required for cost, performance, and flexibility needed in distributed applications such as the power grid. Ultimately, the organizations that move toward the more open alternatives will have the most options and be the most flexible in responding to the marketplace.

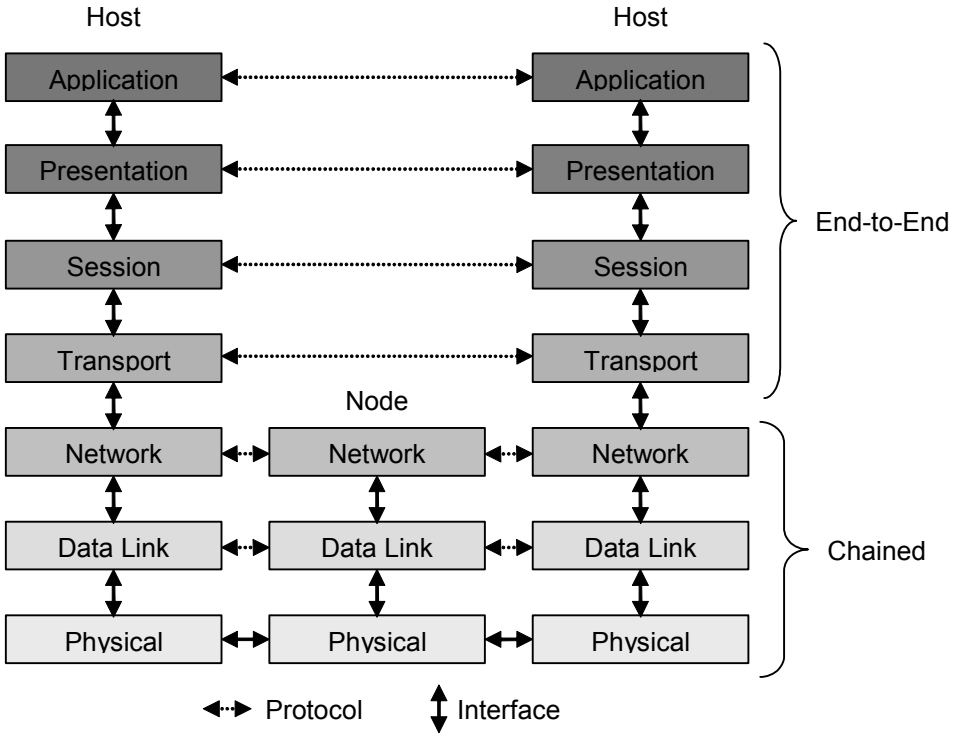


Figure C.1—ISO OSI seven-layer model (an open interface is defined between each layer)

C.2 Open source

Open source is one of two names that apply to a broad concept for licensing software. The other name is free software (in Europe called "libre software"). The free software concept was first promulgated and is championed by the Free Software Foundation (www.gnu.org) and is embodied in its primary license, the GNU General Public License (GPL). The Open Source Initiative (www.opensource.org) was later formed. It defined the term "open source" as an alternative to free software to avoid misinterpretations that arise between meanings of the word "free." (These are often summarized by the Free Software Foundation as "free as in speech, not as in beer" and can also be differentiated as "libre" versus "gratis," as in Europe.) The Open Source Initiative also certifies licenses relaxing the GPL's requirements and publicizes business cases for free and open-source software.

In all open source licenses, the copyright holder conveys to the recipient of the software the rights to use, copy, modify, and redistribute the software in both binary and source code forms and to create and distribute derivative works, all without payment of a license fee or requirement of any further permission. All such licenses disclaim warranties and damages arising from exercise of those rights.

Lawrence Rosen, in his book *Open Source Licensing* [B59] identifies two kinds of open source licenses—academic and reciprocal. The academic licenses place few obligations on recipients, mainly a requirement to maintain copyright notices on redistribution and often some form of restriction on using the name or trademarks of the provider in advertising. There is no barrier to a recipient of academically licensed software distributing either the original software or derivative works under a proprietary license in binary form only.

The reciprocal licenses place more extensive obligations on recipients, mainly some form of requirement that recipients convey to further recipients of redistributed software or derivative works the same rights as they originally received, often using the same license. The GPL is most restrictive in this regard and defines derivative works as "any work that you distribute or publish, that in whole or in part contains or is derived from the [GPL-licensed] Program or any part thereof" and requires them to be "licensed as a whole" under the GPL. There are some exceptions, primarily "identifiable sections of [a]work [that] are not derived from the [GPL-licensed] Program, and can be reasonably considered independent and separate works in themselves."

There are extensively detailed discussions, mainly from a technical perspective, interpreting how to determine that a work is independent and separate and is distributed as a separate work. In general, if a program communicates with a GPL-licensed program by means ordinarily used for communication between separate programs (such as using inter-process communication protocols), the works are to be treated as separate.

Most other reciprocal licenses are less demanding and require only that changes to the work itself be redistributed freely but not bring in other works that may be integrated with the licensed work. These include a license called the Lesser GPL, also promulgated by the Free Software Foundation, and are especially intended to allow licensing of function libraries without extending reciprocity to the using application programs.

Free/open source software is not the same as so-called "freeware" that is provided without charge (gratis) in binary form and may be freely redistributable. Such software does not convey the rights or capabilities for recipients to develop modifications or derivative works. Such rights are at the core of the free and open source software concepts. Free/open source software is also not in the "public domain." It is copyrighted work placed by its originators into what Lawrence Lessig calls an "innovation commons."

Annex D

(informative)

Introduction to business process concepts

UML was developed to provide the abstract modeling needed to ensure top-down understanding of the entire system and to provide mechanisms for translating those abstract models into actual computer code. UML is used to capture requirements, designs, and implementation issues associated with software and information system design. Because this guide does not attempt to prescribe specific designs or implementations, only a sub-set of the UML tools and terminology are needed to document the business process interactions and information modeling.

D.1 Business process modeling in UML

One of the key business process modeling concepts is abstraction. Abstraction is the ability to describe real things in terms of their characteristics, attributes, and relationships and interactions with other things. For example, when one describes a car, he or she notes that it has four tires, an engine, and a body and that it runs on fuel, has an owner, and so on. Abstraction allows one to generalize, to describe many types of cars, or to classify and describe specific types of cars (e.g., sports cars, vans, or sedans). By capturing the relevant abstract characteristics of a thing, one can focus on appropriate details while ignoring others. This is important for effectively communicating ideas and gaining insight. Modeling provides the ability to abstract from the large volume of characteristics about real-world things to develop a focused, coherent description relevant to the problem at hand.

Software engineering experience has taught some important techniques in modeling, including the following:

- Abstract characteristics of a model need to be associated with real things.
- Complex systems need to be analyzed and described from different views. A small set of nearly independent views of a model is ideal.
- Models may be expressed at different levels, ranging from highly abstract to the concrete. By abstracting to higher levels, more common characteristics about things can be described. This enforces consistency in dealing with like aspects in the model. It is called normalization.

The key UML modeling construct to capture the business process modeling is the use case.

D.2 Use cases

Use cases are modeling constructs that focus on the interactions between the system and the users of the system, known as “actors.” A use case captures the functionality provided by the system as it relates to the actors. Actors represent anyone or anything that interacts with the system. As such, actors are not necessarily humans. For instance, the DR operator is an Actor when it requests a DR unit to turn on. Similarly, a distribution system relay is an Actor when it signals an isolation breaker system to disconnect a DR unit from the distribution system.

Use cases are layered or iterative in concept. For instance, at a high level, a use case can represent a group of functions interacting with various actors. At a more detailed level, individual use cases can be defined to describe each function in the group. As an example, in one use case, the function “Aggregation of DR for Ancillary Services” could be defined as a single entity, while this use case could be expanded into separate use cases describing individual ancillary services (such as non-spinning reserve and voltage support) as separate entities.

Therefore, the scope of a particular use case is a function of how one wishes to organize the various capabilities in question. Often, use cases are used first to define the overall business processes and then to take each function within this overall set and drill down to more detailed levels. In this way, use cases are powerful for organizing functions.

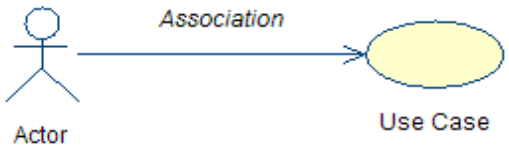


Figure D.1—Use case diagram

Modeling implies diagrams. Use case diagrams consist of actors (represented as little stick people) and use cases (ovals) linked by lines that indicate relationships. (See Figure D.1.) These relationships are termed "associations." An association, which is represented as a line with one or two arrows, provides a pathway for interaction. The interaction can be between any combination of use cases and actors.

Some benefits of use cases are listed as follows:

- They encourage the visualization of processes and interactions that otherwise might be obscure or lost in the complexity of a system.
- They capture requirements from a user's perspective.
- Users are involved in providing requirements and can understand and validate the interactions.
- They identify information that will be exchanged among the functions and actors.
- They are a way to estimate the percentage of requirements captured.
- They categorize functions and show where each affects the others.
- They provide a better way of estimating the percentage of requirements completed during development.
- Test plans can be generated based on use cases.

Use cases are beneficial for the following additional aspects of software development beyond those discussed in this guide:

- They help technical writers structure the overall work on users manuals at an early stage.
- They provide better traceability throughout the system development process.
- They improve the quality of the software by identifying the exception scenarios earlier in the development process.

Annex E

(informative)

Use case template

Use case name: Provide the name of the use case.

Description: Describe briefly the scope and objectives of the use case.

Narrative: Create a walkthrough of the scenario from a domain expert's point of view. This describes what occurs in which order, why, and under what conditions. This acts as the basis for identifying the steps in the section number sequence.

Actors: List the actors (stakeholder roles) involved in the use case (e.g., DR operator, AEPSO, DR aggregator, and DR maintainer).

Name	Role description
Actor 1	Provide a brief description of the role that an Actor/stakeholder has in this particular use case. An Actor can be a human or a system. The same Actor can play different roles in different use cases but only one role in one use case. If the same Actor does play multiple roles in one use case, list these separately.
Actor 2	

Participating systems: List the devices, control equipment, and other systems involved in the use case (e.g., DR device, DR controller, and isolation switch).

System	Services provided
System 1	Provide a brief description or list of services provided by this system in the context of this use case. A system can be a computer system, a set of applications, or manual procedures.
System 2	

Assumptions/design considerations: State any known assumptions, limitations, constraints, or variations that may affect this use case. Consider the following:

- Regulations, policies, financial considerations, and physical constraints
- Performance and timing requirements
- Frequency of use
- Sizing, configuration of equipment and systems, numbers of devices, and volume characteristics
- Security needs

Pre-conditions: Describe conditions that exist prior to the initiation of the use case, such as the state of the actors and systems.

Normal sequence: Describe the normal sequence of events, and focus on steps that identify new types of interactions, new information, or new issues to address. Should the sequence require detailed steps that are also used by other functions, consider creating a new "sub" function and then referring to that "sub-routine" in this function.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	Triggering event	What actor or system is sending to what other actor or system	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.	Identify the information that will be exchanged. Indicate special conditions such as accuracy, security, and availability requirements.	Describe the response to the action in present tense form as for the "Actor action." "If…Then…Else" scenarios can be captured as multiple responses or as separate steps.
2.					
3.					
4.					

Alternative/exception sequences: Describe any alternative or exception sequences that may be required that deviate from the normal course of activities.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.					
2.					
3.					
4.					

Post-conditions: Describe conditions that should exist at the conclusion of the use case.

References: List other use cases referenced by this use case, "sub" use cases, or other documentation that clarifies the requirements or activities described.

Issues: As the use case is developed, identify issues that need clarification, resolution, or other notice taken of them. This can act as an action item list.

ID	Description	Status

Revision history:

No	Date	Author	Description
0.			

Diagram: For clarification, draw (using UML diagram conventions, as appropriate) the interactions described above and identify the steps where possible.

Annex F

(informative)

Sample use cases

The following collection of use cases represents a sample of the uses of DR integrated with the EPS and their corresponding information exchange interactions. A summary of the contents is listed in Table F.1.

Table F.1—Summary of use cases

Use case	Description
DR unit dispatch	The DR operator dispatches a single DR unit for parallel operation with the area EPS and coordinates with the AEPSO for economic energy (but no ancillary services) for shaving peak. This is a diesel generating unit that requires environmental monitoring.
DR unit dispatch for energy export	The DR operator of a single-unit 1.1-MW wind turbine intends to operate as an independent power producer. The DR operator will dispatch his DR unit with the intention of selling energy back to the owner of the area EPS.
DR unit scheduling	The DR operator creates, edits, and deletes schedules to dispatch commands to a DR unit. The DR operator's system communicates the scheduled operation to the DR controller, who invokes commands to the DR unit at appropriate times and notifies the DR operator of status.
DR aggregation	The DR operator dispatches multiple DR units during peak periods of energy use per information (e.g., real-time pricing, dispatch request, or interruptible rate) provided by the DR aggregator and coordinated with the AEPSO. The DR aggregator monitors net metering information from the site.
DR maintenance	The DR owner contracts with a DR maintainer to periodically service a DR unit and perform emergency repairs. The DR maintainer monitors key performance indicators and coordinates with the DR operator when service is required.
DR ancillary services	The DR may be used to provide any or all of the following ancillary services: load regulation, energy losses, spinning and non-spinning reserve, voltage regulation, and reactive supply.
DR providing reactive supply	The DR unit may provide reactive supply by absorbing VARs or producing VARs by changing the field current to match a pre-established schedule. Alternatively, a stated power factor on the high side of the interconnection transformer or PCC can be established.

F.1 IEEE Std 1547.3 Use case: DR unit dispatch

Use case name: DR unit dispatch

Description: The DR operator dispatches a single DR unit for parallel operation with the area EPS and coordinates with the AEPSO for economic energy (but no ancillary services) for the area EPS to shave peak on a distribution feeder. This is a diesel generating unit that requires environmental monitoring.

Narrative: The distribution system is experiencing high demand on a feeder that is approaching its capacity limit. DR is known to be in the region to help alleviate the problem. The AEPSO calls the DR operator to schedule dispatch of the unit at the top of the hour to alleviate the problem. The DR operator checks the contract terms of use and the status of the DR unit and, seeing that it is available for use, initiates start-up for the unit. The DR controller receives the information to start the unit, starts it, synchronizes it with the EPS, and reports the monitored information. After peak conditions subside (or after a previously agreed-upon period), the AEPSO informs the DR operator that the unit is no longer needed. The DR operator initiates shutdown of the unit. The DR controller receives the shutdown information, shuts down the unit, and reports back when it is successfully completed.

Actors:

Name	Role description
DR operator	Person responsible for instructing the operations of the DR unit
Area EPS Operator (AEPSO)	Person responsible for the safe and reliable operation of the distribution system (area EPS) to which the DR site is connected

Participating systems:

System	Services provided
DR controller	Performs communications services between the DR installation site and the outside world
DR unit	The generation or storage device providing electric energy

Assumptions/design considerations:

- The DR unit capacity is significantly less than the local EPS load, so there is no energy back feed into the area EPS.
- Contract arrangements have been made with the DR operator to pay a fee for being on call and having the DR available for distribution system support.
- The AEPSO communicates with the DR operator to request the DR to run. The form of communication (e.g., a phone call or e-mail) is not important, but they are not within the same organization.
- The AEPSO has measuring equipment to verify operation and the amount of energy involved from the system perspective.
- The DR unit is to be operational within 10 min from the time that DR operator is informed. (AEPSOs need to be assured that this sort of response can be met.)
- The DR unit is operated at a standard capacity setting (e.g., on or off, without remote set point adjustment).
- This situation occurs occasionally, and the unit runs for about 1–4 h.
- The DR unit is big enough to satisfy IEEE Std 1547.
- The DR controller runs the DR unit in voltage-following mode.
- The communication between DR operator and the DR controller is secure from non-authorized parties.

Pre-conditions:

The distribution system is experiencing high demand on a feeder that is approaching its capacity limit. DR is known to be in the region to help alleviate the problem. The DR is not presently operating but is available for dispatch.

Normal sequence:

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	Peak condition occurs	AEPSO informs DR operator energy is needed	AEPSO contacts (e.g., calls, e-mails, or alarms) the DR operator that energy from the particular site is needed at the top of the hour for 4 hours.	The DR controller identifier, location, and request for energy	DR operator confirms request and initiates DR unit start-up
2.	Request to start	DR operator to DR controller	At the top of the hour, the DR operator initiates the start command, which is sent to the DR controller for implementation at the DR site.	DR controller identifier, time stamp, and start command	Start command communicated to the appropriate DR controller, which starts the DR unit
3.	Start received	DR controller to DR operator	The DR controller acknowledges the start signal is received and starts the DR unit.	DR controller identifier, timestamp, and start signal acknowledgement	DR operator records acknowledgement
4.	DR unit started	DR controller to DR operator and AEPSO	The DR unit starts and synchronizes with the area EPS. The DR controller confirms the DR unit is started (by measurement or signal) and reports success and current operating measurements.	DR controller identifier, DR operator and AEPSO addresses, DR unit on signal, timestamp At point of DR unit connection: real power output, reactive power output, and voltage At PCC: area EPS connection status, voltage magnitude, frequency, phase rotation, phase angle For environmental monitoring: SO_2, particulate matter, NO_X, CO_2	DR operator and AEPSO witness and record information received The AEPSO may independently meter the energy change at the PCC.
5.	DR unit operational	DR controller to DR operator and AEPSO	Periodically, the DR controller sends operational information.	DR controller identifier, DR operator and AEPSO addresses, timestamp, and operational parameters in Step 4	DR operator and AEPSO witness and record information received
6.	Peak conditions subside	AEPSO to DR operator	The AEPSO contacts the DR operator that energy from a particular site is no longer needed.	DR controller identifier, timestamp, and suspension of request for energy	DR operator confirms request and initiates DR shutdown
7.	Request to stop	DR operator to DR controller	The DR operator sends a stop command to the DR controller for implementation at the DR site.	DR controller identifier, timestamp, and stop command.	Stop command communicated to the appropriate DR controller, which stops the DR unit

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
8.	Stop received	DR controller to DR operator	DR controller acknowledges the stop signal is received and stops the DR unit.	DR controller identifier, timestamp, and stop signal acknowledgement	DR operator records acknowledgement
9.	DR unit shutdown	DR controller to DR operator and AEPSO	The DR unit stops and disconnects from the area EPS. The DR controller confirms the DR unit is stopped (by measurement or signal) and reports success and current operating measurements.	DR controller identifier, timestamp, stop acknowledged, and area EPS connection status. At point of DR unit connection: real power output, reactive power output, and voltage	DR operator and AEPSO witness and record information received The AEPSO may independently meter the energy change at the PCC.

Alternative/exception sequences:

Alternative A: The DR controller may allow the DR operator to specify a power output set point. The remaining steps are unchanged from the normal sequence.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
2.	Request to start	DR operator to DR controller	At the top of the hour, the DR operator initiates a start command, which is sent to the DR controller for implementation at the DR site.	DR controller identifier. start command, and megawatt output set point	Start command communicated to the appropriate DR controller, which starts the DR unit and sets output to valid set point
3.	Start received	DR controller to DR operator	The DR controller acknowledges the start signal is received and starts the DR unit.	DR controller identifier, timestamp, and start signal and set point acknowledgement If set point not valid: return not valid exception	DR operator records acknowledgement

Alternative B: The DR controller may only offer status when queried.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	DR unit request for operational information	DR operator or AEPSO to DR controller	The DR controller is periodically requested for operational information.	DR controller identifier, timestamp, requester of information identifier, and request for operational parameters (perhaps these are different for each requestor)	DR controller confirms requests are legitimate and prepares response
2.	Service information request	DR controller to DR operator and AEPSO	The DR controller responds to the request for information	See #5 in normal scenario	See #5 in normal scenario

Exception: The DR unit does not start.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	DR unit does not start after request	DR controller to DR operator	The DR controller informs the DR operator that the unit failed to start.	DR controller identifier, timestamp, failed to start status (A reason may also be given.)	DR operator receives information, informs AEPSO, and proceeds to remedy the issue
2.	Monitor status	DR controller to DR operator and AEPSO	The DR controller responds to the request for information.	See #5 in normal scenario	See #5 in normal scenario

Post-conditions:
The DR unit is shut down and becomes available for use at another time. The DR operator records the operational event and submits information to the AEPSO for settlement and closure per their contract.

References:

Issues:

ID	Description	Status
1.	Do the DR operator and AEPSO agree on a single metering device to monitor DR unit output for revenue purposes? Is their independent measurement being done by the AEPSO to corroborate the operation of the DR?	
2.	Is there measurement of isolation breaker/switch status typically?	
3.	Is there supervisory control of isolation breakers? By whom?	
4.	This use case needs to consider distinguishing issues surrounding the different information exchange required by synchronous, asynchronous, and inverter-based DR interconnections.	

Revision history:

No	Date	Author	Description
0	12 Jun 03	S. Widergren	Captured meeting discussion and expanded for exemplary purposes
1	1 Oct 03	S. Widergren	Updated per inputs from D. Goodrich and R. Zhou
2	22 Oct 03	S. Widergren	Updated to reflect changes in the template
3	12 Jan 05	S. Widergren	Updated to include environmental monitoring
4	27 Jun 04	R. Zhou	Added use case and interaction diagrams

Diagrams:

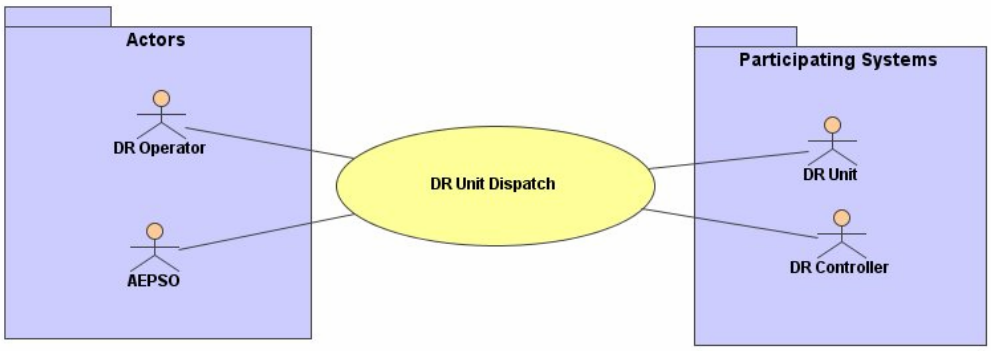


Figure F.1—Use case diagram

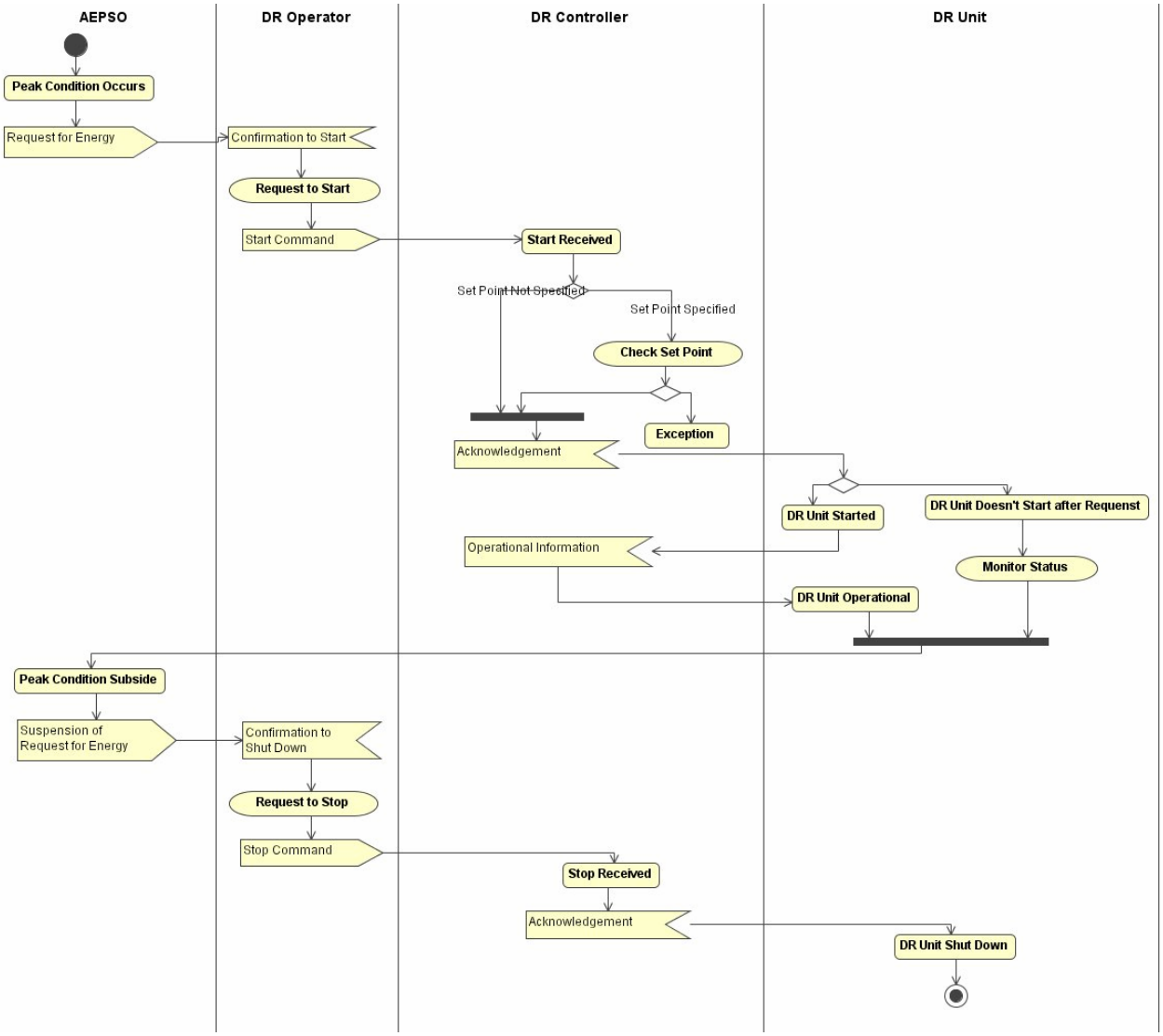


Figure F.2—Interaction diagram

F.2 IEEE Std 1547.3 Use case: DR unit dispatch for energy export

Use case name: DR unit dispatch for energy export

Description: The DR operator of a single-unit 1.1-MW wind turbine intends to operate as an independent power producer. The DR operator will dispatch his/her DR unit with the intention of selling energy back to the owner of the area EPS.

Narrative: The AEPSO has recently interconnected with a 1.1-MW wind turbine. The load on the wind turbine's local EPS is substantially less than the output of the wind turbine, so the DR installation intends to operate as an independent power producer. According to the agreement between the AEPSO and the DR owner, the DR operator can operate the DR unit at any time (unless directed by the AEPSO to disconnect), and the area EPS will accept any amount of energy produced by the unit. The DR owner and the AEPSO have negotiated a contract for the purchase of the DR-generated energy. A dual-metering scheme records the time and energy produced into the area EPS and the energy consumed by the DR installation.

Actors:

Name	Role description
DR operator	Person responsible for instructing the operations of the DR unit
Area EPS operator (AEPSO)	Person responsible for the safe and reliable operation of the distribution system (area EPS) to which the DR site is connected

Participating systems:

System	Services provided
DR controller	Performs communications services between the DR installation site and the outside world
DR unit	The 1.1-MW wind turbine producing energy for export

Assumptions/design considerations:

- The distribution system to which the wind turbine is connected has sufficient capacity to accommodate the DR's power output.
- An impact study was performed to ensure that the DR installation will not adversely affect the existing distribution system. In this scenario, the wind turbine uses an induction generator. (Alternative generation schemes do not use induction generators.) Because the wind turbine is an induction machine, the impact study resulted in the installation of a capacitor bank in the local EPS to provide additional VAR support.
- The DR unit is not placed on the AEPSO's automatic generation control.
- The DR owner has decided he does not want the AEPSO to dispatch the wind turbine.
- The DR can only be brought online when there is sufficient wind. The unit can be taken off line at any time.
- The DR installation has not been contracted to provide ancillary services and will run in voltage-following mode.
- Being a single-unit installation, there is a single DR controller from which all data can be obtained.
- Because of the size of this DR installation, the AEPSO has required the installation of a comprehensive protection scheme that includes a dedicated relay and breaker scheme as well as a transfer trip scheme with the area EPS substation protection.

— Because this particular DR installation is relatively small, the independent system operator, to which the AEPSO belongs, has no interest in knowing the status of this installation.

— The generating agreement has a fixed price for exported energy.

— A transfer trip scheme has been integrated with the area EPS substation protection.

— The unit is big enough to satisfy IEEE Std 1547.

— The communication between DR operator and the unit is secure from non-authorized parties.

— The AEPSO and the DR operator have agreed how the DR protection scheme will perform during faulted conditions, including the prevention of an island. (The implementation of these protection schemes is outside the scope of this document.)

— Three-phase feeder load is balanced and harmonics free.

Pre-conditions:
The AEPSO has a distribution SCADA available at the substation. Therefore, the DR controller to AEPSO communication interfaces with this SCADA system.

Configuration information was previously exchanged in a manual operation.

Normal sequence:

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	DR operator wishes to generate and export power	DR operator informs the AEPSO and schedules a start time	The DR operator contacts (via telephone) the AEPSO, schedules a start time, and provides an estimate of the amount of energy that will be supplied.	Estimate of power (in kilowatts) and schedule (hour starting) NOTE—Power consumed at the DR site when the unit is not exporting is metered by the AEPSO.	AEPSO confirms the request, schedules the start time, and updates the EMS to expect an energy input
2.	Request to start	DR operator to DR controller	The DR operator initiates the start command that is sent to the DR controller.	DR controller identifier and start command and time stamp	Start command communicated to the appropriate DR controller, which starts the DR unit
3.	Start received	DR controller to DR operator	The DR controller acknowledges the start signal is received and starts the DR unit.	DR controller identifier and start signal and time stamp acknowledgement	DR operator records acknowledgement
4.	DR unit started	DR controller to DR operator and AEPSO	The DR unit starts and synchronizes with the area EPS. The DR controller confirms the DR unit is started (by measurement or signal) and reports success and current operating measurements.	DR controller identifier, DR operator and AEPSO addresses, DR unit on signal, timestamp At PCC: real power output, reactive power output, voltage, area EPS connection status, voltage magnitude	DR operator and AEPSO witness and record information received The AEPSO may independently meter the energy change at the PCC.
5.	DR unit operational	DR controller to DR operator and AEPSO	Periodic (2 s): The DR controller sends operational information.	DR controller identifier, DR operator, and AEPSO addresses, timestamp and operational parameters in Step 4	DR operator and AEPSO witness and record information received
6.	DR operator wants to disconnect	DR operator to DR controller	The DR operator instructs the DR controller to open the interconnect breaker.	DR controller identifier, timestamp, and command to open interconnect breaker	DR controller confirms request and opens interconnect breaker
7.	Stop received	DR controller to DR operator	The DR controller acknowledges the stop signal is received and stops the DR unit.	DR controller identifier and stop signal acknowledgement	DR operator records acknowledgement
8.	Stop status	DR controller to DR operator and AEPSO	The DR unit stops and disconnects from the area EPS. The DR controller confirms the DR unit is stopped (by measurement or signal) and reports success and current operating measurements.	DR controller identifier, stop acknowledged, and timestamp At PCC: real power output, reactive power output, and voltage, and area EPS connection breaker status	DR operator and AEPSO witness and record information received The AEPSO may independently meter the energy change and the PCC.

Alternative/exception sequences:

Alternative: The DR operator is instructed to disconnect by the AEPSO.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	AEPSO requests DR disconnect	AEPSO operator to DR operator	The AEPSO calls the DR operator by phone to request a disconnect.	DR controller identifier, disconnect directive, and time to disconnect	DR operator initiates DR disconnect
2.	DR operator directs disconnect	DR operator to DR controller	The DR operator instructs the DR controller to open the interconnect breaker at the appropriate time.	DR controller identifier and command to open interconnect breaker, schedule time to open	DR controller confirms request and opens interconnect breaker at scheduled time
3.	Stop received	DR controller to DR operator	The DR controller acknowledges the stop signal is received and stops the DR unit at the scheduled time.	DR controller identifier and stop signal acknowledgement	DR operator records acknowledgement
4.	Stop status	DR controller to DR operator and AEPSO	The DR unit stops and disconnects from the area EPS. The DR controller confirms the DR unit is stopped (by measurement or signal) and reports success and current operating measurements.	DR controller identifier, stop acknowledged, and timestamp At PCC: real power output, reactive power output, and voltage, and area EPS connection breaker status	DR operator and AEPSO witness and record information received

Exception: A fault occurs on the feeder.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	Fault occurs on feeder	Area EPS protection trips feeder breaker	The protection scheme isolates the fault.		Feeder breaker opens and DR disconnect breaker opens
2.	DR connection breaker opens	DR controller to DR operator	The DR operator is informed that the disconnect tripped.	DR controller identifier, timestamp, disconnect breaker trip event	DR operator alarmed, DR controller logic shutdown DR unit operation
3.	Subsequent status of DR	DR controller to DR operator and AEPSO	The DR controller sends periodic (2 s) status and measurement information.	See Step 5 in normal use case sequence	AEPSO and DR operator respond to abnormal system event (such as tag and lock the disconnect breaker and fix fault) and restore service

NOTE—Restoration and maintenance steps can be added.

Post-conditions:
The DR unit is shut down and becomes available for use at another time. The DR operator records the operational event and submits information to the AEPSO for settlement and closure per their contract.

References:

Issues:

ID	Description	Status
1.	Do the DR operator and AEPSO agree on a single metering device to monitor the DR unit output for revenue purposes? Is there independent measurement by the AEPSO to corroborate the operation of the DR?	
2.	Is there measurement of isolation breaker/switch status typically?	
3.	Is there supervisory control of isolation breakers? By whom?	
4.	Restoration and maintenance steps are not yet added. Are they needed (define new MIC needs)?	

Revision history:

No	Date	Author	Description
0	4 Aug 04	P. Dolloff, S. Widergren	Captured meeting discussion and expanded for exemplary purposes
1	17 Jan 05	S. Widergren	Updated to make consistent with other use cases
2	6 Jun 05	S. Widergren	Revised based on comments from General Electric (Rui Zhou and Reigh Walling) These address contradictions if an induction generator is assumed.
3	27 Jun 04	R. Zhou	Added use case and interaction diagrams

Diagrams:

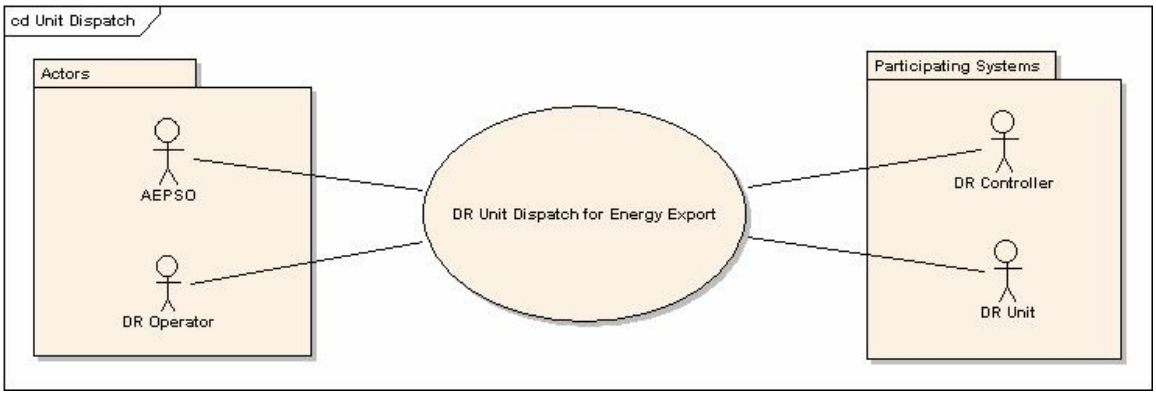


Figure F.3—Use case diagram

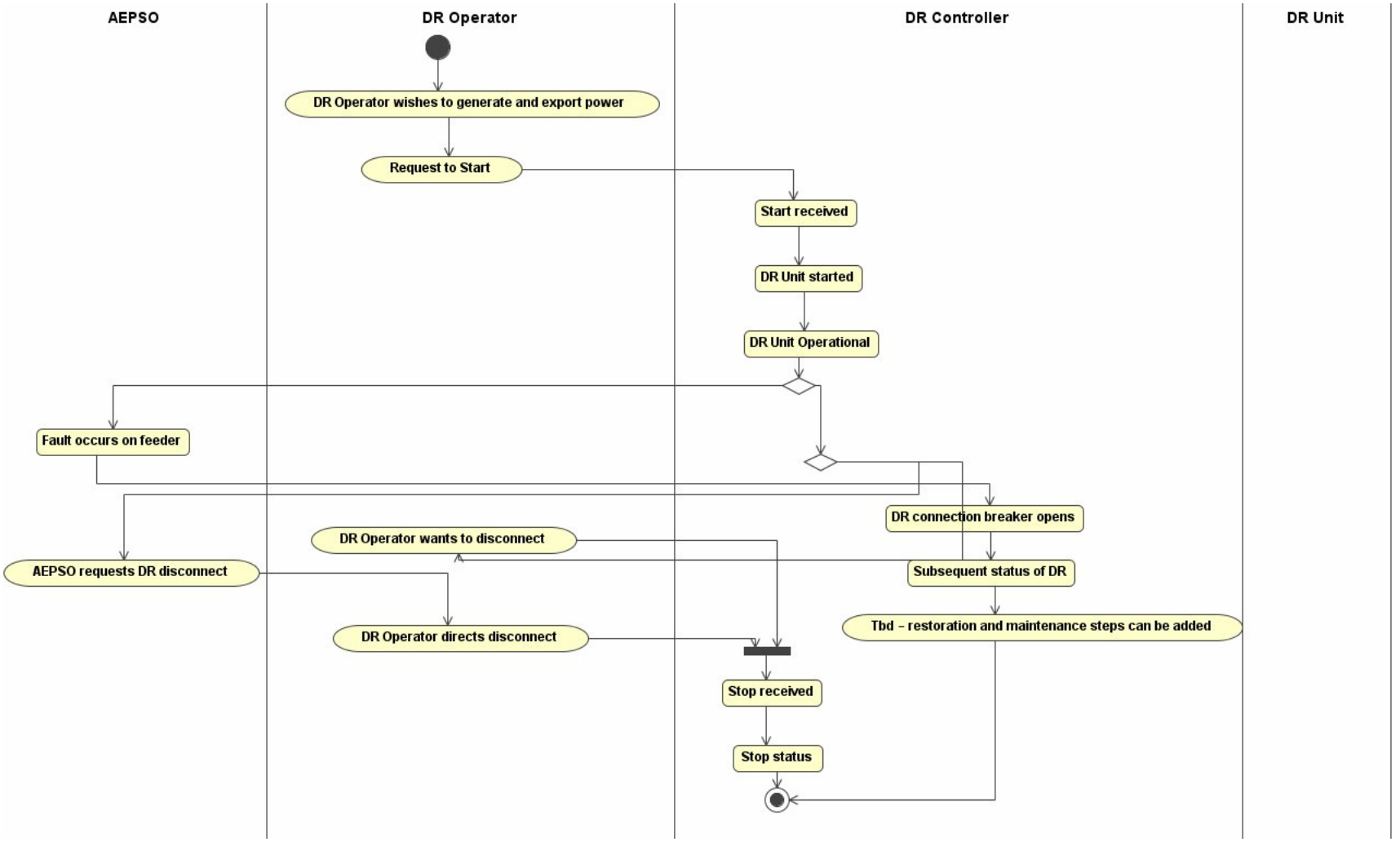


Figure F.4—Interaction diagram

F.3 IEEE Std 1547.3 Use case: DR unit scheduling

Use case name: DR unit scheduling

Description: A DR operator creates, edits, and deletes schedules to dispatch commands to a DR unit. The DR operator's system communicates the scheduled operation to the DR controller, who invokes commands to the DR unit at appropriate times and notifies DR operator of status.

Narrative: A DR operator logs into the DR Dispatch application to create, edit, or delete a schedule for future command dispatches to DR units via a DR controller. The DR operator creates a schedule by defining the schedule parameters, including scheduled commands, time of command invocation, frequency of invocation, and schedule start and end dates. The DR operator then applies the defined schedule to a DR controller, which instructs a DR unit or a predefined group of DR units at a site. The DR controller interprets the active schedules and, at scheduled-defined times, invokes the corresponding schedule-defined commands on the associated DR units. Any exceptions to this normal sequence are conveyed back to the DR operator.

Actors:

Name	Role description
DR operator	Person responsible for instructing the operations of the DR unit
AEPSO	Person responsible for the safe and reliable operation of the distribution system (area EPS) to which the DR site is connected

Participating Systems:

System	Services provided
DR controller	Performs communications services between the DR installation site and the outside world The DR controller coordinates DR unit operation and can store and interpret DR dispatch schedules in this use case
DR unit	The generation or storage device providing electric energy

Assumptions/design considerations:

— The DR site is licensed to operate in parallel with the area EPS under pre-arranged agreements.

— The DR units may be scheduled to operate for a variety of reasons, including those described in other use cases.

— The DR controller is assumed to have the hardware and software capacity to interpret DR unit operation schedules and translate that into real-time operation.

Pre-conditions:

All participants in the DR program have already been identified within the system. Corresponding user entities (including login name and password) have been created and assigned to stakeholders. The system is aware of notification targets and addresses.

Normal sequence:

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	DR operator determines the next day's schedule of operation for a DR unit	DR operator to AEPSO	The DR operator initiates a dispatch schedule and notifies the AEPSO.	E-mail messages to AEPSO address indicating a new DR unit dispatch, with identification of the DR unit, and schedule	AEPSO confirms schedule and OKs operation per established agreements
2.	DR operator creates a new schedule and assigns it to a DR controller	DR operator to DR controller	The DR operator creates a new schedule in his system and communicates this to the DR controller.	DR operator identifier, schedule identifier, DR controller identifier, start and end time and dates, on request or kilowatt set point	DR controller confirms receiving schedule
3.	Scheduled dispatch start time	DR controller to DR operator and AEPSO	The DR controller verifies that the DR site is available to generate and parallel operation equipment is operational.	DR operator, AEPSO, DR controller, and schedule identifiers, timestamp, DR site ready-to-operate signal	DR operator and AEPSO note intent to operate
4.	DR controller implements schedule	DR controller to DR operator and AEPSO	The DR controller implements dispatched commands on the DR unit and reports status to the DR operator and the AEPSO.	Identifiers and DR unit operation data as in DR unit for Dispatch Use Case	DR operator and AEPSO note and record monitored information
5.	Scheduled dispatch end time	DR controller to DR operator and AEPSO	The DR controller notifies the DR operator and AEPSO that the scheduled end time has been reached.	Identifiers, timestamp, scheduled-end time-reached notification	DR operator and AEPSO note and record intent to cease operation
6.	DR controller shuts down DR unit	DR controller to DR operator and AEPSO	The DR controller reports status.	Identifiers, timestamp, and other status and operation data as specified at shutdown in DR unit Dispatch Use Case	DR operator and AEPSO note and record monitored information

Alternative/exception sequences:

Exception A: The DR unit is unavailable to start or is already running.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	At schedule start time, DR unit unavailable	DR controller to DR operator and AEPSO	The DR controller prepares to initiate the schedule but finds the DR unit is already running or not available. The DR controller then notifies concerned parties.	DR operator, AEPSO, DR controller, and schedule identifiers, timestamp, and exception status that schedule cancelled with reason DR unit unavailable	DR controller aborts schedule, DR operator and AEPSO note that schedule is not to take place

Exception B: The DR controller is directed to terminate the schedule before operation.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	DR operator determines schedule is to be cancelled before operation	DR operator to DR controller	The DR operator sends a cancel-schedule message.	DR operator, DR controller, and schedule identifiers, timestamp, and schedule cancel indicator	DR controller confirms cancel message received and removes schedule
2.	DR controller removes schedule	DR controller to DR operator and AEPSO	The DR controller confirms the schedule cancellation.	Identifiers, timestamp, schedule cancellation-received indication and schedule cancelled	DR operator and AEPSO note schedule cancelled

Exception C: The DR controller is directed to terminate the schedule during operation.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	DR operator determines schedules is to be cancelled during operation	DR operator to DR controller	The DR operator sends a cancel-schedule message.	DR operator, DR controller, and schedule identifiers, timestamp, and schedule-cancel indicator	DR controller confirms cancel message received, removes schedule, and shuts down DR unit
2.	DR controller removes schedule and shuts down DR unit	DR controller to DR operator and AEPSO	The DR controller confirms the schedule cancellation and shuts down the DR unit	Identifiers, timestamp, schedule-cancellation-received indication, DR unit shutdown status as in DR unit Dispatch Use Case	DR operator and AEPSO note schedule cancelled and DR unit status

Post-conditions:

The DR schedule is confirmed completed.

References:

Issues:

ID	Description	Status
1.	Is this a reasonable use case to consider, or should we presume that DR controllers do not operate autonomously but are always directed by a DR operator function?	
2.	This use case needs to consider distinguishing issues surrounding the different information exchange required by synchronous, asynchronous, and inverter-based DR interconnections.	

Revision history:

No	Date	Author	Description
1.	23 Jun 04	Arup Barat	Initial use case document
2.	12 Jan 05	SE Widergren	Differentiated use case to emphasize remote scheduling of a DR site and make complementary with other use cases
3.	27 Jun 04	R. Zhou	Added use case and interaction diagrams

Diagrams:

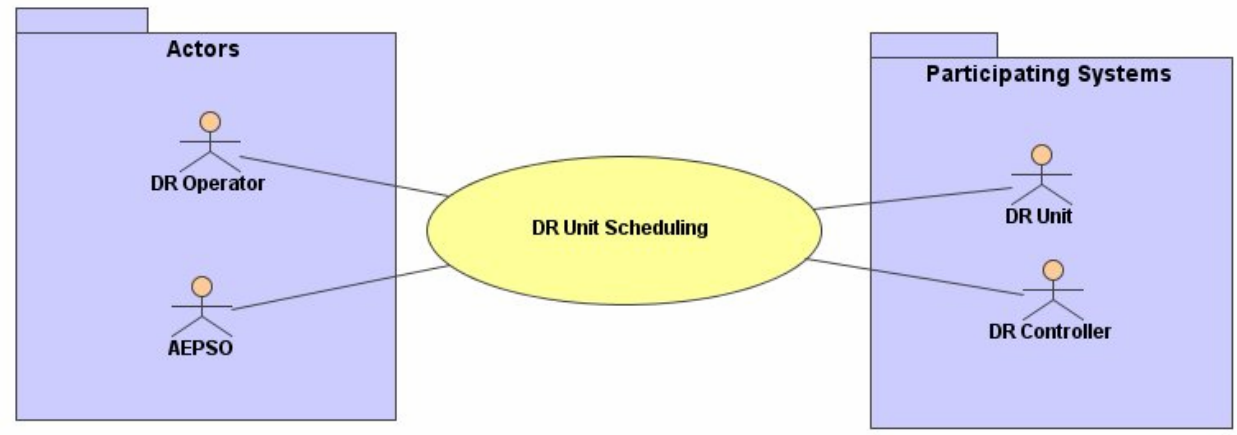


Figure F.5—Use case diagram

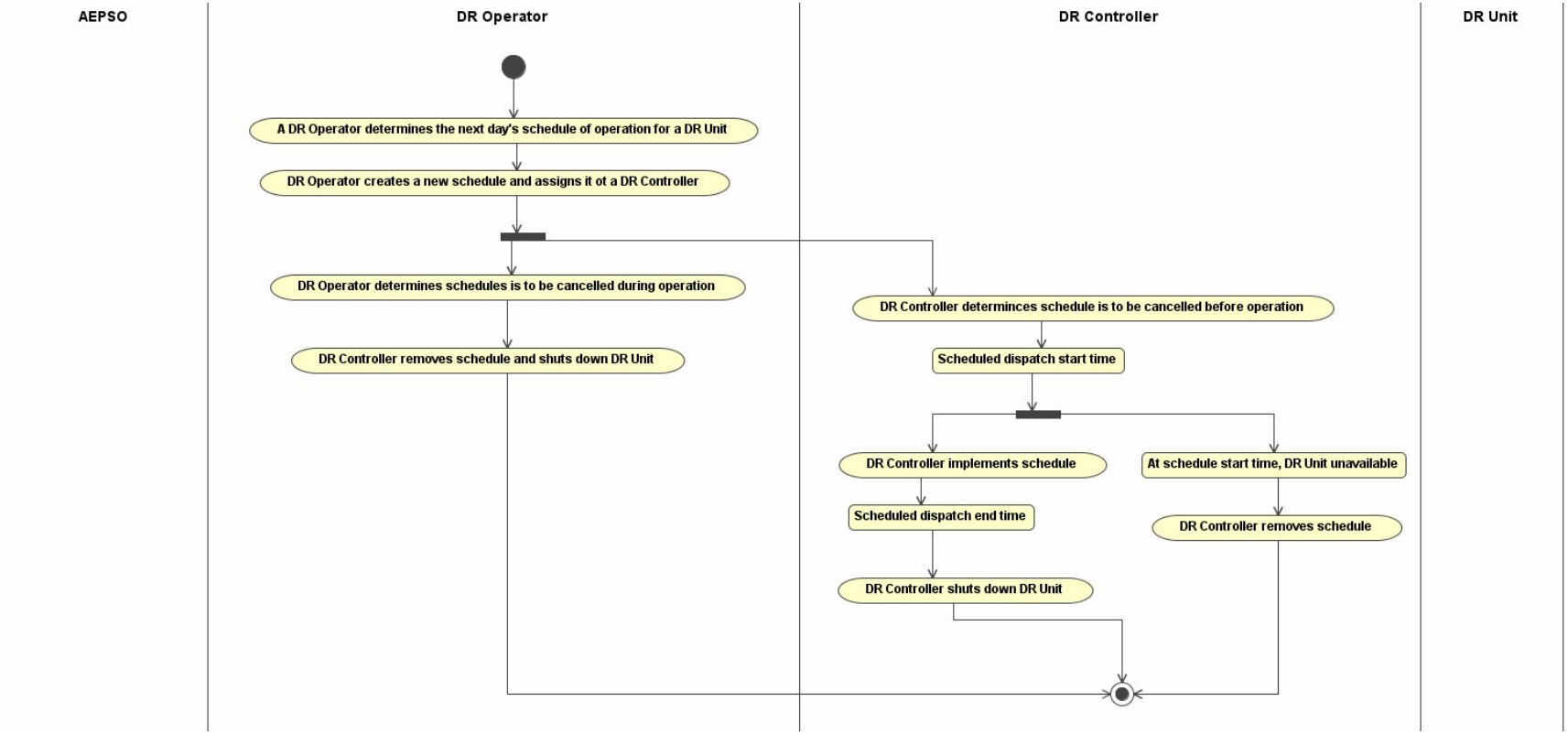


Figure F.6—Interaction diagram

F.4 IEEE Std 1547.3 Use case: DR aggregation

Description: The DR operator dispatches multiple DR units during peak periods of energy use per information (e.g., real-time pricing, a dispatch request, or interruptible rate) provided by the DR aggregator and coordinated with the AEPSO. The DR aggregator monitors net metering information from the site.

Narrative: An aggregator assembles a cadre of DR that are coordinated to provide energy to the area EPS to meet stressed conditions caused by capacity, energy prices, or both. To do this, the AEPSO notifies the DR aggregator of his resource needs in an area. The DR aggregator analyzes the resource pool and determines a dispatch schedule for operations. DR operators are informed of the needs from their resources and dispatch their resources as described in the use case "DR unit Dispatch." To accomplish this use case, the aggregator needs to understand the status of the resources prior to and during operation. At the conclusion of the aggregated operation, the aggregator needs the information needed to reconcile the performance with contract and billing information (net metering) for the DR owners and the AEPSO.

In areas with high energy costs such as New York City, load curtailment programs have been initiated in which facilities can make use of onsite generators to provide backup power for peaking, reserve, or load management capability. In many instances, the generators are in the 1-MW range. To make economic sense, it is necessary to aggregate multiple units into one virtual power plant that can be dispatched as a normal power plant by the DR aggregator. The DR aggregator is responsible for the collection and aggregation of DR units. It generally has a contract to split revenues with the DR owners of the DR units. The DR aggregator is the point of interface to the AEPSO. The aggregator also maintains a control room and responds to calls and inquiries from the AEPSO before, during, and after generation. The aggregator owns and maintains communication channels to the DR operators and DR unit sites as well as all of the monitoring equipment used for performance verification. It is responsible for calculating settlement, verifying with the AEPSO, and distributing payments to the DR owners. The DR operators are responsible for starting, stopping, and monitoring their DR units.

Actors:

Name	Role description
AEPSO	Person/entity responsible for the safe and reliable operation of the distribution system Responsible for providing some information (e.g., real-time price or interruptible rate signal) to allow the DR aggregator to make DR operation schedules
DR aggregator	Entity responsible for the aggregation and dispatch signals to DR operators of DR units in response to an area EPS-contracted need
DR owner	Owns the DR units used by the DR aggregator to supply local loads
DR operator	Person/entity responsible for instructing the operation of DR units

Participating systems:

System	Services provided
DR controller	Performs communications services between the DR installation site and the outside world
DR unit	The generation or storage device providing electric energy
DR aggregator Dispatch System	Aggregates multiple DR sites to appear as larger power generation devices to allow area EPS peak-shaving with minimal work by the dispatcher

Assumptions/design considerations:

- Contract arrangements have been made between the DR aggregator and the DR owner to pay a fee for being on call and having the DR available for distribution system support.
- The AEPSO contracts with the DR aggregator to provide energy that reduces system load in a local region. The form of communication (e.g., a phone call or e-mail) is not important, but they are not within the same organization.
- The AEPSO has measuring equipment to verify operation and the amount of energy involved from the system perspective.
- The DR unit is to be operational within 10 min from the time that the DR operator is informed.
- The DR unit is operated at either a standard capacity setting or a variable power setting.
- This situation occurs occasionally, and the units run for about 1–4 h.
- All units are big enough to satisfy IEEE Std 1547.
- The communication between the DR operator and the unit is secure from non-authorized parties.
- All necessary data for reporting, monitoring, and billing is monitored and recorded to allow for the creation of the necessary statements and reports.
- All units have been aggregated (grouped) by the DR aggregator according to the needs of the AEPSO and the availability of the DR units. This grouping may be based on DR unit location, DR unit fuel type, DR unit emissions, or DR unit contract status (e.g., real-time versus interruptible rate).

Pre-conditions:
The area EPS (multiple distribution feeders all the way to the transmission system) is experiencing high demand and approaching capacity limits. DR units are known to be available in the affected region(s) and can be used to mitigate the problem. Adequate DR units are available for coordination by the DR aggregator to meet area EPS needs.

Normal sequence:

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	Stressed condition occurs	AEPSO informs aggregator energy is needed	The AEPSO calls/e-mails the DR aggregator, informs that power is needed, and gives location regarding the required energy.	Location, unit type, time period, amount of power requested.	DR aggregator confirms request for power and initiates a dispatch request in his system
2.	Select DR units to start	DR aggregator to his Dispatch System	The aggregator decides which DR units best meet the criteria to mitigate the peak demand.	DR unit parameters that affect selection decision (e.g., location and fuel type)	DR units selected for dispatch
3.	Aggregator contacts DR operators	Aggregator to DR operator	The aggregator contacts individual DR operators and requests that they run their generators either connected with the grid or separated from the grid.	Request from aggregator to DR operator for DR unit dispatch, amount, and scheduled period	DR operator confirms request for DR unit operation
4.	Request to start DR units	DR operator to DR controllers	The DR operator initiates start commands to selected units.	See DR unit Dispatch use case	DR units start and operate at specified power levels
5.	Generation start time	DR aggregator to DR operator	The DR aggregator contacts the DR operators at the start time to make sure they comply with the request.	DR unit identifier, request for operational confirmation, timestamp	DR operator responds to aggregator with the DR status
6.	DR units monitoring	DR controllers to DR operators and DR aggregator, and AEPSO	Immediately after the start and periodically thereafter, all units report operational information. Data are aggregated and reported to the DR operator.	Each DR controller has identifiers for DR operator, DR aggregator, and AEPSO Operational information, including emissions values, are reported to each party as needed	DR operator, DR aggregator, and AEPSO witness and record data received
7.	DR site net metering	DR controllers to DR operator and DR aggregator	Power accumulators at the point of DR connections are scanned by the DR controller and reported to the DR operator and DR aggregator. The AEPSO has its own metering equipment at the PCC, which it communicates with independent of this use case.	Megawatt-hour values are reported periodically with timestamp	DR operator and DR aggregator record Megawatt-hour values
8.	Peak condition subsides	AEPSO to DR aggregator	The AEPSO calls/e-mails the DR aggregator and informs that energy is no longer needed per the original transaction request.	Dispatch transaction identifier to terminate	DR aggregator confirms request to terminate the transaction

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
9.	Select group/units to stop	DR aggregator to his Dispatch System	The aggregator interprets data from the AEPSO and selects units to stop.	DR units to stop	DR units selected for shutdown
10.	DR aggregator notifies DR operators	DR aggregator to DR operator	The aggregator contacts individual DR operators to request that they stop the DR units.	DR operator identifier, stop-DR unit request	DR operator confirms request to stop DR unit
11.	Request to stop units	DR operator to DR controller	The DR operator initiates stop commands to selected DR controllers.	See DR unit Dispatch Use Case step to stop DR unit	DR units stop operation
12.	DR units stopped	DR controller to DR operator, DR aggregator, AEPSO	The DR controller reports the shutdown and gives appropriate operational data to prove the shutdown.	Multiple DR units operational information (e.g., timestamp and kilowatts)	DR operator, aggregator, and AEPSO witness and record data received
13.	Report net-metering	DR controller to DR operator and DR aggregator	The DR controller obtains metered data at the point of DR Connection and reports final values.	DR operator and DR aggregator identifiers, timestamp, and megawatt-hour values	DR operator and DR aggregator record the net-metered values and use this for settlements with DR owner and AEPSO (not described here)

Alternative/exception sequences:

Exception A: The DR unit is off line or already running.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	DR unit off line or already running	DR controller to DR operator	Send any operational data pertinent to the operation of the DR unit and its availability for dispatch.	DR unit identifier and offline or unit-on status	DR operator witnesses and records data and marks DR unit as unavailable

Exception B: The DR unit goes off line during dispatch.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	DR unit goes off line during dispatch operation	DR controller to DR operator	Send any operational data pertinent to the operation of the DR unit and its availability for dispatch.	Besides normally monitored information, uncommanded shutdown exception sent	DR operator witnesses and records data and marks DR unit as unavailable

Exception C: There is a power outage from the area EPS side of the PCC.

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	Power outage on a DR unit's utility connection	DR controller to DR operator	Send any operational data pertinent to the operation of the DR unit and its availability for dispatch. DR unit disconnects from utility and operates as emergency generation for the site.	DR aggregator and DR controller identifiers, timestamp, PCC energize status, PCC disconnect status	DR operator witnesses and records data and marks DR unit as unavailable

Post-conditions:
DR units are shut down and available for dispatch at another time or for emergency (backup) power generation for the DR facility.

References:
DR unit for Dispatch use case

Issues:

ID	Description	Status
1.	How far do we go in defining the aggregating (grouping) parameters? These parameters will change on a system-by-system basis and are really the prevue of the Aggregator (DR operator) and not subject to this guideline. This guideline, as I understand it, is to define the minimum data available from a DR unit for dispatch as well as some of the basic types of technology needed.—C. Whitham	

Revision history:

No	Date	Author	Description
0.	26 Jun 03	C. Whitham	Initial draft of Aggregated Energy Use Case
1	27 Oct 03	S. Widergren	Updated to fit changes in use case template, add a narrative, and include questions concerning the role of the aggregator in the use case
2	26 Jul 04	R. Zhou	Merged with Integrated Energy and Communication Systems Architecture Distribution Generation aggregator use case
3	13 Jan 04	S. Widergren	Updated to be consistent with the DR unit for Dispatch Use Case, merged the Demand Response Program—Dispatch Applications Use Case, and added a net metering aspect
4	27 Jun 04	R. Zhou	Added use case and interaction diagrams

Diagrams:

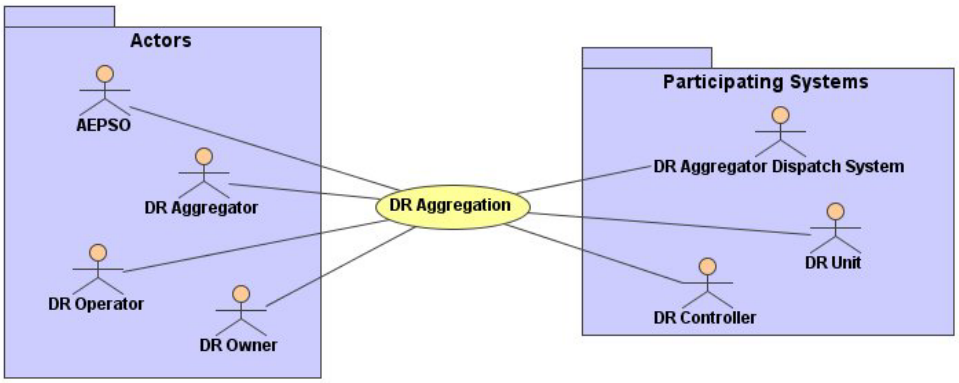


Figure F.7—Use case diagram

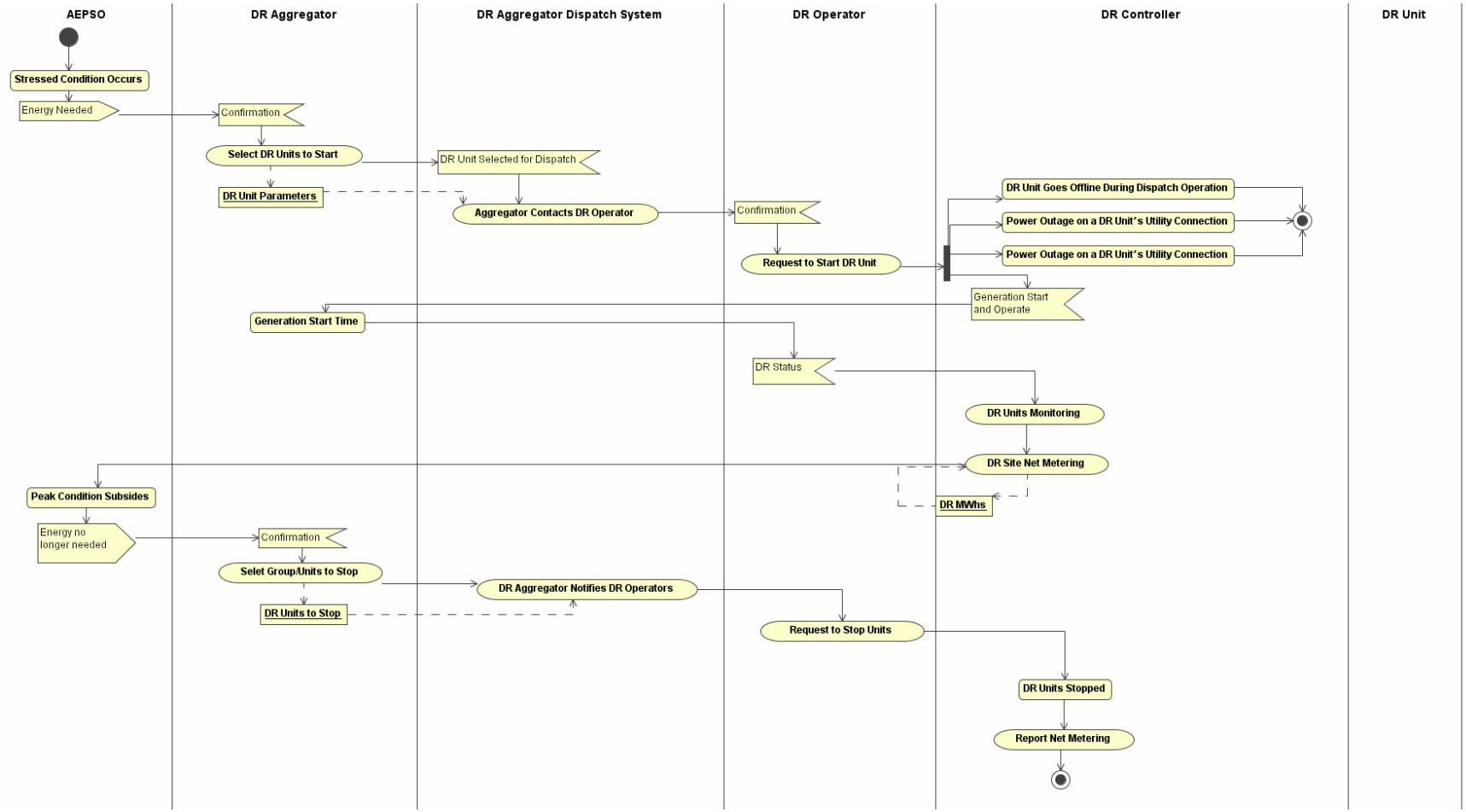


Figure F.8—Interaction diagram

F.5 IEEE Std 1547.3 Use case: DR maintenance

Use case name: DR Maintenance

Description: A DR owner contracts with a DR maintainer to periodically service a DR unit and perform emergency repairs. The DR maintainer monitors key performance indicators and coordinates with the DR operator when service is required.

Narrative: A DR maintainer works for a company that services DR. This company has contracted with DR owners to perform periodic and emergency maintenance on the DR units and monitor performance to determine preventive maintenance. The DR maintainer has a communication link to the DR controller of the site of interest to obtain periodic updates of operational parameters when the DR controller operates the DR unit. The DR maintainer coordinates with the DR operator, who informs the DR maintainer of abnormal operation. The DR maintainer can also ask the DR operator to run or stop the DR unit to monitor operating parameters or lock out DR unit operation for maintenance. Otherwise, the DR maintainer does not directly operate the unit unless he or she overrides DR operator control at the site.

Actors:

Name	Role description
DR operator	Person responsible for instructing the operations of the DR unit
DR owner	Person who owns the DR units and contracts with the DR maintainer to provide real-time maintenance
DR maintainer	Person responsible for monitoring the performance of the DR unit, performing diagnostics, and generally maintaining the DR unit

Participating systems:

System	Services provided
DR controller	Performs communications services between the DR installation site and the outside world The DR controller coordinates DR unit operation and can store and interpret DR dispatch schedules in this use case
DR unit	The generation or storage device providing electric energy

Assumptions/design considerations:

- The DR site is licensed to operate in parallel with the area EPS under pre-arranged agreements.
- The DR owner contracts with the DR maintainer to provide maintenance.
- The communications, addresses, identification, and security systems are in place to enable the DR operator and DR maintainer interaction with the DR controller.

Pre-conditions:

The DR unit is in the shutdown state, but the DR controller is active and ready to communicate.

Normal sequence:

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	DR maintainer queries operational parameters	DR maintainer to DR controller	The DR maintainer asks for static performance parameters from the DR controller on the DR units it represents.	Identifiers for DR maintainer, DR controller, DR unit(s) Timestamp, type of static information on DR unit(s) (see type table below)	DR controller collects static maintenance information
2.	DR controller provides static maintenance parameters	DR controller to DR maintainer	The DR controller responds to the request for static information about the DR unit(s).	Identifiers for DR maintainer, DR controller, DR unit(s) Timestamp, present static information on DR unit(s) (see type table below)	DR maintainer records this information Internal software may perform diagnostics on the information as well as store it for analysis of the dynamic situation
3.	DR maintainer coordinates with DR operator to test DR unit	DR maintainer to DR operator to AEPSO	The DR maintainer requests a DR unit maintenance test from the DR operator. The DR operator checks schedules and status and coordinates with the AEPSO. (See DR unit Dispatch Use Case.)	Identifiers of DR controller, units, operator, maintainer, AEPSO, as well as timestamp	DR operator coordinates with AEPSO, schedules test operation and provides DR maintainer with the schedule of operation
4.	DR operator starts DR unit	DR operator to DR controller, AEPSO, and DR maintainer	The DR operator performs the DR unit Dispatch Use Case and informs the DR maintainer when the unit is running.	Identifiers of DR controller, units, operator and maintainer, as well as timestamp and indication of whether DR unit is operational	DR maintainer acknowledges unit is operational and initiates information-gathering from DR controller
5.	DR maintainer requests dynamic information	DR maintainer to DR controller	The DR maintainer asks for dynamic performance parameters from the DR controller on the DR units it represents.	DR maintainer, DR controller and unit(s) identifiers, timestamp, type of dynamic information (see DR type table below), and frequency of update	DR controller verifies the dynamic information requested is available and initiates periodic updates to DR maintainer based on frequency of update
6.	DR controller updates DR maintainer with dynamic information	DR controller to DR maintainer	The DR controller periodically sends updated dynamic operational information to the DR maintainer per the request.	Identifiers for DR maintainer, DR controller, DR unit(s). Timestamp, present dynamic information on DR unit(s) (see type table below)	DR maintainer records updates from DR controller and uses this information to perform maintenance diagnostics, potentially resulting in a scheduled maintenance
7.	DR maintainer requests shutdown	DR maintainer to DR operator	The DR maintainer informs the DR operator that the DR unit maintenance test is done and the unit can be shut down.	Identifiers for DR maintainer, operator, DR controller, and units, timestamp, and request to shut down	DR operator coordinates with AEPSO and DR controller to shut down DR units (see DR unit Dispatch Use Case)

Information by DR type:

DR type	Static maintenance information	Dynamic maintenance information
Diesel reciprocating engine	Voltage level rating Current rating Temperature rating Volt-amps rating Watt rating Var rating Power factor rating Total hours operated Hours operated since reset Total number of starts Number of starts since reset Fuel type/grade Fuel tank capacity Maximum turbine pressure Maximum inlet temperature Minimum speed Maximum speed	On/off status Area EPS synchronization status Excitation status Exceptions: voltage high/low, current high/low, frequency, emergency trip, oil pressure high/low, coolant pressure high/low, engine alarm Generator frequency Generator voltage Engine temperature Engine speed Engine timing Air pressure Coolant pressure Intake manifold pressure Intake manifold temperature Battery voltage Fuel level
Fuel cell	…	…
Gas turbine	…	…
…		

Alternative/exception sequences:

None.

Post-conditions:

The DR units are down and ready to be called. The DR maintainer arranges maintenance calls as needed.

References:

Issues:

ID	Description	Status
1.	This needs to be carefully reviewed by DR maintenance experts.	

Revision history:

No	Date	Author	Description
	12 Jan 05	SE Widergren	Draft of a maintenance use case
	27 Jun 04	R. Zhou	Added use case and interaction diagrams

Diagrams:

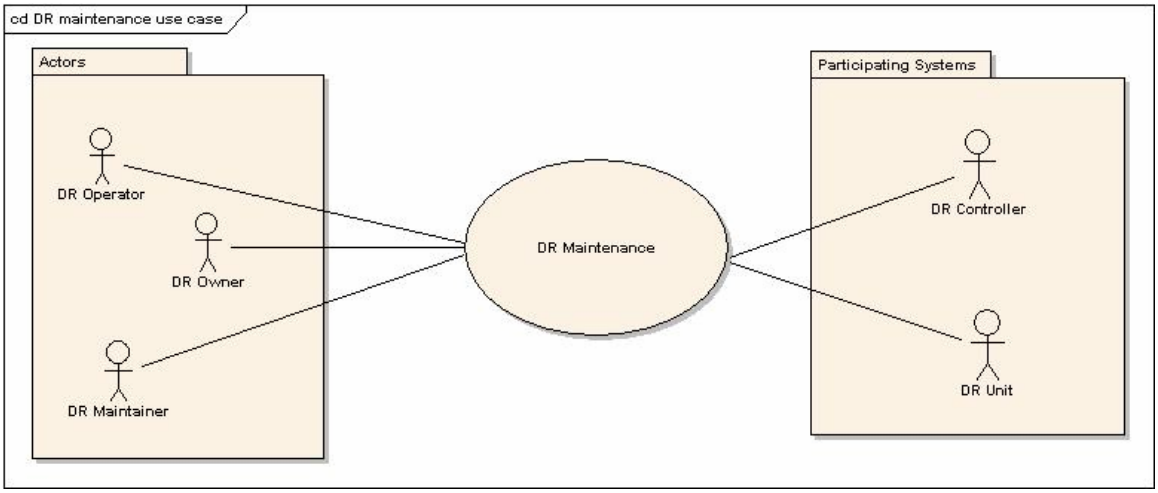


Figure F.9—Use case diagram

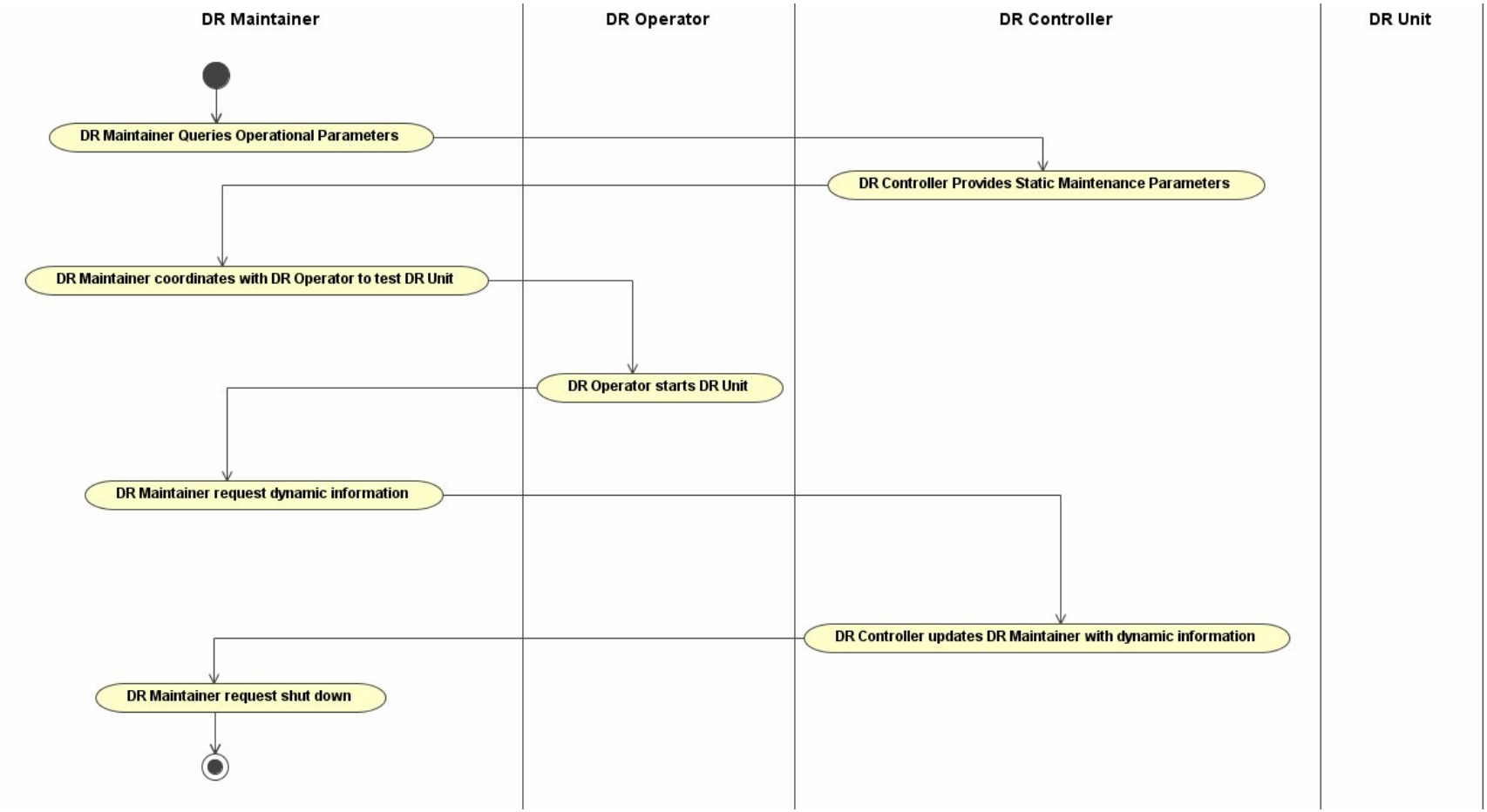


Figure F.10—Interaction diagram

F.6 IEEE Std 1547.3 Use case: DR ancillary services

Use case name: DR ancillary services

Description: The DR may be used by the area EPS operator to provide any or all of the following ancillary services:

1) Load regulation
2) Energy losses
3) Spinning and non-spinning reserve
4) Voltage regulation
5) Reactive supply

Narrative: Because item 4) and item 5) above have been covered in other use cases, spinning reserve is selected as an example of ancillary services.

Actors:

Name	Role description
DR operator	Person responsible for operating the DR unit
AEPSO	Person responsible for the safe and reliable operation of the distribution system (area EPS) to which the DR is connected

Participating systems:

System	Services provided
DR controller	Performs communication services between the DR site and the AEPSO and DR operator This controller also provides the status of the existing unit output and capability
DR unit	The generating unit provides spinning reserve

Assumptions/design considerations:

— The DR unit is capable of providing the spinning reserve function.

— Contract agreements have been made between the DR operator and the AEPSO to provide spinning reserve ancillary services.

Pre-conditions:

The AEPSO informs the DR operator of an anticipated need for spinning reserve.

Normal sequence:

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	Spinning reserve shortage	AEPSO to DR controller	The AEPSO makes request to provide spinning reserve.	Spinning reserve amount	DR controller accepts request
2.	DR controller limits output to provide spinning reserve amount	DR controller to AEPSO	The DR controller informs the AEPSO of actual and generation output and unit capability.	kilowatt output and capability	AEPSO acknowledges DR data

Alternative/exception sequences:

None.

Post-conditions:

References:

Issues:

ID	Description	Status

Revision history:

No	Date	Author	Description
0.	26 Oct 05	M. Davis	Submitted new use case
1	6 Nov 05	S. Widergren	Revised for consistent format and naming conventions

Diagram:

None.

F.7 IEEE Std 1547.3 Use case: DR providing reactive supply

Use case name: DR Providing Reactive Supply

Description: The DR unit may provide reactive supply either by absorbing VARs or producing VARs by changing the field current to match a pre-established schedule. Alternatively, a stated power factor on the high side of the interconnection transformer or PCC can be established.

Narrative: The DR unit may be required to contractually provide a fixed amount of VARs for a customer served from the distribution circuit, or the AEPSO may ask the DR unit to maintain a source power factor for the circuit as measured at the circuit line breaker.

Actors:

Name	Role description
DR operator	Person responsible for operating the DR unit
AEPSO	Person responsible for the safe and reliable operation of the distribution system (area EPS) to which the DR is connected In this use case, the AEPSO is the DR operator, not necessarily the DR owner

Participating systems:

System	Services provided
DR controller	Performs communication services between the DR site and the DR operator This controller accepts reactive supply or power factor schedules and controls the unit to provide the required reactive or power factor The actual measured data is communicated to the AEPSO
DR unit	The DR unit provides the required reactive supply or maintains the power factor schedule

Assumptions/design considerations:

- The DR unit is capable of providing the reactive supply.
- Contract agreements have been made between the DR owner and the AEPSO to provide reactive supply services.
- The AEPSO receives the required reactive supply data.

Pre-conditions:

The circuit voltage profile is below limits.

Normal sequence:

Step	Event	Sender to receiver	Description of process/action	Information to be exchanged	Response to action
1.	Reactive or power factor schedule sent to DR controller	DR operator to DR controller	The DR operator sends hourly reactive or power factor schedules.	Reactive or power factor schedule	DR controller accepts and initiates control per schedule
2.	DR excitation system adjusts field current to attain the required reactive output or power factor at the PCC	DR controller to DR operator	The DR controller informs the DR operator of actual and scheduled reactive output or power factor.	Reactive output or power factor at the PCC	DR operator acknowledges DR data when voltage is within limits on the circuit
3.	Voltage on circuit is out of limits	DR operator to DR controller	The DR operator informs the DR controller to modify the reactive supply schedule.	New reactive or power factor schedule	DR controller implements new schedule; new schedule resolves out-of-limit condition

Alternative/exception sequences:

None.

Post-conditions:

References:

Issues:

ID	Description	Status

Revision history:

No	Date	Author	Description
0.	26 Oct 05	M. Davis	Submitted new use case
1	6 Nov 05	S. Widergren	Revised for consistent format and naming conventions

Diagram:

None.

Annex G

(informative)

Sample information exchange agreement

The information in Annex G is given for informational purposes only. It is only an example, and there may be other examples in the market.[1] This annex is an example of an MIC approach for information exchange with DR sites.

Sample IEA	Description
COMSYS™	This IEA is provided by Connected Energy as an example of the MIC approach it uses to integrate DR.

Connected Energy hereby acknowledges the co-sponsorship of the U.S. Department of Energy (DOE) under the Cooperative Agreement DE-FC26-04NT42213 in producing the work captured in this annex. The content provided by Connected Energy, in whole or in part, may be used, reproduced, published and distributed in reports submitted to DOE and in other academic, technical and professional publications, conference proceedings, Web sites or similar works.

[1] This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same results.

Table of Contents

Revision history:

No	Date	Author	Description
1.	18 May 2005	Author 1	Initial Draft of a sample IEA
2.	3 June 2005	Author 2	Corrections and input on template modification
3.	28 June 2005	Author 1	Revised sections
4.	19 Nov 2005	Author 2	Moved section on Choreography Rules and some titles to align with change made at 17-18 Nov 05 1574.3 meeting.

G.1 Introduction

The purpose of the document is to articulate a sample information exchange agreement (IEA) for participants in Connected Energy's *COMSYS*™—DR remote monitoring and control system. The document is developed as per the guidelines set by IEEE Std 1547.3 Clause 7. It shall be used as a standard reference to enable interoperability between devices, controls and stakeholders internal and external to the system.

G.2 Theory of operation overview

The primary interface for interoperability between components in *COMSYS* is ener*TALK*™. ener*TALK* builds on a messaging protocol for exchanging data and initiating remote command calls between a field-deployed data source client and Connected Energy Corp's (CEC's) Network Operations Center (NOC): Machine Operations Center (MOM) is designed to be used over an asynchronous, multi node, selectively routable, messaging layer. XML is used to markup the message in accordance with the protocol schema.

ener*TALK* is a request/response protocol for posting remote site's real-time data to a NOC and dispatching commands to the remote sites. ener*TALK* producers installed at remote data source clients initiate posting 'ener*TALK*' messages to an identified server hosting MOM's ener*TALK* consumer application—Connection Manager. The ener*TALK* consumer explicitly acknowledges each posting ener*TALK* message when the posting message has been processed without error. In the event of errors an error message is returned to the posting client with explicit error identifiers. It is the responsibility of the data source client to keep track of the acknowledgement timeouts and execute reporting logic to insure real-time data are not lost to the MOM.

Commands from the MOM are marked-up as ener*TALK* messages and dispatched to an ener*TALK* consumer installed at the remote data source client. The result of the command execution is reported as an ener*TALK* message.

ener*TALK* messages are most commonly transported over HTTP as the body of an HTTP-POST. The transport is encapsulated within an IPSEC VPN Tunnel between the remote sites' VPN Client and the NOC VPN Concentrator. All the ener*TALK* producers located at a remote site share a VPN Client and the IPSEC Tunnel.

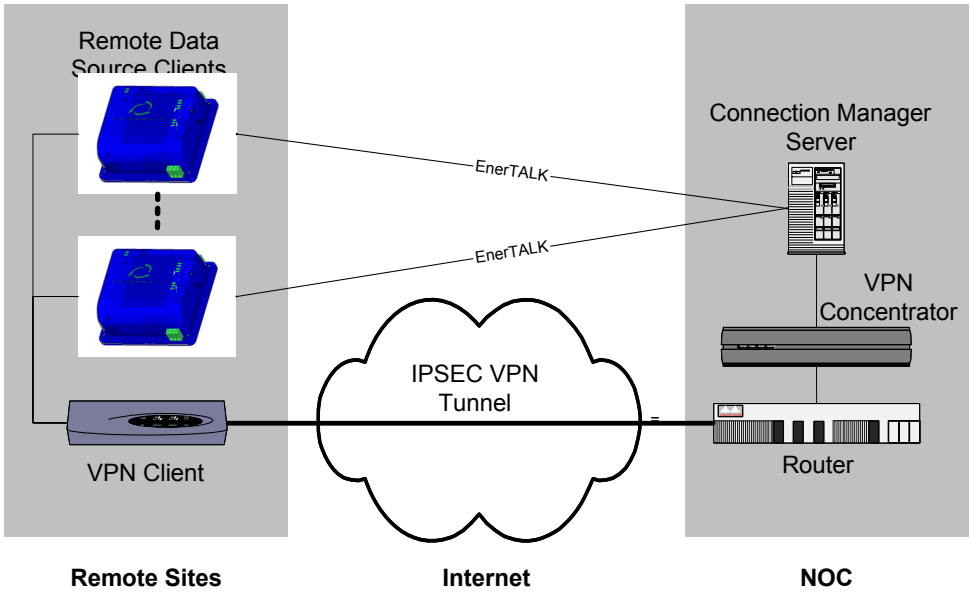


Figure G.1—Network diagram

G.3 Shared ontology

ener*TALK* is capable of supporting multiple shared ontologies between integration partners sharing a common IEA. Entities and their attributes defined by the ontology are mapped to xml objects and attributes for message based transport. Natively supported xml mapping models include the following:

— IEC 61850 [B14] DER Object Models

— ASERTII testing protocol dataset

— ener*TALK* DER Object Models

G.4 Message structure

ener*TALK* Messages are comprised of three autonomous sections:

a) *Envelope*: Acts as the message container

b) *Header:* Provides the context for the message within the messaging subsystem

c) *Payload*: Defines the contents of an ener*TALK* message

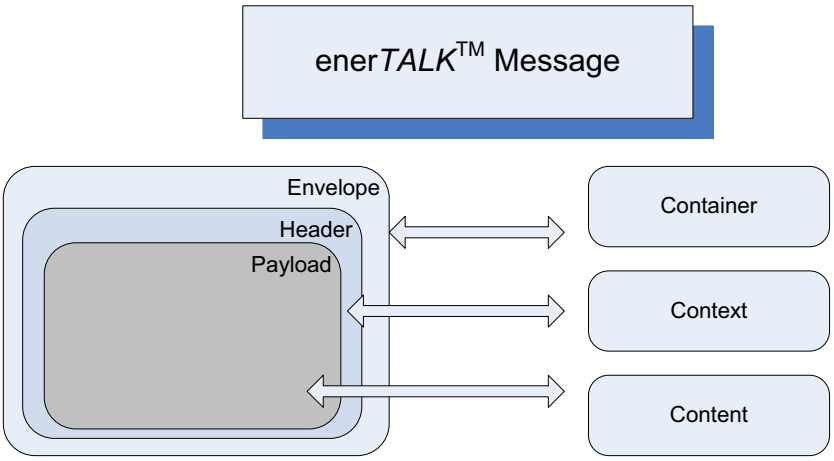


Figure G.2—ener*TALK* message structure

G.4.1 Message envelope

The ener*TALK* message envelope provides a container for the entire ener*TALK* message. For the most common implementation of ener*TALK* over HTTP, a single HTTP-POST serves as the message envelope. The purpose of the envelope is to encapsulate mandatory transport layer services.

G.4.2 Message header

The message header provides the context for the ener*TALK* message. It is comprised of sets of header attributes that qualify the entire ener*TALK* message regardless of the payload. A list of message header attributes follows:

Header key	Header Values	Description	Optional
ener*TALK* - version	*Version number*	Identifies the ener*TALK* version encapsulated in the message	No
ener*TALK* - compression	Gzip Deflate	Identifies compression algorithm. Absence of this header indicates uncompressed data	Yes (default is uncompressed)
ener*TALK*— processing control	Return Receipt Requested Allow Fragmentation Allow Aggregation Return address Do not forward Discardable	Identifies messaging infrastructure processing directives	Yes
ener*TALK*— routing	*Routing Log*	Identifies each hop in the ener*TALK* message delivery route. Time stamped.	No
ener*TALK*— message priority	*Priority Level*	Indicates message delivery priority.	Yes (default is normal priority)
ener*TALK*— message ID	*Unique Message ID*	Uniquely identifies message	No

Message headers may or may not be integrated with the transport layer. In the case of ener*TALK* over HTTP, the message headers are implemented as custom HTTP headers.

G.4.3 Message payload

The ener*TALK* message payload is dependent on the shared ontology specific to the particular implementation partners in context. It may contain data and commands as defined by the supported ontology.

G.5 Interface services and collaboration agreements

The following services are available to *COMSYS* subsystems:

G.5.1 Business message definitions

While *COMSYS* is capable of supporting multiple message definitions, it is natively equipped to support two primary Business Message families:

a) Command Centric: ener*TALK* generation 2.0 is command centric where each business message has an implied 'subject' and a 'predicate'. This closely resembles a remote procedure call like software implementation where all remote commands must be declared ahead of time and implemented at runtime. An example of a command centric business message is represented by the following message payload extract:

```
<?xml version='1.0'>
< enerTALK version='2.5'>
 <momAction>
  <postData>
    <data>
                <ET-500 date="2003-01-01" timestamp="23:10:36">280</data>
    </data>
  </postData >
 </momAction>
```

```
</ enerTALK >
```

b) Data Centric: ener*TALK* generation 3.0 is data centric where each business message simply broadcasts node specific data and metadata. The consumption of the data is determined by the listening nodes and implemented only at runtime. An example of a data centric business message is represented by the following message payload extract:

```
<?xml version='1.0'>
< enerTALK version='3.0'>
      <data type="time series data" org="testOrg" site="testSite" equip="Generator">
            <ET-500 date="2005-01-01" timestamp="23:10:36">280</data>
    </data>
</ enerTALK >
```

G.5.2 Choreography rules

To be determined as part of the specific agreement. Figure G.3 and Figure G.6 give examples of the sequencing rules of messages to accomplish registration or access and authentication.

G.5.3 Transaction services

G.5.3.1 Reliability

The provisioning of various application level services increases system reliability. This includes but is not limited to the following:

G.5.3.1.1 Message storage and forwarding

COMSYS subsystems shall optionally support message storage and forwarding. This functionality implies that an ener*TALK*-implemented node is capable of local message storage when required and later forwarding of the ener*TALK* message to a final or intermediate message destination. The message forwarding address is parse able from the message header information and reflects the message destination

G.5.3.1.2 Autonomous device operation

COMSYS subsystems are capable of autonomous operation in the absence of a external control. This includes the ability to perform a predefined schedule of commands and operations on a DER device, real time monitoring and local storage of DER device state data, and time drift correction in the absence of a time synchronization authority.

G.5.3.2 Message delivery prioritization

COMSYS is built upon a messaging framework that is used for delivery of system- and user-generated messages between subsystems. Prioritized message delivery in this framework is made possible by providing priority-sensitive message routing, message tagging, and application level preferential processing. Message lifetimes are also managed by lifetime and timestamp tagging at the message level, which are subsequently used for application level lifetime processing

G.5.3.3 Synchronous/asynchronous communication

COMSYS is capable of handling asynchronous messaging. Unique message identification as implemented by ener*TALK* message ID headers are used for downstream message correlation. Time-stamping along with originator identity (*EIP: Return Address Design Pattern*) is used to uniquely identify each message and used for delayed acknowledgement, loop closing and auditing.

G.5.3.4 Timeouts and failure notification

All communication timeouts within *COMSYS* subsystems shall be configurable and defined prior to implementation. Additionally, a configurable list of administrative email addresses may be notified in the event of a system failure. Failure notifications may be toggled on and off and notification logic such as do not notify repeatedly for the same failure may be implemented.

G.5.4 Resource identification

Comprehensive resource identification is possible in *COMSYS* by identifying two complementary attributes of any entity within *COMSYS*, namely:

a) What the resource is, and

b) How it relates to other resources within *COMSYS*.

All resources within a *COMSYS* system are therefore attributed with the following two separate identifiers:

a) Globally unique: *COMSYS* assigns a system wide unique ID for each resource. This is internally referred to as the 'NodeID' and is used for asset permission modeling.

b) Hierarchical identifier: *COMSYS* resources are also attributed a hierarchical identifier which identifies the relationships with other resources. The most commonly used hierarchy comprises of the following elements:

   1) Organization ID

   2) Site ID

   3) Equipment ID

   4) Data Type ID

G.5.5 Resource registration and discovery

Node registration and discovery is provided in *COMSYS* using a common registry authority. The following sequence diagram illustrates a common discovery sequence.

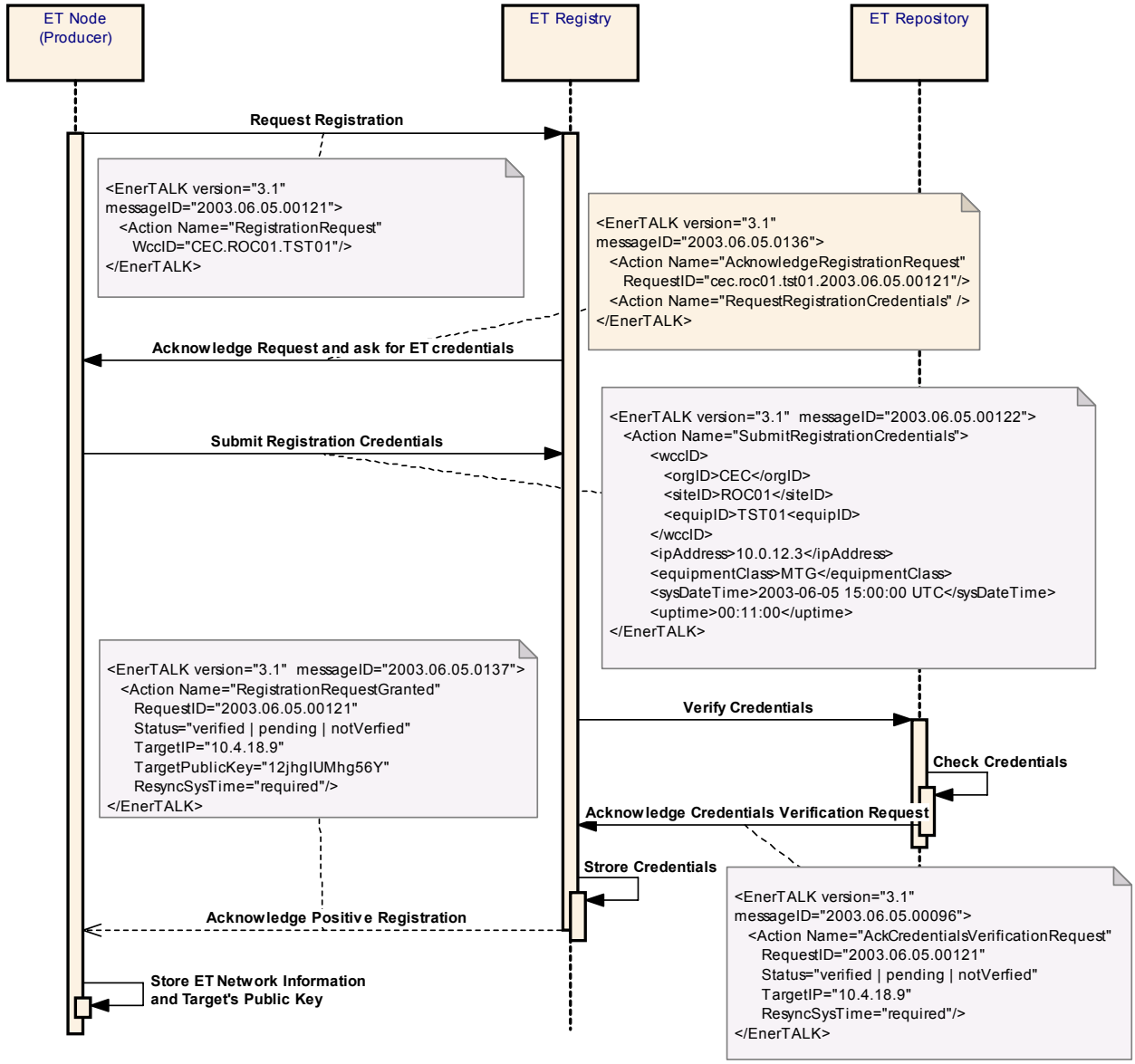


Figure G.3—ener*TALK* discovery

G.5.6 Data and time formats

All time data in ener*TALK* is formatted in accordance with the ISO 8601 standard. References to this can be found at the following location: http://www.w3.org/TR/NOTE-datetime.

G.5.7 Time synchronization

All participant subsystems and nodes in *COMSYS* run under Coordinated Universal Time (UTC) and must be time synchronized to the naval atomic clock or one of its delegates. Top-level *COMSYS* nodes may serve as time authorities using the NTP protocol.

Remote *COMSYS* nodes are also programmed to accommodate for time drift for short durations of time if the top-level time authority is temporarily unavailable.

G.5.8 Security agreement

A comprehensive security approach is adopted in *COMSYS* as defined by DOE—ACCP, CE System Protection Profile (SPP) authored by Sandia Labs (Ref : CEC ACCP spp v0.1.doc). All participants in *COMSYS* must comply with the SPP. Some features of the security approach include the following:

- Layered security
- Multiple sources of authority
- AAA services at the data element level
- Role based security at aggregation levels
- Autonomous operation

The following diagram illustrates the various sources of authority as implemented in ener*TALK*:

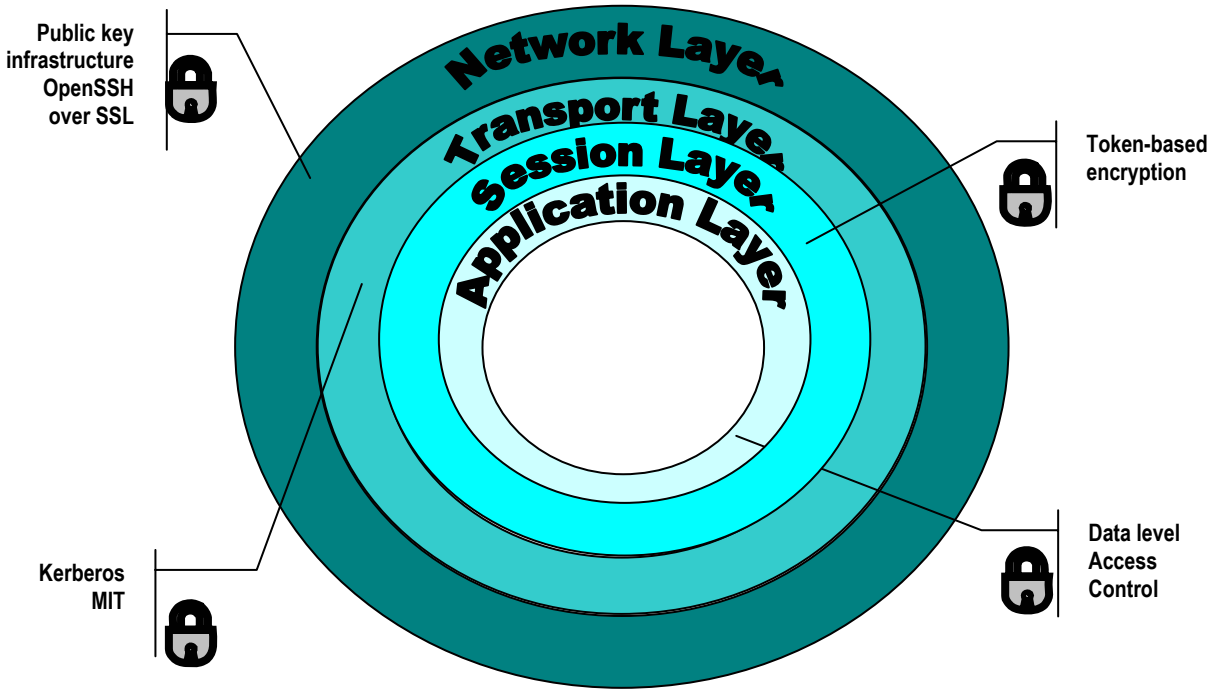


Figure G.4—ener*TALK* security stack

G.5.8.1 Access

COMSYS views are implemented using the ener*VIEW*™ application. The ener*VIEW* security model is a role-based; that is, roles are created and granted permissions, and then these roles are in turn assigned to users or to other roles. Roles can be assigned to roles in chains of unlimited length. If a user is granted a permission via one role and denied that same permission via another role, then the user is considered to have been granted the permission and may perform the action in question. With only a couple exceptions, permissions cannot be granted directly to users. Permissions in the enerVIEW application allow actions to be performed on individual application entities, and most permissions can also be granted for groups of entities. These groups correspond to the hierarchy of organizations, sites, equipment groups, and equipment.

Permissions are grouped into two categories: intransitive and transitive permissions. Intransitive permissions have no object. For example, the "Change Password" permission has no object. A user is simply either allowed or not allowed to change his password. By contrast, a transitive permission does have an object. For example, the "View Screen" permission must be tied to a particular screen. A user may have permission to view screen X but not screen Y.

G.5.8.2 Authentication and authorization

In compliance with the *COMSYS* security policy, node AAA is provided in the following two separate layers:

a) Network Layer: AAA services provided by Kerberos based system. The following diagrams illustrate an AA sequence:

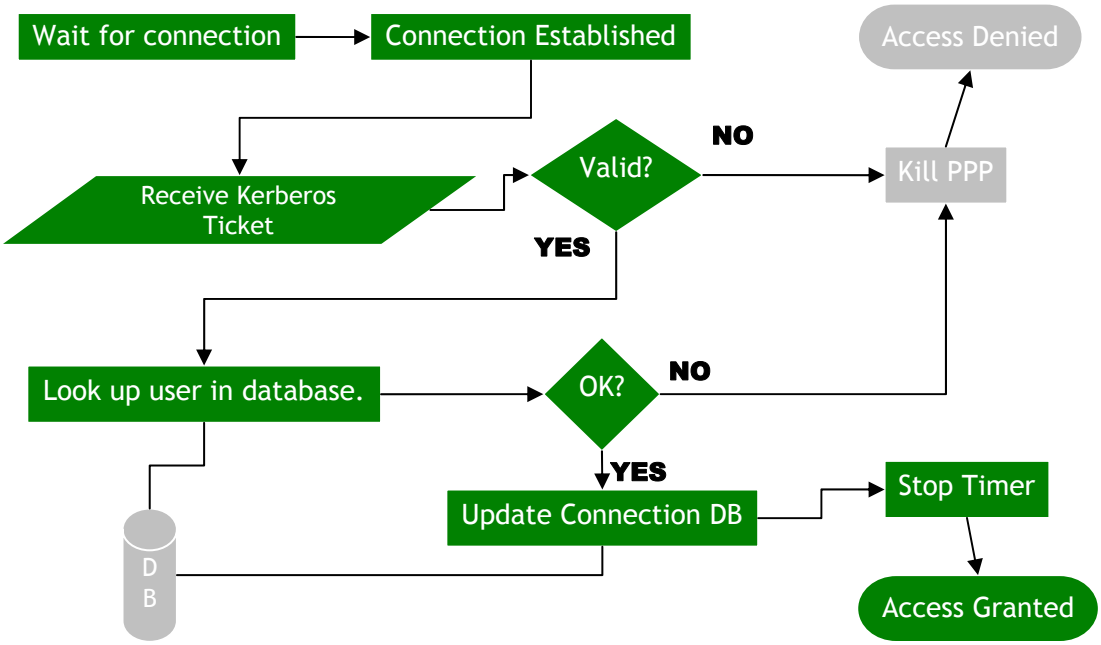


Figure G.5—Server AAA

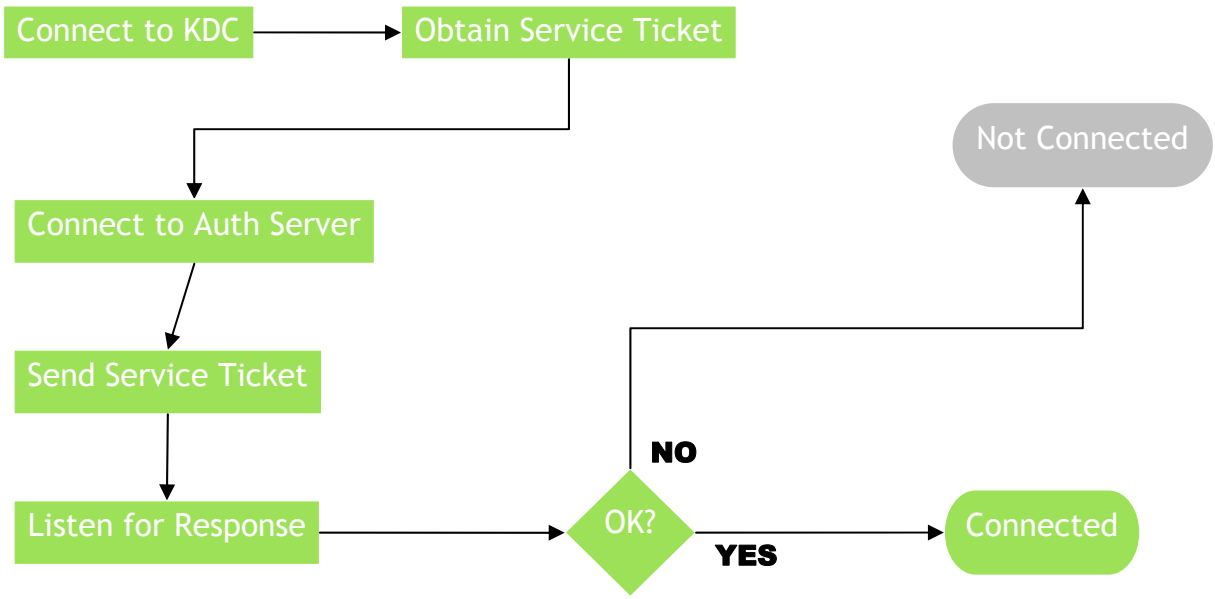


Figure G.6—Client AAA

b) Application Layer: AAA services provided by ener*TALK* based system. Figure G.7 illustrates an AA sequence:

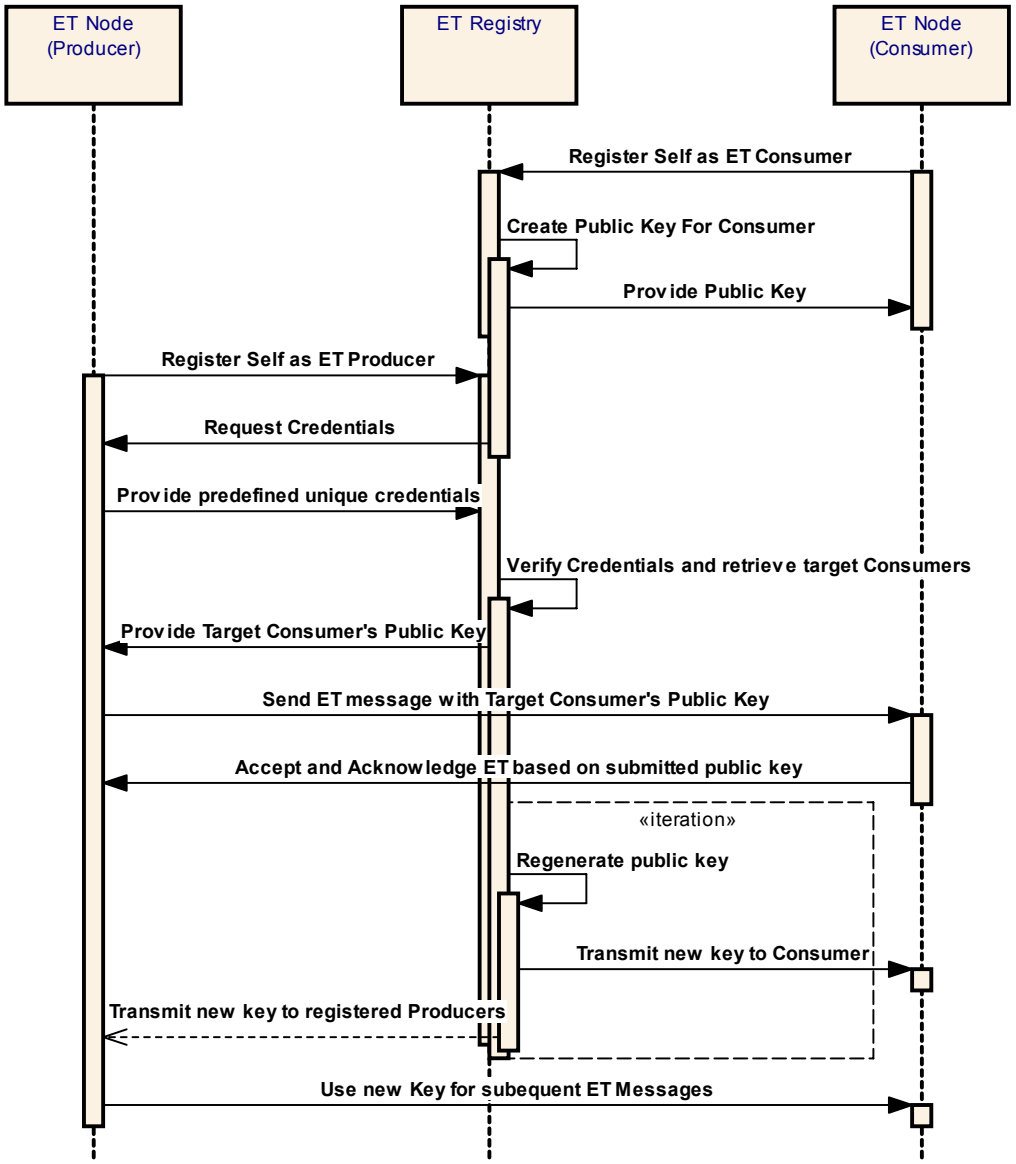


Figure G.7—ener*TALK* AAA

G.5.9 Expected standalone behavior

Each *COMSYS* node must be capable of implementing one or more of the following modes of autonomous operation:

— *Steady-state operation:* COMSYS Nodes can be preconfigured to operate in steady state when a node is disconnected from the network. This steady state may be externally updated once a node reconnects with the network.

— *Scheduled operation: COMSYS* Nodes capable of receiving a predefined schedule of operation which is implemented regardless of network connectivity state.

— *Default operation: COMSYS* Nodes are optionally capable of resorting to a default state if loss of network connectivity is detected. This is most useful for high security nodes where a loss of network connectivity should trigger an immediate shutdown.

G.6 Performance requirements and constraints

G.6.1 Data collection

— DER Monitoring Data is collected at a scan rate of 4 s.

— DER Data may be compressed for local storage.

— A *COMSYS* remote node must be capable of storing 30 days worth of DER monitoring data.

G.6.2 Data storage

— Centralized Data Storage of DER data in *COMSYS* must be capable of storing unlimited data histories.

G.6.3 Data presentation

— *COMSYS* must be capable of displaying real-time monitored data within 15 seconds of collection for real-time connected data sources.

G.7 Communication protocol profile

[http 1.1]

G.8 Version compatibility

To be determined as part of the specific agreement.

G.9 Miscellaneous

None.

G.10 Sample usages*: ener**TALK*** usage examples (version 2.6)*

*Note that the current ener*TALK* version is 3.0.

G.10.1 Posting data from a single source—success state

— ***Use case***: CENTRYwcc™ successfully posting data to mom

— ***Request* ener*TALK***: Sent from CENTRYwcc (CEC.TST01.DEV01) to mom

```
<?xml version='1.0'>
< enerTALK version='2.6'>
  <momAction type="postData" orgID="CEC" siteID="TST01"
                watermark="2003-12-01T10:16:20Z" backlog="8">
     <data equipID="DEV01 alarmCount="1">
```

```
            <ET-500 timestamp=”2003-11-29T23:10:36Z”>280</ET-500>
            <IT-650 timestamp=”2003-01-01T23:10:36Z”>100</IT-650>
            <JT-780 timestamp=”2003-01-01T23:10:36Z”>68</JT-780>
      </data>
  </momAction>
</enerTALK>
```

— ***Response* enerTALK**: Sent from MOM to CENTRYwcc as a response to the HTTP post indicating success

```
<?xml version=’1.0’>
< enerTALK version=”2.6”>
  <wccAction>
    <remoteAction>
      <action name=’tagsProcessed’>3</action>
    </remoteAction>
  </wccAction>
</enerTALK>
```

G.10.2 Posting data—system errors

— ***Use case***: CENTRYwcc unsuccessfully posting data to mom

— ***Request* enerTALK**: Empty ener*TALK* sent from CENTRYwcc to mom

```
<?xml version=’1.0’>
< enerTALK version=’2.5’/>
```

— ***Response* enerTALK**: Sent from mom to CENTRYwcc™ as a response to the HTTP post

```
<?xml version=’1.0’>
< enerTALK version=’2.5’>
  <error errorID=”17”>
    <status>Empty enerTALK submitted</status>
  </error>
</enerTALK>
```

— ***Request* enerTALK**: Sent from CENTRYwcc mom

```
<?xml version=’1.0’>
< enerTALK version=’2.5’>
  <momAction>
```

```
  <postData>
    <data>
            <ET-500 date=”2003-01-01” timestamp=”23:10:36”>280</data>
    </data>
  </postData >
 </momAction>
</enerTALK>
```

— ***Response* enerTALK**: Sent from mom to CENTRYwcc as a response to the HTTP post

```
<?xml version=’1.0’>
< enerTALK >
<xmlError>
  <message>EndElement does not match BeginElement</message>
  <lineNumber>6</lineNumber>
  <linePosition>53</linePosition>
  <source>” 280</data>”</source>
 </xmlError>
</enerTALK>
```

G.10.3 Posting remote action command—success state

— ***Use case***: MOM successfully posting remote action command to CENTRYwcc

— ***Request* enerTALK**: Sent from mom to CENTRYwcc

```
<?xml version=’1.0’>
< enerTALK version=’2.5’>
<remoteAction>
    <action type=’scheduled’ name=’start’ timestamp=’01:01:23’ date=’2003-03-01’ />
    <action type=’scheduled’ name=’reset’ timestamp=’03:02:19’ date=’2003-03-01’ />
  </remoteAction>
 </wccAction>
</enerTALK>
```

— ***Response* enerTALK**: Sent from CENTRYwcc to mom

```
<?xml version=’1.0’>
< enerTALK />
```

G.10.4 Posting remote action command—error state

— ***Use case***: MOM unsuccessfully posting remote action command to CENTRYwcc

— ***Request* ener*TALK***: Sent from mom to CENTRYwcc

```
<?xml version=’1.0’>
< enerTALK version=’2.5’>
<remoteAction>
      <action type=’manual’ name=’start’ />
   </remoteAction>
  </wccAction>
</enerTALK>
```

— ***Response* ener*TALK***: Sent from CENTRYwcc to mom

```
<?xml version=’1.0’>
< enerTALK>
  <error errorID=”21”>
     <status>Unable to start</status>
  </error>
</enerTALK>
```

Appendix A: Sample ener*TALK* schema (version 2.5)*

*Note that the current ener*TALK* version is 3.0.

The following summarizes the ener*TALK* 2.5 schema for command centric messaging over *COMSYS*.

Root element ener*TALK*

Introduction

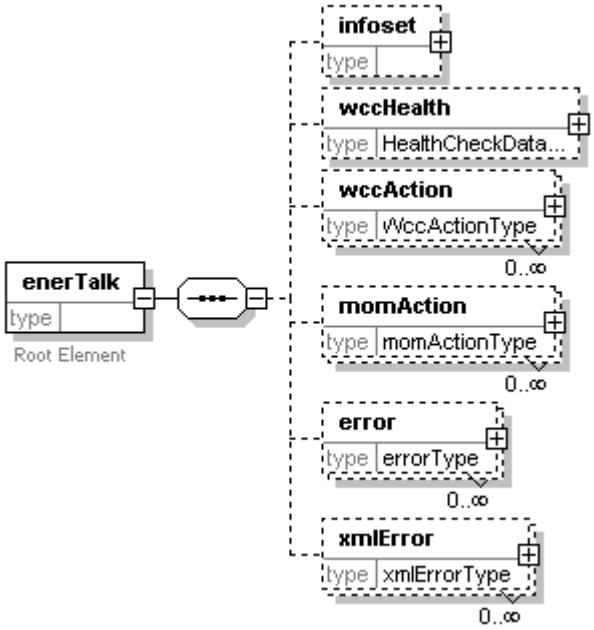
A root element of complex type 'ener*TALK*' is required for the message to be considered valid ener*TALK*. The root element has an optional attribute 'version' to specify the ener*TALK* version. The data type for the 'version' attribute is a double. Default for the version attribute is '1.0'.
Beneath the root element are six optional elements:

- <infoset>—element of complex type for CENTRYwcc identifier and network address.
- <wccHealth>—element of complex type for communicating CENTRYwcc system state with time stamp and an optional error internal identifier.
- <wccAction>—element of complex type for pre-defined commands to be performed internal to the CENTRYwcc or by the CENTRYwcc to affect the device connected to the CENTRYwcc.
- <momAction>—element of complex type for pre-defined commands to be performed by the MOM.
- <error>—element of complex type for the CENTRYwcc and MOM to communicate *EnerTALK* error occurrences within the current *EnerTALK* session.
- <xmlError>—element of complex type for the CENTRYwcc and MOM to communicate XML error occurrences within the current *EnerTALK* session.

Example

< ener*TALK* version="2.6"/>

Diagram



Namespace http://connectedenergy.com/

Children **infoset wccHealth wccAction momAction error xmlError**

Attributes

Name	Type	Use	Default	Fixed	Annotation
version	xs:double	optional	1.0		

Annotation
documentation Root Element

Source

```
<xs:element name="EnerTALK">
 <xs:annotation>
  <xs:documentation>Root Element</xs:documentation>
 </xs:annotation>
 <xs:complexType>
  <xs:sequence>
   <xs:element name="infoset" minOccurs="0">
    <xs:complexType>
     <xs:sequence>
      <xs:element name="deviceInfoset" type="DeviceInfosetType" minOccurs="0"/>
      <xs:element name="wccInfoset" type="WccInfosetType" minOccurs="0"/>
     </xs:sequence>
    </xs:complexType>
   </xs:element>
   <xs:element name="wccHealth" type="HealthCheckDataType" minOccurs="0"/>
   <xs:element name="wccAction" type="WccActionType" minOccurs="0" maxOccurs="unbounded"/>
   <xs:element name="momAction" type="momActionType" minOccurs="0" maxOccurs="unbounded"/>
   <xs:element name="error" type="errorType" minOccurs="0" maxOccurs="unbounded"/>
   <xs:element name="xmlError" type="xmlErrorType" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="version" type="xs:double" use="optional" default="1.0"/>
 </xs:complexType>
</xs:element>
```

Element ener*TALK*/infoset

introduction <infoset> is a complex type element with two optional child elements. Only a single such element is allowed as a child of the root element.

- <deviceInfoset>—element is of complex type 'DeviceInfosetType' with required child elements:
  - <orgID>: no strictly enforced type or string length.

    CEC uses a four-character convention for orgID.
  - <siteID>: no strictly enforced type or string length.

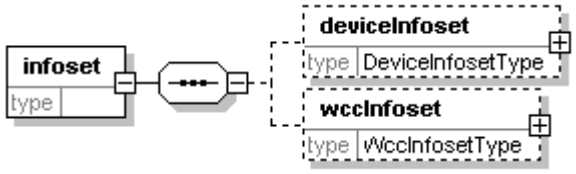
    CEC uses a five-character convention for siteID.
  - <equipID>: no strictly enforced type or string length.

    CEC uses a five-character convention for equipID.
- <wccInfoset>—element is of complex type 'WccInfosetType with required child elements:
  - <ipAddress>: CEC internal IP address assigned to the CENTRYwcc.
  - <hostname>: CEC internal hostname (if any) for the CENTRYwcc.

example

```
<infoset>
  <deviceInfoset>
    <orgID>CEC</orgID>
    <siteID>TST1</siteID>
    <equipID>DEV01</equipID>
  </deviceInfoset>
</infoset>
```

diagram



namespace http://connectedenergy.com/

children **deviceInfoset wccInfoset**

source
```
<xs:element name="infoset" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="deviceInfoset" type="DeviceInfosetType" minOccurs="0"/>
      <xs:element name="wccInfoset" type="WccInfosetType" minOccurs="0"/>
    </xs:sequence>
```

```
    </xs:complexType>
</xs:element>
```

Element ener*TALK* /wccHealth

introduction <wccHealth> is an optional element of complex type *HealthCheckDataType* with child elements:

- <time>: required element. This element is of type xs:date as defined by W3C xsd specifications.
- <systemState>: required element.
- <error>: optional element defined with minimum occurrence of 0 and unbounded maximum occurrences. An unbounded number of these elements may be present as siblings.

Example

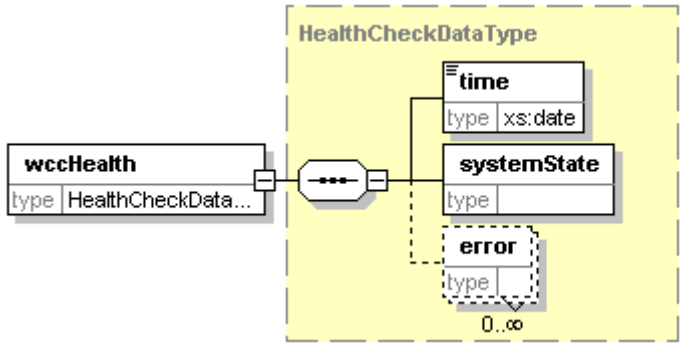
<wccHealth>

<time>2003-03-01T10:09:02</time>

<systemState>ok</systemState>

</wccHealth>

diagram



namespace http://connectedenergy.com/

type **HealthCheckDataType**

children **time systemState error**

Source <xs:element name="wccHealth" type="HealthCheckDataType" minOccurs="0"/>

Element ener*TALK* /wccAction

Introduction <wccAction> is an optional element of complex type *'WccActionType'* defined with minimum occurrence of 0 and unbounded maximum occurrences. This is the element used for dispatching commands to the data source client or to the equipment connected to the data source client.
Each <wccAction> element contains one of two child elements <remoteAction> and <adminAction>:

- <remoteAction>—element for dispatching MOM commands to the connected equipment is of complex type '*RemoteActionType.* This element may contain an unbounded number of child element:
    - <action> - Child element for dispatching MOM commands. This element has required attributes 'type' and 'name' and optional attributes 'timestamp', 'date' & 'timezone', and optional child elements <key> and <value>:
        - 'type'—required attribute with enumerations 'manual' and 'scheduled'.
        - 'name'—this element has enumerations:

          'start' - command to sequence the equipment to "START" state.
          'stop'—command to sequence the equipment to "STOP" state.
          'reset'—command to clear fault or alarm state within the equipment.
          'setPoint'—command to set equipment parameters
        - 'date'—date in any xs:date format. Preferred: "yyyy-mm-dd'
        - 'timestamp'—time in any xs:time format. Preferred: "hh:mm:ss".
        - <key> - optional identifier for the equipment parameter.
        - <value> - optional numeric value for the equipment parameter.
- <adminAction> - element for dispatching MOM commands to the data source client is of complex type '*AdminActionType'*. This element contain child element:
    - <action> - child element with required attributes 'name' and 'value'. The 'name' attribute has enumerations:
        - 'schedulingState—required attribute to specify if the equipment is currently under 'SCHEDULED' or 'MANUAL' operation.

- ‘dropSchedule’—invalidates the current set of scheduled actions within the data source client.

The ‘value’ attribute is of type xs:anySimple type.

examples Setting equipment parameter**:**

```
< enerTALK version='2.5”>
  <wccAction>
    <remoteAction>
      <action type=”manual” name=”setPoint”>
        <key>RT-304</key>
        <value>3</value>
      </action>
    </remoteAction>
  </wccAction>
</ enerTALK >
```

Setting equipment’s scheduling state:

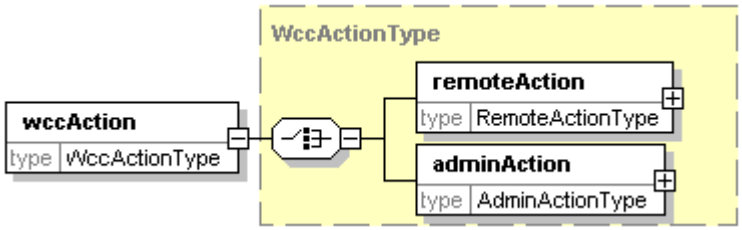
```
< enerTALK version='2.5”>
  <wccAction>
    <adminAction>
      <action name=”schedulingState” value=”manual”/>
    </adminAction>
  </wccAction>
</enerTALK >
```

Setting scheduled actions

```
< enerTALK version='2.5”>
  <wccAction>
    <remoteAction>
      <action type=”scheduled” name=”start” timestamp=’01:01:23’ date=’2003-03-01’/>
      <action type=”scheduled” name=”reset” timestamp=’03:02:19’ date=’2003-03-01’/>
    </remoteAction>
  </wccAction>
```

</ener*TALK*>

diagram



namespace http://connectedenergy.com/

type **WccActionType**

children **remoteAction** **adminAction**

Source <xs:element name="wccAction" type="WccActionType" minOccurs="0" maxOccurs="unbounded"/>

Element ener*TALK*/momAction

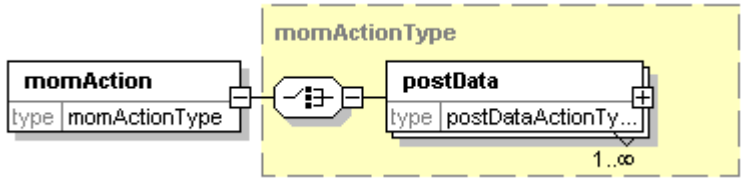
introduction <momAction> is an optional element of complex type ‘momActionType’ defined with minimum occurrence of 0 and unbounded maximum occurrences. This is the element used for posting data from the data source client to the MOM.
Each <momAction> element has a child element <postData> of complex type ‘postDataActionType’:

- <postData>—command for MOM to process the data for posting to data store.
    - <data> - element containing the value for posting to the data store. This element has the required child element of type ‘tagType’ defined in cecDataTypes.xsd with optional attributes ‘alarm’, ‘date’, ‘timestamp’ and ‘timezone’. The tag name for the data to be posted does not follow strictly enforced type or string length. CEC follows the SIE two-letter standard as identifiers.
        - ‘alarm’—optional attribute of type Boolean used to indicate whether data point in question is in alarm condition or not.
        - ‘date’—date in any xs:date format, preferably “yyyy-mm-dd’ for data timestamp.
        - ‘timestamp’—time in any xs:time format, preferably “hh:mm:ss” for data timestamp.
        - ‘timezone’—optional timezone attribute. By default ‘UTC’ is used.

example Posting equipment data:

```
< enerTALK version='2.5”>
  <momAction>
    <postData>
      <ET-500  timestamp=’01:01:23’ date=’2003-03-01’>280</ET-500>
      <IT-650  timestamp=’23:10:36’ date=’2003-03-01’>100</IT-650>
      <JT-780  timestamp=’01:01:23’ date=’2003-03-01’>68</JT-780>
    </postData>
  </momAction>
</enerTALK >
```

diagram



namespace http://connectedenergy.com/

type **momActionType**

children **postData**

source <xs:element name="momAction" type="momActionType" minOccurs="0" maxOccurs="unbounded"/>

Element enerTALK /error

element **enerTALK /error**

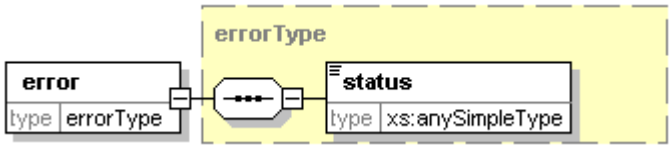
introduction <error> is an optional element of complex type ‘errorType’ defined with minimum occurrence of 0 and unbounded maximum occurrences. This is the element used to identify errors with invalid *EnerTALK*.
Each <error> element has an optional attribute ‘errorID’ and a required child element <status>:

- <status>—child element containing the error message returned.
- ‘errorID’—CEC defined error code to uniquely identify system errors

example

```
< enerTALK/ version='2.5”>
  < error errorID='17”>>
    <status>Empty EnerTALK submitted</status>
  </error>
</enerTALK >
```

diagram



namespace http://connectedenergy.com/

type **errorType**

children **status**

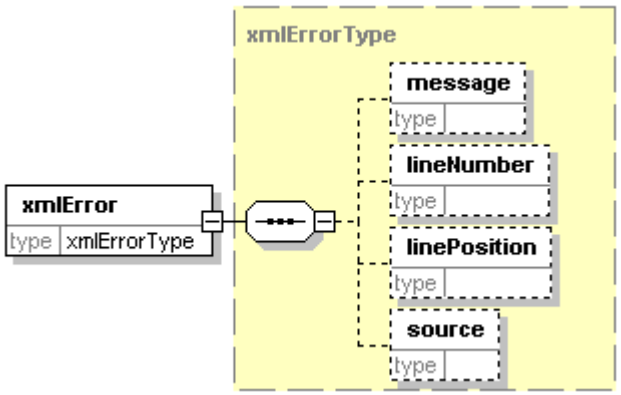
attributes

Name	Type	Use	Default	Fixed	Annotation
errorID	xs:anySimpleType	optional			

source <xs:element name="error" type="errorType" minOccurs="0" maxOccurs="unbounded"/>

Element ener*TALK* /xmlError

diagram



namespace http://connectedenergy.com/

type **xmlErrorType**

children **message** **lineNumber** **linePosition** **source**

source <xs:element name="xmlError" type="xmlErrorType" minOccurs="0" maxOccurs="unbounded"/>

Appendix B: Posting sequences

An ener*TALK* session consists of posting, processing and success/error acknowledgement of an ener*TALK* message. Figure G.8 illustrates the steps involved using an UML Sequence Diagram.

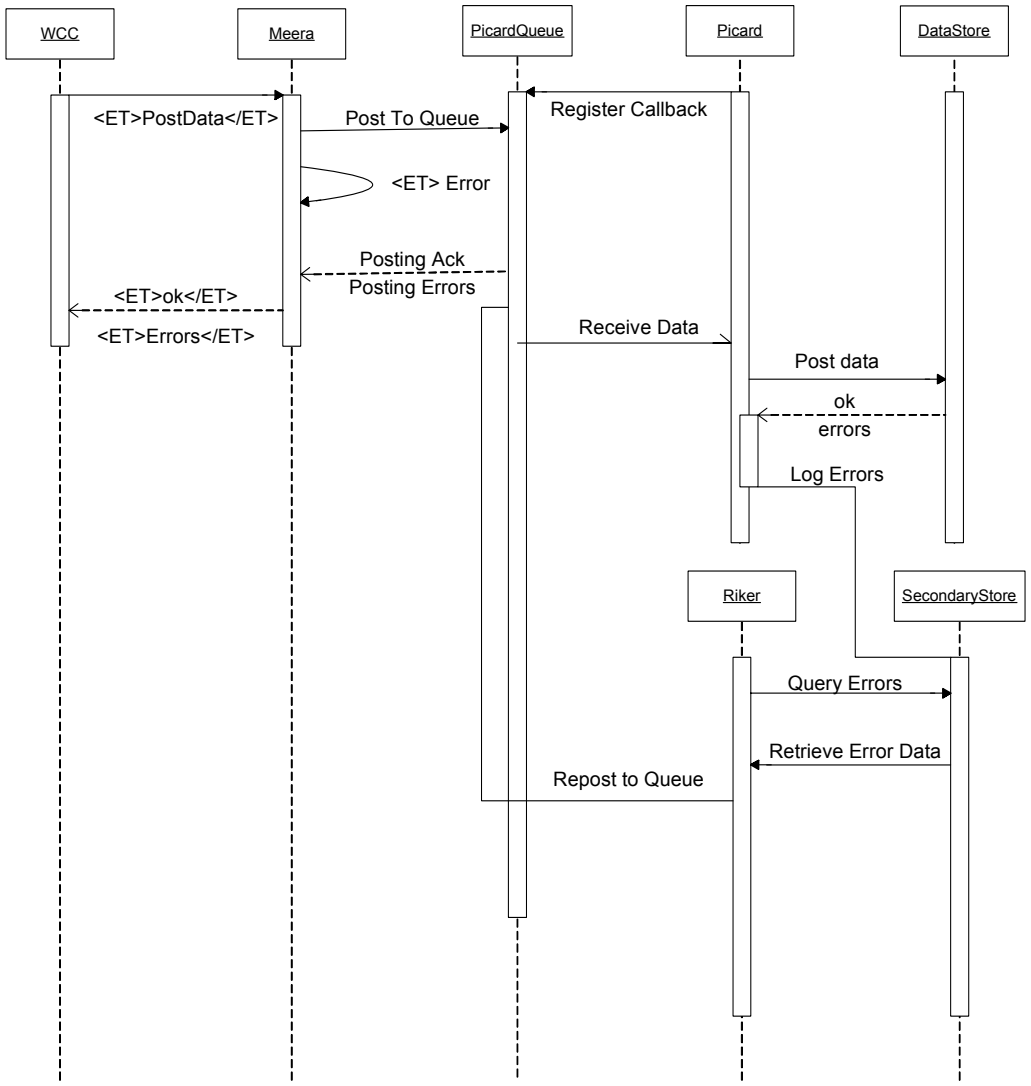


Figure G.8— ener*TALK* sequence diagram

Appendix C: Glossary

— **Node:** A *COMSYS* node is a conceptual entity that encapsulates the behavior of a *COMSYS* consumer. A node must be minimally capable of accepting, parsing, generating and sending *COMSYS* messages. It may optionally be capable of storing, aggregating, forwarding and implementing ener*TALK* defined data and commands. The most common implementation of a *COMSYS* node is Connected Energy's *CENTRY* Web Communication Controller (*CENTRY*wcc) that natively supports the ener*TALK* protocol.

— **CENTRYwcc:** Connected Energy's implementation of a *COMSYS* node.

Appendix D: Useful links

The latest versions of the *COMSYS* system may be available at: http://www.connectedenergy.com

The latest versions of ener*TALK* are available at: http://www. ener*TALK*.com

Annex H

(informative)

Information security issues and guidance

H.1 Overall security process

H.1.1 Five-step security process

Security should be planned and designed into systems from the start. Security functions should be considered an integral part of system design. Planning for security in advance of deployment provides a more complete and cost-effective solution. In addition, advanced planning can ensure that security services are supportable because it may be cost-prohibitive to retrofit adequate security measures into non-planned environments. This means security needs to be addressed at all levels of architecture.

As shown in Figure H.1, security is an evolving process. It is not static. It takes continual work and education to keep security processes up with the demands placed on the system. Security will continue to be a race between corporate security policies/security infrastructure and hostile entities. The security processes and systems will continue to evolve. By definition, no communication-connected systems are 100% secure. There will be always be residual risks that should be taken into account and managed. Thus, to maintain security, constant vigilance and monitoring are needed as is adaptation to changes in the overall environment.

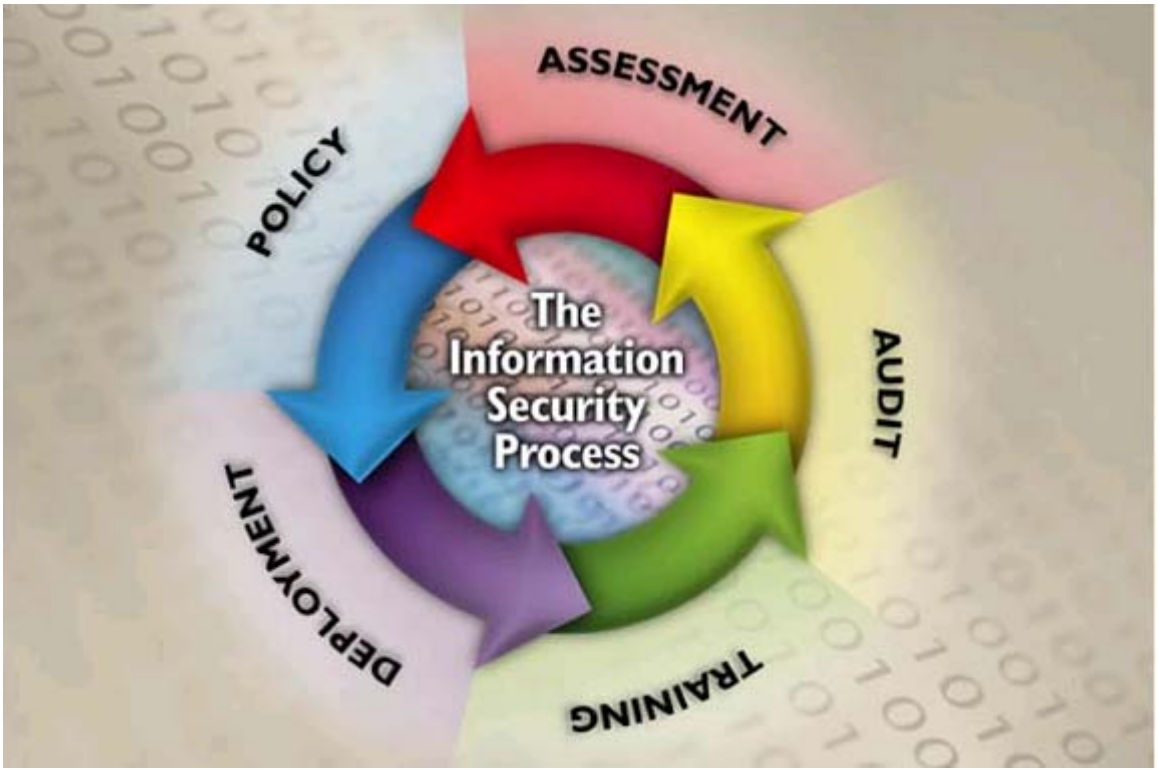


Figure H.1—General security process—a continuous cycle

The following five-step process should be performed continually:

a) Security assessment—A security assessment is a review of assets based on probable risks of attack, the liabilities of a successful attack, and the cost to ameliorate the risks and liabilities. Recommendations lead to the creation of security policies, the procurement of security-related products and services, and the implementation of security procedures. The assessment should take required availability into account because any security approach will likely affect overall performance (e.g., throughput, latency, and reliability) of the communications system. Goals should be set so that implementations reflect required performance.

b) Security policy—Security policies should be created for managing, implementing, and deploying security within a security domain. Policies are developed to ensure that security assessment recommendations are implemented and maintained over time. A commitment to the policy by senior management is critical to the overall success of the program.

c) Security deployment—Security deployment is the purchase and installation of security products and services and the implementation of security policies and procedures to meet the security needs described in the security assessment.

d) Security training—Security training should include training on security threats, security technologies, and corporate and legal policies that affect security as well as the potential effect on availability.

e) Security audit (monitoring)—A security audit should include the processes for the detection of security attacks and breaches and performance assessment of the installed security infrastructure. The concept of an audit is typically applied to post-event/incursion; however, it can be part of the continual evaluation of the security system. In the MIC context, this means maintaining logs of all significant MIC transactions and all changes to the DR security system and analyzing the logs for potential attacks, vulnerabilities, and equipment problems. Monitoring should include measuring critical parameters associated with network performance (e.g., throughput, latency, and reliability) as well as the effect on availability for authorized users performing authorized actions.

Many tools for performing these steps are available for a fee from commercial sources or for free over the Internet. The Internet Site Security Handbook, IETF RFC 2196 [B41] summarizes the security process as follows:

— Identify what you are trying to protect.

— Determine from what you are trying to protect it.

— Determine how likely the threats are.

— Implement measures that will protect your assets in a cost-effective manner.

— Review the process continuously, and make improvements each time.

H.1.2 Security specification rules of thumb

This subclause is an overview of common security rules of thumb for specifying, selecting, designing, and implementing security measures. The reference material contains detailed information for complete specifications.

— Review North American Electric Reliability Council Security Guidelines and Critical Infrastructure Protection 002-009 [B56] to get a good understanding of the issues. However, these documents were not developed with DR as a focus, so some aspects may not be applicable. Therefore, they should be viewed as material from which one can select issues and alternatives that best meet one's needs.

— Develop a security policy that meets the specific needs. Train to it, and enforce it.

— Perform a security risk assessment of assets. Determine the costs (e.g., financial, social, political, legal, and safety) of successful breaches of security for each asset and then determine the cost (including purchase cost, maintenance cost, and "hassle" cost) of implementing different types of security measures to protect the asset. This assessment can be used to determine which security measures (preferably layers of security) should be implemented. There is always a trade-off between the cost to implement security and the possible cost of a breach of security.

— Assess the "hassle" impact of security measures. These can range from irritated personnel to deliberate bypassing of security measures (which leaves the system open to security risk) to malfunctions and serious failures because the security measures themselves prevented access or actions by authorized personnel. "Hassle" is, of course, one aspect of availability, which should be considered in security strategy.

— Determine the security metrics based on the security risk assessment. The success of a security implementation is measured by the estimate of how long and how much it costs to do specified damage to specified assets.

— Use proven, open standards. Security is a complex area. Techniques that appeared to be sound in the past have proved to be flawed under close scrutiny. Open standards allow this scrutiny and have drawn on the range of knowledge and experience gained in areas such as banking and internet services. An example is the use of the IEC 62351 set of security standards [B28] for communication protocols. IEEE Std 802.11i [B34] is another example of the use of open standards for security.

— Security by obscurity (i.e., hiding behind proprietary protocols) is not a good method when the asset is attractive enough for disgruntled employees or industrial espionagers to quickly learn the "obscure" protocol.

— Hide your assets. Techniques are available to make internal IP addresses invisible to the outside network.

— Provide individual and role-based security access control. Provide different levels of data access and control for the various stakeholders.

— Change the default passwords on equipment and systems. Vendors typically have these default passwords installed in the factory so users can quickly access new equipment. All too often, users find it convenient to keep the default password.

— Design for resiliency. Provide multiple layers of security to protect against threats. Use multi-factor methods for identity establishment. Allow for suitable autonomous control to protect against denial-of-service attacks. Provide alternate communication paths for critical information exchanges.

— Design security as an integral part of a system. Security needs to be designed at the system level. For instance, it serves little purpose to encrypt DR data if the data files end up on a public Web server in unencrypted form.

H.2 Basic security concepts

H.2.1 Security requirements, threats, and attacks

Security threats are not just Internet hackers, and security measures are far more than the simple encryption of data. Figure H.2 illustrates the four main security requirements, the types of threats against those requirements, and various attacks that could realize those threats.

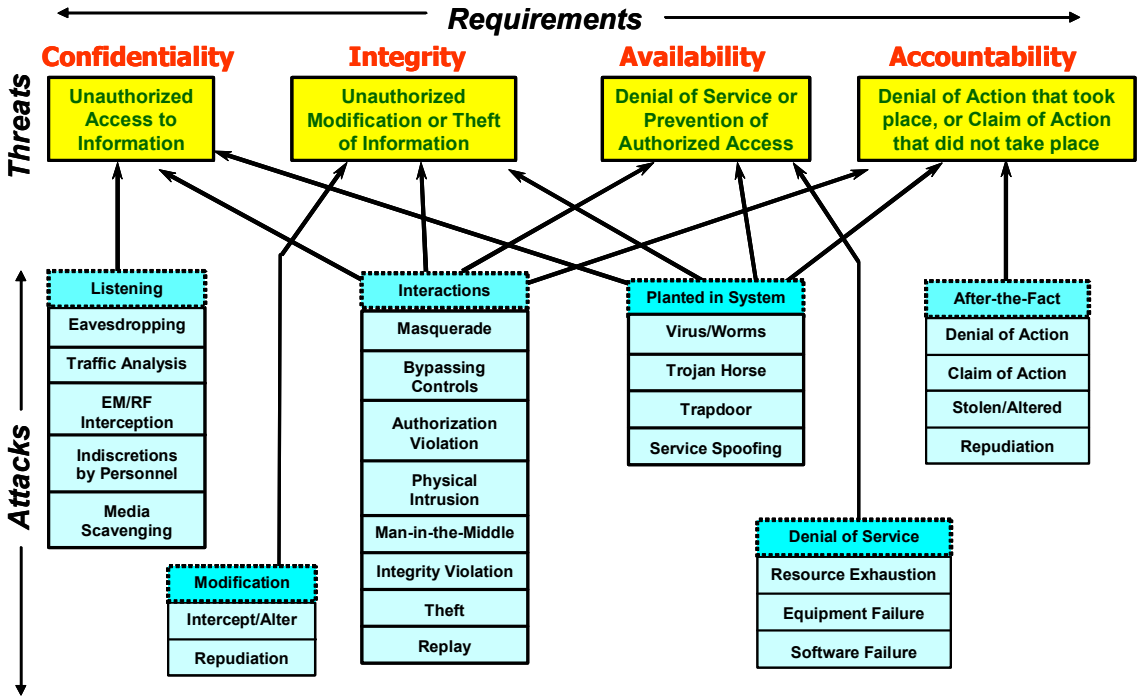


Figure H.2—Security requirements, threats, and attacks

H.2.2 Security categories

From one perspective on security (there are many perspectives, depending on the issues of interest), cyber security can be categorized into four areas (see Figure H.3).

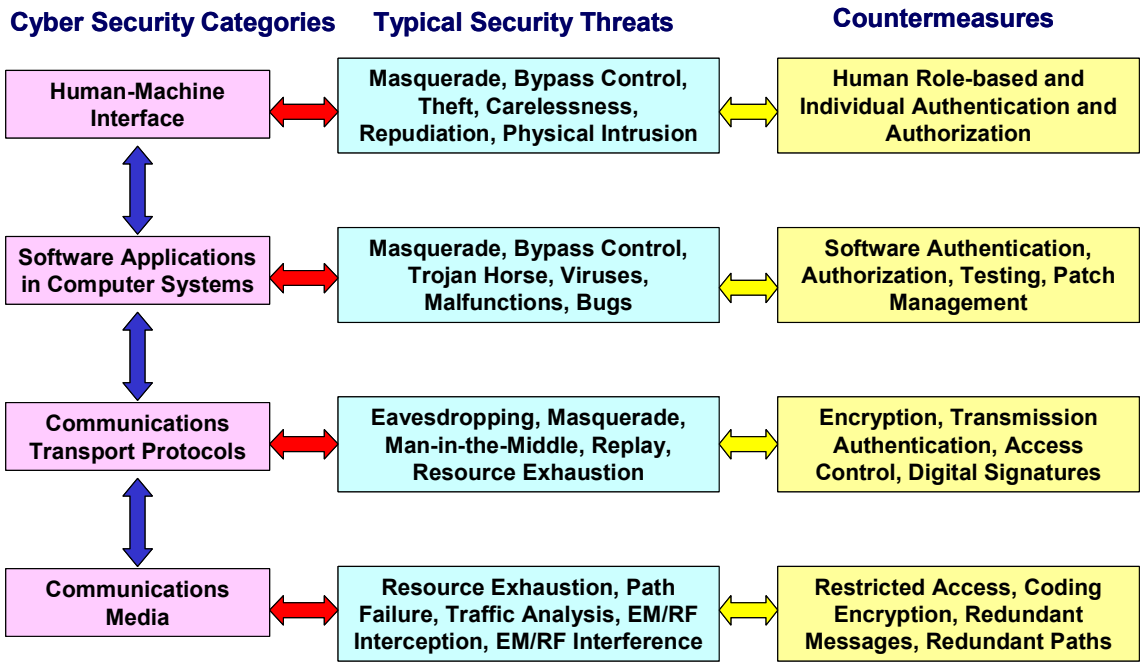


Figure H.3—Security categories, typical threats, and countermeasures

The categories of security needed for a DR device will depend on its application, nameplate rating, and connected loads (all elements related to the risk assessment of the device).

For example, critical power applications such as industrial process control and life support systems require a higher level of security and reliability than small residential photovoltaic systems. Similarly, larger systems have more overall grid effect than smaller systems. Smaller generators cannot afford the high level of security offered by dedicated communication links and may have adequate protection using public media such as the Internet. In general, systems that require only monitoring are less critical than those that require control.

H.2.3 Security policy

Security policies should address the overall criteria and the detailed specifics of the following issues:

- Identity establishment
- Individual and role-based access control
- Security risk assessment of assets for confidentiality, integrity, availability, and non-repudiation (accountability)
- Audit policies and information
- Deployment and equipment
- Access control lists for networks

H.2.4 Security perimeters and security domains

The following definitions apply to security perimeter and domain issues:

— *Electronic security perimeter:* The logical border surrounding a network to which critical cyber assets are connected and for which access is controlled (NAERC CIP 002-009 [B56])

— *Physical security perimeter:* The physical six-wall border that surrounds computer rooms, telecommunications rooms, operations centers, and other locations in which critical cyber assets are housed and for which access is controlled (NAERC CIP 002-009 [B56])

— *Security domain:* The area that organizationally belongs to one section, department, company, or other grouping in which the security requirements are the same (IntelliGrid [B6]).

Many entities, political aspects, and technological choices aggregate into an enterprise. Implementing security at the enterprise level is a daunting task. To simplify analysis, allow various entities to control their own resources. To focus on the important aspects, security can be analyzed in security perimeters and security domains.

In this way, appropriate security policies can be applied for each part of the power system. For example, the DR device can have security policies and procedures managed by the owner in one security domain. The operator of the DR may have other security policies and procedures in another security domain. Each domain has its own internal security policies, but it should also be able to exchange information securely with other domains.

Examples of physical security perimeters include the following:

— The fence around a DR facility

— The building around a control facility

Examples of electronic security perimeters include the following:

— An end-to-end cyber communications link between a DR facility and the operational control facility

— A controlled electronic boundary (e.g., through a firewall) around the network of communications within a DR facility

Examples of security domains are as follows:

— DR owner facilities

— The utility control center

— Telecommunication provider equipment covered under a service level agreement

The following list is a subset of security services that a security domain should define and implement:

— Security policy: As described above

— Security management infrastructure: The elements and activities that support security policy by monitoring and controlling security services and mechanisms distributing security information and reporting security events

— Access control: The prevention of unauthorized use of resources or information

— Trust: A device or entity will behave exactly as expected (Layered security, as described in most guides, recommends that trust always be limited.)

— Confidentiality: Information will not be made available to unauthorized parties

— Integrity: To prevent information from being modified or otherwise corrupted maliciously or accidentally

— Auditing

— Training

Different security requirements will be required for intra-domain and inter-domain communications.

H.2.5 Identity establishment

The identity of a user (human or software application) can be established many ways. In general, it is recommended that multiple factors be used for identity establishment (e.g., a smart card in combination with a combination keypad for physical access to a DR site or a combination of username/password and address resolution for communications access).

Many mechanisms are available to establish identity. These include the following:

- Challenge/response—The remote user requests a challenge and then converts this via a secret algorithm to a response, which is returned to the DR device for validation.
- Username/password—This is a typical mechanism employed by Web-based and maintenance interfaces. Fixed passwords are a potential threat either through publication or caching in Web interfaces. A challenge-response scheme is therefore recommended. Equipment should set an alarm or inhibit operation if default passwords are in use. The challenge-response should be on an individual basis (e.g., no group-assigned passwords). A good rule of thumb is that passwords should have a minimum of seven characters and included uppercase, lowercase, punctuation, and numeric characters.
- Address resolution—This is a useful technique, but it can be easily attacked (by address spoofing). Therefore, address resolution should not be used on its own.
- Smart cards —These can be used in the implementation of physical security. See ISO 7816 [B52] and the Java Card Platform Specification. A combination of a smart card and a numeric key is often recommended for physical access control and auditing.
- Digital certificates—These assert identity using public key encryption techniques. The industry-accepted standard is X.509. (See IETF RFC 2527 [B45].)
- Digital signatures—These ensure that the message content and the identity of the sender are correct. (See IETF RFC 2313 [B42].)
- Biometric identification—This is useful for physical authentication. This area is presently undergoing rapid development.
- Single sign on service—This relieves an entity having successfully completed the act of authentication once from having to re-authenticate for subsequent accesses for some reasonable period of time.
- Account names and privileges—Default user accounts should be removed or a least have their credentials (e.g., passwords) changed. This should include all user accounts, including remote diagnostic accounts.

H.2.6 Confidentiality

Confidentiality is assurance that information is not disclosed to unauthorized persons, processes, or devices. Confidentiality can be provided by encryption or transmission over a secure infrastructure.

The recommended standard for DR encryption is the Advanced Encryption Standard (IETF RFC 3268 [B48]). With the current Internet, secure infrastructure can be provided with VPN (IPSEC IETF RFC 1826 [B39] and IETF RFC 1827 [B40]) and Encapsulating Security Payload (IP Encapsulating Security Payload—IETF RFC 1827 [B40] and IETF RFC 2406 [B44]) technologies.

H.2.7 Information integrity

Information integrity ensures unauthorized changes or deletions made to messages may be detected by the recipient.

To provide message integrity, an algorithm that generates a result similar to a cyclic redundancy code needs to executed and imbedded in the message. However, this alone will not guarantee integrity, as a man-in-the-middle attack could change the message, recalculate the cyclic redundancy code, and then forward the message.

To prevent this, a digital signature is typically used on the cyclic redundancy code-like result, and both are embedded in the message. It is this digital signature "seal" that actually prevents the attack. Such signatures are typically referred to as message authentication codes. Similar tools are available to detect breaches in the integrity of files.

H.2.8 Accountability/non-repudiation

Accountability is the capability to uniquely trace the actions of an individual or software application to that entity. Non-repudiation is one aspect of accountability and is the ability to provide proof that a given exchange action has or has not occurred. This is used to resolve disputes with other entities that claim the action did not occur. To provide this service, a strong audit service should be present. Non-repudiation is part of an overall requirement for accountability.

H.2.9 Auditing

Audit information involves logging events such as MIC transactions and changes to a DR security system. Audit information can be used to discover hostile attacks, analyze equipment failures, determine vulnerabilities, establish accountability and non-repudiation, assess damage, and recover a system after a failure or attack. In addition to standard logging, a mechanism should be implemented to ensure the integrity of audit logs and detect tampering with transferred audit records.

Audit information should be archived and thus available for specified periods of time because it can be used for detection and forensic analysis of possible security attacks. For example, upon revocation of a security certificate, a mechanism could detect and indicate that revoked credential has been used. Auditing can also be used to analyze non-repudiation and accountability issues.

Audit trails could also span more than one security domain to ensure coordinated analysis. In particular, coordinated and secure timestamp and time representation, such as ISO/IEC 18014-1 [B51] and UTC time, should be used for audit records to allow the creation of an appropriately time-sequenced audit trail.

H.2.10 Intrusion detection

Intrusion detection is the process of determining that an unauthorized interaction has occurred. The prevention of physical intrusions requires locks, gates, smart cards, and other mechanisms.

The prevention of cyber intrusions requires mechanisms and tools that can detect that such an intrusion has taken place. Audit logging and archiving of data can capture the interactions. Then, tools can analyze these records. For instance, pattern recognition can be used to determine if anomalies in communications interactions have occurred, although the intent cannot be determined.

Passive intrusion (eavesdropping) is difficult if not impossible to detect. It could be prevented by encryption and secure communications infrastructure.

H.2.11 Discovery of security services

A security domain should provide a mechanism for an entity (human or software application) to discover what security services are available for its use. This could be a manual method or an electronic mechanism.

H.2.12 Firewalls

Firewalls are deployed to protect critical infrastructure computational resources and should be deployed at electronic security perimeter connectivity points. Firewalls depend on maintenance of the internal filters (e.g., access control lists). Neglect here will result in reduced, not improved, security.