

**57/525/CDV****COMMITTEE DRAFT FOR VOTE (CDV)
PROJET DE COMITÉ POUR VOTE (CDV)**

		Project number Numéro de projet		IEC 61968-1 Ed. 1.0	
IEC/TC or SC: TC 57 CEI/CE ou SC:		Date of circulation Date de diffusion		Closing date for voting (Voting mandatory for P-members) Date de clôture du vote (Vote obligatoire pour les membres (P)) 2001-10-05	
		2001-05-04			
Titre du CE/SC: Conduite des systèmes de puissance et communications associées			TC/SC Title: Power system control and associated communications		
Secretary: Dr. Andreas Huber, Germany Secrétaire:					
Also of interest to the following committees Intéresse également les comités suivants			Supersedes document Remplace le document 57/443/CD - 57/510/CC		
Horizontal functions concerned Fonctions horizontales concernées					
<input type="checkbox"/> Safety Sécurité		<input type="checkbox"/> EMC CEM		<input type="checkbox"/> Environment Environnement	
				<input type="checkbox"/> Quality assurance Assurance qualité	

CE DOCUMENT EST TOUJOURS A L'ETUDE ET SUSCEPTIBLE DE MODIFICATION.
IL NE PEUT SERVIR DE REFERENCE.

LES RECIPIENDAIRES DU PRESENT DOCUMENT SONT INVITES A PRESENTER,
AVEC LEURS OBSERVATIONS, LA NOTIFICATION DES DROITS DE PROPRIETE
DONT ILS AURAIENT EVENTUELLEMENT CONNAISSANCE ET A FOURNIR UNE
DOCUMENTATION EXPLICATIVE.

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT
SHOULD NOT BE USED FOR REFERENCE PURPOSES.

RECIPIENTS OF THIS DOCUMENT ARE INVITED TO SUBMIT, WITH THEIR
COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH
THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Titre :

**Système d'interfaces pour la gestion de la
distribution –Partie 1 : Architecture des
interfaces et spécifications générales**

Title :

**System interfaces for distribution management –
Part 1: Interface architecture and general
requirements**

Note d'introduction

Introductory note

ATTENTION

**CDV soumis en parallèle au vote (CEI)
et à l'enquête (CENELEC)**

ATTENTION

Parallel IEC CDV/CENELEC Enquiry

INTERNATIONAL ELECTROTECHNICAL COMMISSION

System Interfaces For Distribution Management –

Part 1: Interface Architecture and General Requirements

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a world-wide organization for standardization comprising all national Electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61968-1 has been prepared by Working Group 14, of IEC technical committee 57: Power System Control And Associated Communications. IEC 61968 is a series of standards:

IEC 61968 Part	Title
1.	Interface Architecture And General Requirements
2.	Glossary
3.	Interface Standard For Network Operation
4.	Interface Standard For Records And Asset Management
5.	Interface Standard For Operational Planning And Optimisation
6.	Interface Standard For Maintenance And Construction
7.	Interface Standard For Network Extension Planning

- | | |
|-----|--|
| 8. | Interface Standard For Customer Inquiry |
| 9. | Interface Standard For Meter Reading And Control |
| 10. | Interface Standard For Systems External To, But Supportive Of, Distribution Management |
| 11. | Distribution Information Exchange Model (DIEM) |

The text of this standard is based on the following documents:

FDIS	Report on voting
57/274/NP	57/294/RVN

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

CONTENTS

	Page
FOREWORD.....	2
Introduction.....	6
1 Scope	10
2 Normative references.....	10
3 Interface Reference Model.....	11
3.1 Domain	11
3.2 Business Functions.....	11
3.3 Interface Reference Model.....	12
3.3.1 Network operation (NO)	13
3.3.2 Records and asset management (AM)	14
3.3.3 Operational planning and optimisation (OP)	15
3.3.4 Maintenance and construction (MC).....	15
3.3.5 Network extension planning (NE)	16
3.3.6 Customer Support (CS).....	16
3.3.7 Meter reading and control (MR)	16
3.3.8 External to DMS (EXT).....	17
4 Interface Architecture.....	19
4.1 Requirements Analysis Methodology	19
5 Interface Profile	19
5.1 Components	20
5.2 Component Adapters	21
5.3 Interface Specification	22
5.4 Middleware Adapter	23
5.5 Middleware services	24
5.6 Communication services	25
5.7 Platform Environment	25
6 Information Exchange Model.....	26
6.1 General Requirements	26
6.2 IEM Management Related services	26
7 Component Reporting And Error Handling	28
7.1 Error Message Handling	28
8 Security and Authentication	29
8.1 Security Threats	29
8.2 Security Functions	30
8.3 Management of Integrity and Security	31
8.3.1 Levels of Immunity.....	31
8.3.2 Levels of Security	31
8.4 Security Agent	31
9 Maintenance aspects	33

Tables

Table 1: Document Overview for IEC 61968 - Part 1	9
Table A.1: Examples of data exchange in a company environment.....	35
Table A.2: Data Categories	36
Table B.1: Example steps in a Use Case (From Use Case 46: Data Acquisition for External EMS)	51
Table B.3: Information Model (From Use Case 46: Data Acquisition for External EMS)	54
Table B.5: Commonly used verbs	56
Table C.1: Typical Load Scenario.....	62
Table C.2: Example of typical transaction volume for DMS	63

Figures

Figure 1: Distribution Management System with IEC 61968 compliant interface architecture ...	6
Figure 2: Example Utility Implementation Of IEC 61968	8
Figure 3: Typical Applications Mapped to Interface Reference Model	12
Figure 4: Overview of the Interface Profile and Corresponding Sub-Clause Numbers	20
Figure A.1: Hierarchy of complexity in a system environment	34
Figure A.2: General utility structure	35
Figure B.1A: Process 1A: IEC TC57 Working Group 14 Process For Developing IEC 61968 Parts 3-11	39
Figure B.1B: Process 1B: (Continuation) IEC TC57 Working Group 14 Process For Developing IEC 61968 Parts 3-11	40
Figure B.2A: Process 2A: Typical business sub-functions of DMS and external systems	41
Figure B.2B: Process 2B: (Continuation) An Overview Of An Utility's Application Of The IEC 61968 Standard	42
Figure B.3A: Typical Components Of Major DMS Business Functions	44
Figure B.3B: Typical Components of the Major DMS Business Functions	45
Figure B.4: Use Case Template	48
Figure B.6: Message Data Model Example (From Use Case 46: Data Acquisition for External EMS)	59
Figure B.7 - CIM Top Level Package	60
Figure D.1: Database views depend on the time and user	65
Figure E.1: Map of Typical utility systems to the business functions of the IRM	67

Annexes

A: Distribution Management Domain	34
B: IEC 61968 Series Of Standards Development Process	38
C: Inter-Application Integration Performance Considerations	62
D: Views Of Data In A Conventional Electric Utility	64
E: Business Functions	67

IEC 61968

System Interfaces for Distribution Management – Part 1: Interface Architecture and General Requirements

Introduction

The IEC 61968 series is intended to facilitate *inter-application integration*, as opposed to *intra-application integration*, of the various distributed software application systems supporting the management of utility electrical distribution networks. Intra-application integration is aimed at programs in the same application system, usually communicating with each other using middleware that is embedded in their underlying runtime environment, and tends to be optimized for close, real-time, synchronous connections and interactive request/reply or conversation communication models. IEC 61968, by contrast, is intended to support the inter-application integration of a utility enterprise that needs to connect disparate applications that are already built or new (legacy or purchased applications), each supported by dissimilar runtime environments. Therefore, IEC 61968 is relevant to loosely coupled applications with more heterogeneity in languages, operating systems, protocols and management tools. IEC 61968 is intended to support applications that need to exchange data on an event driven basis. IEC 61968 is intended to be implemented with middleware services that broker messages among applications, will complement, not replace utility data warehouses, database gateways, and operational stores.

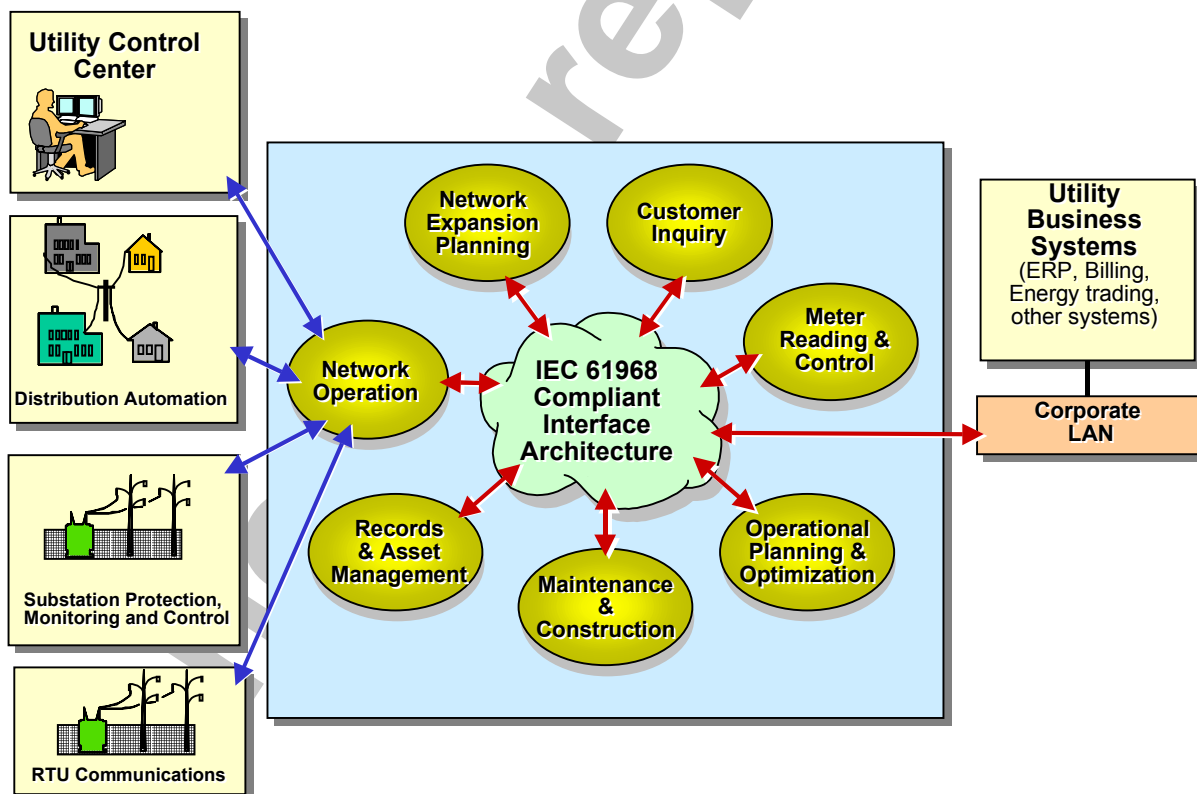


Figure 1: Distribution Management System with IEC 61968 compliant interface architecture

Figure 1 clarifies the scope of IEC 61968-1 graphically in terms of business functions and shows a Distribution Management System with IEC 61968 compliant interface architecture.

As used in IEC 61968, a DMS consists of various distributed application components for the utility to manage electrical distribution networks. These capabilities include monitoring and control of equipment for power delivery, management processes to ensure system reliability, voltage management, demand-side management, outage management, work management, automated mapping and facilities management. Standards interfaces are to be defined for each class of applications identified in the Interface Reference Model (IRM), which is described in Clause 4.

IEC 61968 recommends that system interfaces of a compliant utility inter-application infrastructure be defined using Unified Modelling Language (UML).

The eXtensible Markup Language XML is a data format for structured document interchange particularly on the Internet. One of its primary uses is information exchange between different and potentially incompatible computer systems. XML is thus well-suited to the domain of System Interfaces for Distribution Management.

Where applicable, Parts 3 to 10 of this standard will define the information required for '*message payloads*'. *Message Payloads* will be formatted using XML with the intent that these payloads can be loaded on to messages of various messaging transports, eg OAG, SOAP etc. The XML encoding rules will be covered in Part 11.

Communication between application components of the IRM requires compatibility on two levels:

- Message formats and protocols.
- Message contents must be mutually understood, including application-level issues of message layout and semantics.

Clause 5 defines abstract middleware services required to support communication between the applications defined in the IRM. These services are intended to be deployed, with little additional software required, by mapping them to commonly available services from various messaging technologies including middleware such as Message Brokers, Message Oriented Middleware (MOM), Message-Queuing Middleware (MQM), and Object Request Brokers (ORBs). This clause is organized as follows:

- Sub-clause 5.1 identifies general requirements of the applications identified in the IRM.
- Sub-clause 5.2 describes how standard information exchange services may either be invoked directly from an application (native mode) or that software may be used to map (adapt) an application to the information exchange services.
- Sub-clause 5.3 identifies standard services required for applications to exchange information with other applications.
- Sub-clause 5.4 describes how information exchange services may either be supported directly by middleware or that software may be required to map (adapt) the utility's middleware services to the standard information exchange services.
- Sub-clauses 5.5 to 5.7 describe environmental requirements for information exchange.

An Example Using IEC 61968

An example of a typical utility's implementation of IEC 61968 is provided in figure 2. In this example, the utility has used *Interface Adapters* as a means to integrate many of its legacy systems with other application systems that are IEC 61968 compliant. Note those legacy systems and IEC 61968 compliant systems both continue to use proprietary integration techniques among their internal applications; only information that needs to be exchanged among applications at the utility enterprise level is expected to use IEC 61968 middleware services.

For purposes of this example, assume that the utility's Outage Management System (OMS) already has the capability to issue controls to and gather device states from the Distribution Automation System (DAS). As it is working acceptably for the utility, this interface does not need to be changed. However, because other applications need to be notified when distribution devices change state, the DAS publishes state changes through middleware services. Another benefit of publishing events is that they can be recorded by an event history application in a data store; this data can then be used in the generation of various types of reports. As much of the information exchanged among these systems is useful for management decision support, a data warehouse application has also been connected to the IEC 61968 middleware services so that it may receive published information.

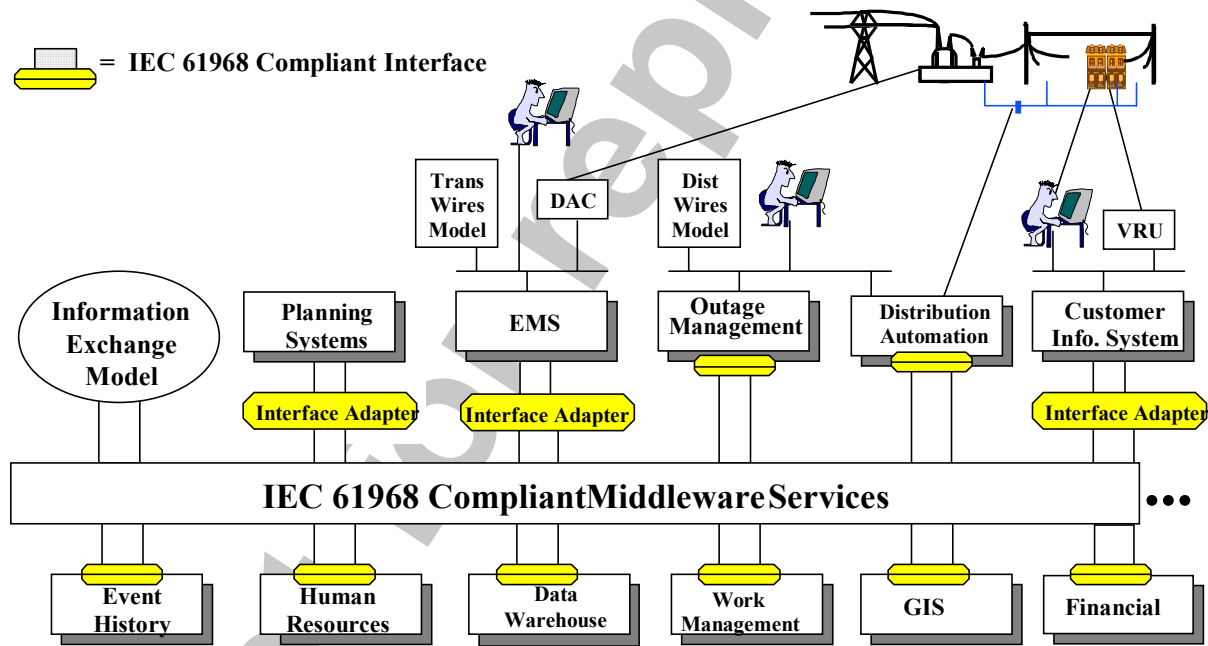


Figure 2: Example Utility Implementation Of IEC 61968

The organization of IEC 61968-1 is described in table 1.

Clause	Title	Purpose
1.	Scope	Scope of IEC 61968, Part 1.
2.	Normative References	Documents that contain provisions which, through reference in this text, constitute provisions of this International Standard.
3.	Interface Reference Model	The domain relevant to IEC 61968 is described. For each relevant business function, a list of abstract components is provided, which is described by the functions performed by the component. IEC 61968 Parts 3-10 define interfaces for these abstract components.
4.	Interface Architecture	The Interface Reference Model for utility inter-application integration is provided along with the rationale for its structure.
5.	Interface Profile	Utility inter-application integration environmental requirements are described. Abstract message passing services are defined that must be available for applications to communicate information to other applications, including publish and subscribe services.
6.	Information Exchange Model	Metadata is used to describe event types that are published by applications. Applications subscribing to receive all messages for a certain event type recognize the fields of a particular event message once they have looked up the metadata for the event type in the Information Exchange Model. While many event types are described in the IEC 61968 series of standards, metadata is the means by which vendors and utilities can add new event types without violating this standard.
7.	Component Reporting And Error Handling	Requirements for audit trails and error message handling authentication necessary to support utility inter-application integration are described.
8.	Security and Authentication	Requirements for security and authentication necessary to support utility inter-application integration are described.
9.	Maintenance Aspects	General maintenance requirements are specified.
Informative Annex A	Distribution Management Domain	An overview of business functions required for electric utility distribution management is described.
Informative Annex B	IEC 61968 Series Of Standards - Development Process	The methodology used to determine interface architecture requirements for utility inter-application integration is described.
Informative Annex C	Inter-Application Integration Performance Considerations	Some typical performance requirements necessary to support utility inter-application integration are described. These requirements are of a general nature as specific implementation requirements will vary by utility.
Informative Annex D	Views of Data in a Conventional Electric Utility	This annex describes some of the underlying principles of defining the reference data dictionary of Part 11.
Informative Annex E	Business Functions	This annex describes the typical data producer and consumer subsystems for each DMS Business Function.

Table 1: Document Overview for IEC 61968 - Part 1

1 Scope

This standard, IEC 61968-1, is the first in a series that, taken as a whole, define interfaces for the major elements of an interface architecture for Distribution Management Systems (DMS). This standard, referred to as Part 1, identifies and establishes *requirements for standard interfaces* based on an Interface Reference Model (IRM). Subsequent parts of this standard are based on each interface identified in the IRM. This set of standards is limited to the definition of interfaces and is implementation independent. They provide for interoperability among different computer systems, platforms, and languages. Methods and technologies used to implement functionality conforming to these interfaces are considered outside of the scope of these standards; only the interface itself is specified in these standards.

As used in IEC 61968, a DMS consists of various distributed application components for the utility to manage electrical distribution networks. These capabilities include monitoring and control of equipment for power delivery, management processes to ensure system reliability, voltage management, demand-side management, outage management, work management, automated mapping and facilities management. The IRM is specified in Clause 4.

2 Normative references

The following normative documents contain provisions that, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 61970-301: CD 1999, Energy Management System Application Program Interface (EMS API) – Common Information Model (CIM)

3 Interface Reference Model

3.1 Domain

Within this document, the Distribution Management domain covers all aspects of management of utility electrical distribution networks. A distribution utility will have some or all of the responsibility for monitoring and control of equipment for power delivery, management processes to ensure system reliability, voltage management, demand-side management, outage management, work management, automated mapping and facilities management.

The Distribution Management domain may be organised as two inter-related types of business, Electricity Supply and Electricity Distribution. Electricity Supply is concerned with the purchase of electrical energy from bulk producers for sale to individual consumers. Electricity Distribution covers the management of the physical distribution network that connects the producers and consumers. In some countries, the responsibility of organisations may be legally restricted and certain sections of the standard will be inapplicable.

A utility domain includes the software systems, equipment, staff and consumers of a single utility organisation, which could be a company or a department. It is expected that within each utility domain, the systems, equipment, staff and consumers can be uniquely identified. When information is exchanged between two utility domains, then identifiers may need extending with the identity of the utility organisation in order to guarantee global uniqueness.

3.2 Business Functions

Various departments within a utility co-operate to perform the operation and management of a power distribution network; this activity is termed Distribution Management. Other departments within the organisation may support the Distribution Management function without having direct responsibility for the distribution network. This segmentation by business function¹ is provided in the Interface Reference Model (IRM), which is described in detail in sub-clause 3.3.

The use of a business-related model should ensure independence from vendor-produced system solutions. It is an important test of the viability of this standard that the IRM be recognisable to utility staff as a description of their own distribution network operation and management.

Major utility business functions, which provide the top level categories of the IRM, are shown in figure 3 below.

¹ The work of the CIRED Working Group on Distribution Automation, published in 1996, is fully acknowledged in the segmentation.

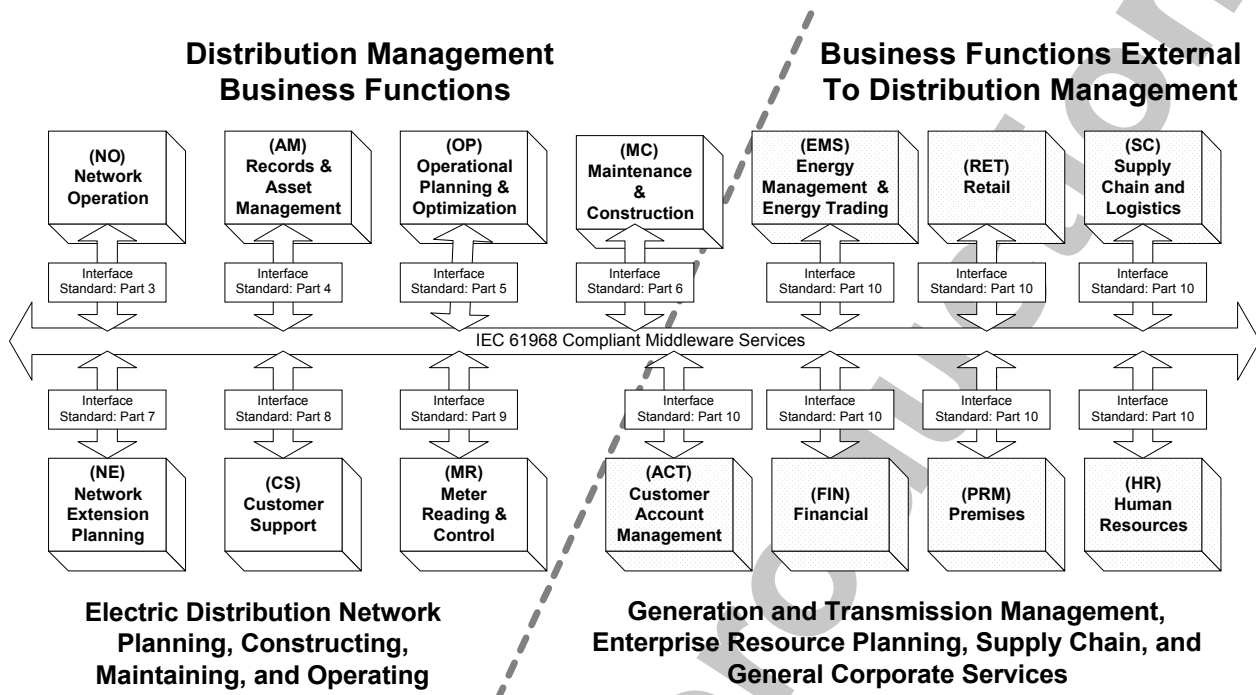


Figure 3 Typical Applications Mapped to Interface Reference Model

3.3 Interface Reference Model

It is not the intention of this standard to define the applications and systems that vendors should produce. It is expected that a concrete (physical) application will provide the functionality of one or more abstract (logical) components as listed in this standard. These abstract components are grouped by the business functions of the Interface Reference Model.

In this standard, the term abstract component is used to refer to that portion of a software system that supports one or more of the interfaces defined in Parts 3 to 10. It does not necessarily mean that compliant software is delivered as separate modules.

In this sub-clause, the definitions of business functions defined in Subclause 3.2 are further extended into:

- Sub-business Functions (second column).
- Abstract Components (third column).

NOTE: Some abstract components may be used by several different business functions. For example, a component like power flow can be used for network operation, short term operational planning and optimisation, and long term network extension planning. Much of the information exchanged for power flow purposes in each of these areas will therefore use many of the same Information Exchange Message Types (refer to Clause 5).

Applications from different vendors package the *functionality* of these abstract components in different ways. To use the IEC 61968 services, each application must support one or more of the *interfaces* for the abstract components.

Part 1 of this standard describes infrastructure services common to all abstract components whilst Parts 3-10 define the details of the information exchanged for specific types of abstract component.

IEC 61968 defines that:

1. An inter-application infrastructure is compliant if it supplies services defined in Part 1 to support at least two applications with interfaces compliant to sections of Parts 3 to 10.
2. An application interface is compliant if it supports the interface standards defined in Parts 3 to 10 for the relevant abstract components defined in the Interface Reference Model.
3. An application is only required to support interface standards of the applicable components listed in Column 3. It is not required to support interfaces required by other Abstract Components (Column 3) of the same Business Sub-Function (Column 2) or within the same Business Function (Column 1). While this standard primarily defines information exchanged among components in different business functions, it will occasionally also defines information exchanged among components within a single Business Function when a strong market need for this capability has been realised.

Business Functions	Business Sub-Functions	Abstract Components
3.3.1 Network operation (NO) [Refer to IEC 61968, Part 3]	Network operation monitoring (NMON)	Substation state supervision
		Network state supervision
		Switching action supervision
		Management of data acquired from SCADA and metering systems
		Management of data acquired through operation (field crews, customers, scheduled and unscheduled outages)
		Alarm supervision
		Operator and event logs
		Weather monitoring (lightning detection)
	Network control (CTL)	User access control
		Automatic controls: <ul style="list-style-type: none"> • Protection (fault clearance) • Sectionalising • Local voltage/reactive power control
		Assisted control: <ul style="list-style-type: none"> • Remote switch control • Load shedding • Voltage reduction broadcast • Local control through field crews
		Safety document management
		Safety checking and interlocks
		Major incident co-ordination

Business Functions	Business Sub-Functions	Abstract Components
	Fault Management (FLT)	Trouble call handling and coherency analysis (LV network)
		Protective relays analysis
		Fault location by analysis of fault detectors and/or trouble call localisation
		Supply restoration assessment
		Customer incident information
	Operation feedback analysis (OFA)	Mal-operation analysis
		Network fault analysis
		Quality index analysis
		Device operation history
	Operation statistics and reporting (OST)	Post-disturbance review
		Maintenance information
		Information for planning
	Network calculations – real-time (CLC)	Information for management control
		Load estimation
		Energy trading analysis
		Load flow/voltage profile
		Fault current analysis
3.3.2 Records and asset management (AM) [Refer to IEC 61968, Part 4]	Dispatcher training (TRN)	Adaptive relay settings
		SCADA simulation
	Substation and network inventory (EINV)	Equipment characteristics
		Connectivity model
		Substation display
	Geographical inventory (GINV)	Telecontrol database
		Network displays
	Asset investment planning (AIP)	Cartographic maps
		Maintenance strategy
		Life-cycle planning
		Reliability centred analysis
		Engineering and design standards
		Performance measurements
		Risk management
		Environmental management
		Decision support
		Budget allocation
		Maintain work triggers
		Asset maintenance groups (lists)
		Asset failure history
		Asset financial performance
		Thermal ratings of network equipment and lines

Business Functions	Business Sub-Functions	Abstract Components
3.3.3 Operational planning and optimisation (OP) [Refer to IEC 61968, Part 5]	Network operation simulation (SIM)	Load forecast
		Power flows computation
		Contingency analysis
		Short circuit analysis
		Optimal power flow
		Supply restoration assessment
		Switching simulation
		Incident simulation
		Weather forecast analysis
		Fire risk analysis
		Thermal ratings of network equipment and lines
	Switch action scheduling / operation work scheduling (SSC)	Release/clearance remote switch command scheduling
		Field crew loading analysis and work order scheduling
		Customer outage analysis and information
3.3.4 Maintenance and construction (MC) [Refer to IEC 61968, Part 6]	Power import scheduling and optimisation (IMP)	
	Maintenance and inspection (MAI)	Maintenance program management
		Maintain work triggers
		Asset maintenance groups (lists)
		Manage inspection readings
		Asset maintenance history
		Asset failure history
		Work order status tracking
		Work order closing
		Financial control
	Construction and design (CON)	Work initiation
		Work design
		Work cost estimation
		Work flow management
		Work order status tracking
		Work order closing
		Financial control
	Work scheduling (SCHD)	Work task planning
		Crew management
		Vehicle management
		Equipment management
		Material coordination
		Permit management

Business Functions	Business Sub-Functions	Abstract Components
	Field recording and design (FRD)	Field design
		Field inspection results
		Crew time entry
		Actual materials
	Work dispatch (DSP)	Field status tracking
		Real-time communication
		Weather monitoring
3.3.5 Network extension planning (NE) [Refer to IEC 61968, Part 7]	Network calculations (NCLC)	Load forecast
		Power flows
		Contingency analysis
		Short-circuit analysis
		Optimal power flow
		Energy loss calculations
	Construction supervision (CSP)	Feeder voltage profiles
		Construction costing
	Project definition (PRJ)	Work management
		Capital approval
	Compliance management (CMPL)	
		Safety compliance
		Technical compliance
3.3.6 Customer Support (CS) [Refer to IEC 61968, Part 8]	Customer service (CSRV)	Regulatory compliance
		Service requests
		Construction billing inquiry
		Work status
		Self service inquiry (Web, VRU...)
		Customer connection
	Trouble call management (TCM)	Turn on, turn off
		Service level agreements
		Outage calls
		Power quality
		Planned outage notifications
		Media communication
3.3.7 Meter reading and control (MR) [Refer to IEC 61968, Part 9]	Meter reading (RMR)	Performance indices
		Restoration projection/confirmation
		Outage history
		Load characteristics
		Consumption meters
		Quality factors

Business Functions	Business Sub-Functions	Abstract Components
3.3.8 External to DMS (EXT) [Refer to IEC 61968, Part 10]	Load control (LDC)	Meter parameter telesetting
		Dynamic tariff application
		Power modulation
	Energy management and energy trading (EMS)	Transmission
		Generation
		Energy trading
	Retail (RET)	Marketing and selling
		Settlements
		Customer registration
		Product line diversification
		Portfolio management
	Supply chain and logistics (SC)	Procurement
		Contract management
		Warehouse logistics
		Materials management
	Customer account management (ACT)	Credit status
		Outage history
		Credit and collections
		Billing and payment
		Customer profiling
	Financial (FIN)	Activity based management
		Accounts payable
		Accounts receivable
		Forecasting
		Budgeting
		General ledger
		Regulatory accounting
		Tax accounting
		Treasury
		Decision support
		Performance metrics
		Strategic planning
		Business development
	Premises (PRM)	Budgeting
		Regulatory relations
		Address
		Source substation
		Meter information
	Human resources (HR)	Right of ways, easements, grants
		Real estate management
		Health/safety reporting
		Payroll
		Safety administration
		Training
		Qualification tracking
		Hours on shift information

Business Functions		Business Sub-Functions	Abstract Components
			Benefits administration
			Employee performance, review, and compensation
			Recruiting

4 Interface Architecture

IEC 61968-1 describes utility inter-application infrastructure requirements necessary to integrate components distributed throughout the enterprise. The services and functionality described is independent of the underlying component-based infrastructure. In the following requirements, an “event” is a unit of information exchange which is issued asynchronously by its source (“push”). A “component” is a module of application software which is a component of the integration bus as either a publisher or subscriber (receiver) of an information exchange.

The business process begins by identifying the information to be exchanged and the components involved. This typically involves one publisher that has the information and initiates the exchange, and zero or more subscribers that will receive the information.

IEC 61968 requires that a compliant utility inter-application infrastructure:

1. Shall allow components to exchange information of arbitrary complexity.
2. Shall be able to be implemented using various forms of distributed component technology (e.g., CORBA, DCOM, message brokers, message oriented middleware, relational databases, object-oriented databases, or others). (refer to Clause 5)
3. Shall provide an Information Exchange Model facility (refer to Clause 6) that users employ to describe the information to be exchanged. This facility presents the user with the models of events and the components to which they relate, and allows the new exchange to be added to the old, so that a comprehensive corporate exchange model, tailored to a utility's specific needs, can be built rather than a collection of independent models.
4. Shall allow publisher and/or subscriber component to be deployed by system administrators independently of other components as far as interfaces remain the same.
5. Shall ensure that, once a given type of event is published, additional subscribing components can be configured to receive the event without having to make any changes or additions in the publisher component.

4.1 Requirements Analysis Methodology

To help solve the problem of effectively sharing information across Electric Utility Departments and systems, a common modelling notation or language is needed. A modelling language extends natural language by adding formal constructs to aid in communication by reducing ambiguity. By using a common modelling language across the utility, utilities can better define what information needs to be shared across departments.

This modelling language should be rich enough to detail the requirements, graphically oriented (visual diagrams) to make it easy to use, widely accepted, and supported by reasonably priced tools. Refer to Informative Annex B for further information regarding this methodology that has been used for the development of IEC 61968. Refer to Technical Report IEC [number and title to be confirmed] for the Use Cases used for the development of the Interface Reference Model.

5 Interface Profile

The Clause 5 is organised according to the Interface Profile, as shown in the following diagram.

5.1	Part 3 Component (Network Operations)	5.1	Part 4 Component (Records And Asset Management)	5.1	Any Part 3-10 Component
5.2	Component Adapter	5.2	Component Adapter	5.2	Component Adapter
5.3	IEC 61968-3 Interface Spec.	5.3	IEC 61968-4 Interface Spec.	5.3	IEC 61968-10 Interface Spec.
5.4	Middleware Adapter	5.4	Middleware Adapter	5.4	Middleware Adapter
5.5	Middleware Services				
5.6	Communication Services				
5.7	Platform Environment				

Figure 4: Overview of the Interface Profile and Corresponding Sub-Clause Numbers

The requirements for all the individual parts in this Interface Profile are explained in the following paragraphs.

5.1 Components

Information exchange among components can either be a piece of data or the result of an execution of functionality (Note: meaning that this function can be invoked remotely) and for this purpose is called a Services Exchange. For example, a Component can be a classic, procedural application (also referred to as a legacy application) or a fully object-oriented application build around the latest technology. Also, Components can be distributed across the network (LAN, Intranet, private corporate WAN or even the public Internet), enabling flexible deployment of DMS applications in the utility-wide ICT-architecture. The scope of a Component is unlimited: it can perform any function that is required for Distribution Management. Typical categories of functions are showed in the Interface Reference Model in Clause 3.

A component can either be *profile-compliant*, meaning that it knows, understands and satisfies Services requirements or *non-profile-compliant*. A *Non-profile-compliant* Component must be made compliant before it can fulfil its role on the Services (see Clause 5.2).²

For Components, IEC 61968 requires that applications shall:

1. implement at least one of the interfaces as specified in the relevant series of documents from IEC 61968-3 onwards.

² For example, each vendor of today's DMS applications may have its own application architecture, its own API and its own mechanism of interfacing the application with other products of the same vendor. Such existing applications may very well have an important role as a client of the Services. But the industry cannot expect that a vendor rebuild all its existing applications to new versions that are *profile-compliant*. Even new applications may not always be *profile-compliant*, but instead use the established vendor-specific architecture and application interface. Therefore, *non-profile-compliant components* probably will be in the majority during the early stages of the IEC 61968 standard series. When IEC 61986 becomes more widely accepted *profile-compliant components* will become more widely available.

2. implement producer and consumer services exchanges in at least one interaction type: publish/subscribe, publish/reply or Conversation (or Request/Reply if without session context).
3. register and unregister as a producer, a consumer or both for at least one interaction type.
4. provide for appropriate error handling & catching and recovery for service exchanges which cannot be produced or consumed. Each interface specification in the series IEC 61968-3 onwards contains a single services exchange for each interaction type. This specific IEC services exchange, for this purpose only, should be produced and consumed by each Component on the services
5. be able to register in at least one specific "context" (e.g. real-time, test, study, version 1, version 2) at the same time such that services exchanges produced within a context will, by default, be delivered only to Components within the same context.
6. be able to override the default context for a service exchange.
7. when producing a service exchange, identify the generic type of the service exchange in order to verify consistency between the Component and the information exchange model.
8. when producing an service exchange, create & package new instances of the service exchange (using the information exchange model to identify items of data that should be filled in).
9. when consuming a service exchange, identify the generic type of service exchange in order to verify consistency between the Component and the information exchange model.
10. when consuming an services exchange, parse & unpack delivered instances of the services exchange (using the information exchange model to identify items of data that should be interrogated).
11. be able to work within transaction contexts in which one or more consumed services exchanges are either committed in full or rolled back (reverted) in full.

NOTE: As an example, in CORBA a Component is equivalent to an object implementation. In DCOM a Component is equivalent to a Client Object or a Server Object.

5.2 Component Adapters

A *Component Adapter* in the context of IEC 61968 is *profile-compliant* software that enables a non-compliant software application to use the services. As such, the component adapter only goes as far as necessary to make the Component conformant to one or more specific interface specifications in the series IEC 61968-3 onwards.

NOTE: This implies that:

- For Components that already are *profile-compliant*, the Component Adapter is not necessary.
- When a non-compliant Component is used in the services-environment, at least one Component Adapter is present for that Component to make it *profile-compliant*. It can also be the case that more than one Component Adapter is used to make a single Component compliant with the the services (e.g. one Component Adapter for each IEC 61968 interface specification).
- For those Components that are non-compliant, each Component Adapter is custom-made for that specific Component because it depends heavily on the architecture and implementation of the Component. A Component also runs in a specific hardware/operating system (HW/OS) environment. Therefore the triple set Component, (set of) Component Adapter(s) and HW/OS are fully dependent on each other.

How the Component Adapter makes a non-*profile-compliant* Component compliant to the services, depends on the Component and the role it performs. A complication is that a Component that was not coded to be *profile-compliant* cannot be made *profile-compliant* directly, and that each Component is different.

NOTE: Examples of how the Component Adapter accesses non-*profile-compliant* Components to make them *profile-compliant* are:

- accessing the Component via its own specific Application Program Interface
- accessing the Component via its data stores (flat files, databases, whatever)
- accessing the Component via screen scraping (emulating a terminal and accessing fixed positions on the emulated screen)
- accessing the Component via batch control or another external application run control method

1. For Component Adapters, IEC 61968 requires that they shall meet the requirements specified in Clause 5.1 for a *profile-compliant component*

NOTE: (A Component Adapter does not exist for a profile-compliant component.)

5.3 Interface Specification

The IEC 61968 Interface Specification requirements consists of three parts: Component-specific specifications, requirements that refer to services specific for the Distribution Management domain and requirements that refer to services which are common in a distributed computing environment based on components. Individual IEC 61968 Interface specification for functional areas (see the Interface Reference Model in Clause 3) are available in following parts of this IEC 61968 standard (IEC 61968-3 and further).

For all three parts in an IEC 61968 Interface specification, it shall:

1. be declarative, containing pre- and postconditions, attributes, methods and parameters as needed for all the service exchanges that are part of the specific interface specification
2. be programming-language neutral
3. emphasize the separation of interface and implementation
4. be middleware-independent

Requirements for Component-specific Interface specifications are exclusive usage of IEC 61968 Interface services for those requirements that can be supported by those services.

NOTE: This means that for requirements not covered, additional services may be specified (and probably need to be programmed or mapped in the Middleware Adapter or Middleware Services)

Required services for the Distribution Management domain shall be as follows:

5. Identifier creation and aliasing service. This is a set of services for creating and maintaining unique identifiers for business objects for which information is transferred between components. There may be multiple types of identifiers based on specific rules for each type of business object. It is expected that within each utility domain (i.e. company or department), the systems, equipment, staff and consumers can be uniquely identified. When information is exchange between two utility domains, then identifiers may need extending with the identity of the utility organisation in order to guarantee global uniqueness.
6. Persistent Exchange service with checkpoint facilities, allowing components that register at different times to synchronize status with other components. This service supports entering and purging exchanges, marking (a group of) exchanges and reading (a group of) historical exchanges
7. System Administration: This service interface allows administration and monitoring of exchanges and components on the Services. Component failure and load balancing are also part of this service.

8. Configuration: This service provides an interface for components to obtain their configuration from a persistent data store at start up or while running after a component has been partially configured locally.
9. Filtering: This service allows for the definition and applying of filters based on exchange types and contents.

Required common distributed computing services in Distribution Management shall be:

10. Component Life Cycle Service: These services allow the starting, stopping, and control of components to be executed on the Services.
11. Naming Service: This service provides a component naming service that supports a hierarchical structure and allows a component to locate other components using a human readable name. The naming service supports use of existing utility names, as well as creation, removal and aliasing of names.
12. Time Service: This service provides a way for distributed components to all have the same time with a configurable accuracy.
13. Concurrency Control Service: This service facilitates management of shared, similar items that are distributed on the Services, for example when multiple Components take care of different parts (exchanges, exchange types) of the same business object in real life.
14. Security services: These services allow an application to set and verify the privilege level of components and users with which exchanges are being performed, as well as encryption and decryption of individual exchanges. This service also supplies host authentication i.e. authentication of node(s) that attach to the Services.
15. Transactional Service: This service allows an application to declare the beginning and end of a multi-step transaction that either succeeds or fails as an atomic unit.
16. Component Interaction services. These services allow for reliable message transfer with a selectable Quality of Service. The Component Interaction services allow for life-cycle management of interaction services (create, delete, copy and move) and querying of established interaction (mainly valid for Publish and Subscribe interactions).
17. There is the Publish and Subscribe Messaging Service, which allows for synchronous and asynchronous message transfer between de-coupled (anonymous) component instances.
18. There is the Request/Reply Messaging service, which allows for reliable synchronous message transfer between coupled, identified component instances.
19. There is the Publish/Reply Messaging service, which allows for a de-coupled initiation of a message transfer (Publish), which is then finished by a coupled transfer (Reply).

5.4 Middleware Adapter

A *Middleware Adapter* in IEC 61968 is *profile-compliant* software that augments existing middleware services so that the utility's inter-application infrastructure supports required Services. As such, the Middleware Adapter only goes as far as necessary to make the used set of Middleware services conformant to the requirements of one or more available the interface specifications in the series IEC 61986-3 onwards. In this context the Middleware services represent **not one** single interface, it represents **a set of interfaces to a set of corresponding** services for Components.

For example, each vendor's Component may use internally any middleware (or no middleware at all!) that is **appropriate for the needs of the specific business function**. Thus we cannot assume that two arbitrary Components will always use the same implementation of Middleware services that are used by the utility. Thus a Middleware Adapter is needed that is able to act as a middleware "gateway" for IEC 61968 exchanges produced by one Component over the

implemented Middleware services into the upper layers of the other Component(s) (which may be based on other middleware).

The IEC 61968 Interface Specifications Parts 3-10 define the required services (see previous clause) that must be present in the total architecture implementation that Components can depend on. However, different Middleware services implementations will provide different levels of services and different operating environments may provide some properties implicitly and require others to be added by the Middleware Adapter. If the Middleware services implementation does not provide a feature, the Middleware Adapter can provide it. It is possible for an Object implementation to have access to a service whether or not it is implemented in the ORB core. If it does not, the Middleware adapter must implement it on top of the implemented Middleware services.

NOTE: This implies that:

- For a Middleware service implementation that provides the Service, the Middleware Adapter is required to provide a mapping to it.
 - When a non-compliant Middleware services implementation is used in an IEC 61968-environment, at least one Middleware Adapter is present for that Middleware services implementation to make it IEC 61968-compliant. It can also be the case that more than one Middleware Adapter is used to make a single Middleware services implementation compliant with the Services (e.g. one Middleware Adapter for each required IEC 61968 Interface service)
 - For those Middleware services that are non-compliant, each Middleware Adapter is custom-made for that specific Middleware services implementation because it depends heavily on the architecture and implementation of the Middleware services implementation. It also runs in a specific, possibly distributed hardware/operating system (HW/OS) environment. Therefore the triple set Middleware services implementation, (set of) Middleware Adapter(s) and HW/OS are fully dependent on each other.
 - The Middleware Adapter (in theory) is reusable for multiple IEC 61968 Interface services running over the same Middleware services implementation in the same computing environment.
1. IEC 61968 requires that Middleware Adapters shall provide the full set of service requirements specified in the specific IEC 61968 Interface specifications. They may do that via simple mapping of Services to Middleware services implementation, or via additional software components dedicated to provide one or more IEC 61968 Interface services

5.5 Middleware services

Information exchanged among components can be performed within the same process (in process), across processes on the same machine (local) and across machines (remote). Object request brokers usually support different communication patterns, e.g. synchronous and asynchronous interaction. Subscription refers to the ability to read or modify objects at cyclic or event driven times. Messaging covers more the features of today's messaging middleware, such as store-and-forward, persistence of messages and guaranteed delivery.

The Middleware services shall provide a set of APIs so that the previous layers in the Interface Profile among others can:

1. locate transparently across the network, and interact with other applications or services
2. are independent from Communication Profile services
3. be reliable and available
4. scale up in capacity without losing functionality
5. provide the ability to support *business-to-business* (B2B) transactions where needed

As an example, in CORBA the Basic Object Adapter supplies some of the basic Middleware services for life cycle and registration.

5.6 Communication services

Integrating two components requires a connection between them. As there is more than one kind of network, different resources speak different protocols, such as IIOP and HTTP. To connect multiple components, an integration system must reconcile network and protocol differences transparently to the components.

IEC 61968 requires that the Communication service:

1. shall guarantee delivery of network messages to their network destination if that is active
2. shall provide guaranteed delivery, ensuring that network messages are delivered exactly once, regardless of network failures or changes
3. shall provide guaranteed ordering, preserving the sending sequence of the source when delivering messages, regardless of network failures or changes
4. shall guarantee that if a network message can not be delivered to a network destination, the network source will receive a message indicating the non-delivery
5. shall provide a selectable quality of service for prioritization of network messages or delivery via specific network paths
6. shall provide dynamic adaptation to the speed of processing network messages by the network destination to allow slow destinations to work on the Services

5.7 Platform Environment

Services are based on hardware and software standard platforms. We have to cope with different hardware and operating system platforms from different vendors. This means that we can't expect that a component running in a dedicated hardware environment (processor, operating system, language and compilers) to run also on another hardware environment without modifications.

The hardware environment (processor, I/O, operating system, GUI, compilers and tools) of the IEC 61968 standard requires that:

1. it shall support multiple local processes running concurrently and does not matter if this is achieved on a single processor or multi-processor hardware
2. it shall support inter-process communication between concurrent processes
3. all other specifics of the hardware environment shall be shielded by the other layers in the Interface Profile

6 Information Exchange Model

6.1 General Requirements

This document defines requirements of an Interface Reference Model (IRM) for Distribution Management where Components distributed over the communication network exchange information using IEC 61698 services. Only functionality and services required to support information exchange are enumerated in this clause; the manner in which this functionality is implemented is outside of the scope of this standard.

IEC 61968 requires that a compliant utility inter-application infrastructure:

1. Shall have one logical IEC 61968 Information Exchange Model (IEM) and its implementation may be physically distributed. This facility allows information exchanged among components to be declared in a publicly accessible manner.

NOTE: Other non-IEC 61968 Information Exchange Models may exist within a single utility. For example, information exchanged for a general business application may be separately designed and maintained from the IEM for Distribution Management. IEC 61968 requirements do not affect these IEMs.

2. The IEM shall maintain descriptions of the contents, syntax and semantics (i.e. meaning) of the information exchanged between Components. Such description is commonly referred to as metadata (or a data dictionary).
3. The IEM shall be accessible in machine-readable and platform independent form.
4. Information is exchanged between Components via one or more events whose types are defined in the IEM.
5. The IEM shall be capable of containing:
 - Names of primitive data types and their mapping to standard data types such as float, integer.
 - Named business object types such as Breaker, Outage Schedule and Network Diagram.
 - Name and data type of the attributes of the business objects such as 'inService', 'voltage'.
 - A name of relationships between business objects such as 'owns', 'connectedTo'.
 - Named event types which act on objects e.g. object attribute update, object creation, object deletion.
6. The IEM may be capable of containing named datasets (i.e. sets of business object types, object attributes, event types or object instances).
7. The IEM shall support Services such that (note that the registration services are specified in subclause 5.1 requirement 3.):
 - A Component can register its name and what event types it may publish.
 - A Component can register its name and what event types it may subscribe to.
 - A Component can register the context (real-time, study, test) for which it publishes/subscribes.

6.2 IEM Management Related services

IEC 61968 requires that a compliant utility inter-application infrastructure shall provide the following IEM life cycle services:

1. IEM Data definition and maintenance. This service shall allow dynamic changes in the information model governing exchanges. If the existing model is amended and component interfaces have not been modified, no re-coding or recompilation of components shall be

required. New versions of components can use the specific information which has changed or was added without affecting the operation of the remaining components.

2. Validation of the information exchange model, for example enforcing uniqueness of names, version control.
3. Synchronisation of components to use the same version of the IEM when it is updated.
4. The IEM management system shall include a method of generating human readable reports.
5. IEM Data discovery. This facility shall make the IEM available to the components in machine-readable forms.
6. The IEM management system may provide facilities for the dynamic creation, modification and deletion by components of named data sets.

7 Component Reporting And Error Handling

IEC 61968 requires that a compliant utility inter-application infrastructure:

1. Shall provide a generic event history facility as a component. This allows all or selected information exchanges to be saved in a permanent store.
2. Event History's schema shall be based on the metadata provided by the Information Exchange Model (refer to clause 6).
3. The Event History component shall record the time at which the publishing component issued each event.
4. Shall be capable of supporting event information model versions and component versions. (This allows a complete audit trail to be preserved which is capable of supporting rigorous reconstruction of history, if that should become a requirement.)
5. Shall provide Inter-application Supervisor component that analyses the state of any application component interface connected to the utility services. It may be enabled and disabled, and has the capability to provide performance monitoring capabilities. Those elements will help to provide statistics in order to identify bottlenecks or areas subject to improvement in the future. The information is required to help the administrators configure information exchanged among components and to ensure availability.
6. A component shall be able to send or request an information without knowing where the receiving component is physically located or if it is currently connected. The receiver may be unreachable because of a network problem, or be naturally disconnected as in the case of mobile users who only connect periodically.

NOTE 1: Components may be unavailable because they have failed or because they only run during certain hours; when the network becomes available or receiving application is ready to process requests, the waiting information must be delivered.

NOTE 2: A Journalizing service may be available and is used for visualisation of computer and communication related (i.e., non-power system) events occurring on the system. The journalising service should be implemented as a of IEC 61968 persistent exchange service.

7.1 Error Message Handling

As a general rule, upper layers of architecture contain operations at higher levels of abstraction. At these levels, less detail information is sufficient because less detail is present concerning the operation that failed. The principle is that error information should match the level of abstraction of the layer in which it is being examined.

1. The information contained in the error report shall contain sufficient detail to be useful in coping with the error.

NOTE 1: There are different types of errors: warnings, non-fatal errors, and fatal errors.

- Warnings: Information messages; e.g., message queue buffer is nearly full.
- Non-fatal errors: Recoverable erroneous condition that does not require re-initialisation; e.g., Data integrity failure.
- Fatal errors: Erroneous condition that requires re-initialisation of one or more components and/or Services. Unaffected components and services continue to operate in a restrictive configuration until recovery is complete.

NOTE 2: An exception specification is part of a function signature; e.g., In C++ it consists of the keyword throw, written after the parameter list and is followed by a parenthesised list of types. The exception specifications are not a statement of what should happen, but a statement of what might happen and a guarantee of what will not happen.

8 Security and Authentication

Security concerns arise at any exposed, via communication or other, interfaces within a system. A secure system enforces at a minimum, authentication at all such exposed interfaces. As a consequence of both deregulation and the growth and utilisation of the web, it will be necessary to ensure that appropriate security measures are taken. For these reasons the standards will be drawn from both IEC and non-IEC sources.

A user, either a human being or component, interacts with a component. The interface between the user and the component represents an exposed component interface through which major security breaches could occur within the system. For human users, it is the responsibility of the requesting component to authenticate that the user has the authority to:

- Use the business function.
- Use the Services on an individual service basis. Although such a restriction will aid in security, the rights to issue service requests of a remote component shall be enforced by the requested remote component service.³

Once the user has been authenticated, it is the responsibility of the component to perform a determination of the user's authentication versus the security parameter values required by the remote component, which the user is attempting to access.

Requirement

1. An IEC 61968 compliant system shall implement security requirements as determined by the utilities security policy.

This implies that a utility will have conducted an appraisal of security requirements for all application components that form an IEC 61968 compliant system as a precursor to forming a utility policy. This would normally be achieved by analysing security threats and their consequences on the business of the utility.

2. The security model must support several choices of implementation and the utility must be free to pick the security model most effective for its needs.
3. IEC 61968 compliant system shall support the security requirements of compliant application components (see Sub-clause 5.3 requirement 16). The security shall work in co-operation with application security and should not have to replace it.

NOTE: A feature of IEC 61968 compliant systems is that an application is able to access the data 'owned' by another application. Both parties have a responsibility to define minimum security levels for use of their data. This may vary according to where the data is to be transported, i.e. inside or outside a firewall.

8.1 Security Threats

Security threats include:

- **Authorisation Violation** - An authorised peer attempts to perform actions/functions for which the peer is not authorised. The appropriate security mechanism to counter this threat is the use of peer authentication coupled with application level access-control.

³ The requesting component service restriction is optional and does not increase the robustness of the overall security integrity of the system. However, such restrictions may be useful as a migration path towards system security for systems where the remote applications do not support the security services as specified in this document.

- **Eavesdropping** - The communication packets are being monitored by a system intruder. This threat impacts the confidentiality of sensitive information. The appropriate security mechanism to counter this threat is the encryption of sensitive information.
- **Information Leakage** - Disclosure of information to an unauthorised entity. This threat impacts the confidentiality of sensitive information. However, the security outlined in this document does not counter the use of network traffic as a means of conveying information. The appropriate security mechanism to counter this threat is the use of peer authentication coupled with application level access-control.
- **Intercept/Alter** - The communication packets are intercepted by an intruder. The information in the packets is then modified and forwarded to the original destination application. This threat poses data integrity issues. The appropriate security mechanism, to counter this threat, is encryption.
- **Masquerade** - This threat is typically referred to as spoofing. An intruder attempts to gain system access by attempting to pretend to be a different entity. This threat poses a severe control and data confidentiality risk. The appropriate security mechanism, to counter this threat, is the use of strong-authentication.
- **Replay** - A communication packet that has been obtained through eavesdropping is retransmitted onto the network at a later time. If the captured packet contains control commands, this threat can have severe consequences. This threat can be countered through appropriate encryption coupled with dynamic encryption key management. The key management mechanisms are a local issue.

8.2 Security Functions

Requirement

4. The agreed utility policy for application components forming an IEC 61968 compliant system shall determine which security and authentication⁴ features are required. These features should include the following as appropriate:-
 - Restriction of access to unauthorised users
 - Automated journalising of all communication system changes
 - Automated management of user authorisations
 - Automated management of communication address⁵ allocations
 - Record level data locking facilities
 - Support for encryption of names and data values
 - Automated virus and worm detection and elimination facilities
 - Protection against threats which may deny service to authorised users⁶

The above features will ensure data integrity and adequate immunity of the communication interface to unauthorised access to data and control functions. The middleware mechanisms take

⁴ Communication security includes all measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by an application. Confidentiality provides assurance that information is not disclosed to unauthorised persons, entities or processes.

⁵ Addressing provides the communication means to identify the source and destination (recipients) of all information transfers.

⁶ Denial of service refers to any action that disables normal operation of any portion of the communication system. A user with the capability to modify information or exhaust system resources could interfere with the legitimate use of the system. For example, service denial may result from a node or application, accidentally or intentionally, overloading a communication network or interfering with application processing in such a way that a well-behaved, legitimate user is blocked from sending information for some significant time period.

responsibility for security and encryption. This includes Guaranteed Delivery, Identification, Authentication, Access Control, and Encryption, where required.

Encryption is provided either by the message transport or by added value message handlers invoked during call processing.

5. Due attention shall be given to the level of security and features which may have been applied elsewhere to certain data, i.e. an IEC 61968 compliant system shall not be the "weak link in a chain".

8.3 Management of Integrity and Security

6. An IEC 61968 compliant system shall provide both integrity- and security-oriented services.

8.3.1 Levels of Immunity

7. Integrity is the immunity of the communication network to data transfer errors resulting from accidental or intentional interference. Three distinct levels of error immunity shall be required.
 - **High:** transfer of data with negligible probability of undetected error; e.g., control commands and system critical parameters
 - **Medium:** transfer of inherently redundant information; e.g., power system measurements and plain text
 - **Low:** transfer of routinely updated information where occasional errors are merely a nuisance; e.g., voice traffic

8.3.2 Levels of Security

8. Three levels are defined for immunity of communication resources to accidental or intentional unauthorised access. Three levels of security shall be required:
 - **High**, where access is limited to predefined and validated components
 - **Medium**, where access is granted to any component meeting simple criteria
 - **Low**, where access (usually read-only) is granted to any Component

The highest level of security may include provision for proof of data origin to a receiver and proof of data delivery to a transmitter.

8.4 Security Agent

The Security Agent is a Service that is responsible for the enforcement of authentication, encryption, access control, maintenance of security configuration, and the maintenance of security management parameters. In general, there is a single instance of the Security Agent within a Server. However:-

9. there shall be no behavioural differences between a single instance and multiple instance implementation, as the agent(s) shall behave in accordance with association specific attributes.
10. The security agent shall authenticate the establishment of an association through a local mechanism. However, once authenticated, the agent for the association shall enforce the appropriate access privileges.

Authentication is performed within a component. Security procedures are enforced based upon three conditions supplied by the communication profiles over which the component executes:

- i. The level of security to be applied.
- ii. A value that represents a logical security parameter, which is to be supplied to the appropriate security functions.

- iii. A value that represents the originating address of the request that is being presented to the application.
11. The Security Agent shall not assign severity codes based upon the security violations that have been attempted. The assignment of such codes is the responsibility of the component that is receiving the security violation reports.

9 Maintenance aspects

Maintenance is an important part of the life cycle, which comes at the end of a long process (design, implementation, exploitation of a system). The level of maintenance problems will reflect the quality of the design and implementation of the integrated components, each of which is produced by different sources. Reduced reliability, increased executable size, and reduced performance are among the likely consequences of a poor implementation. Reduced testability, reduced usability and reduced modifiability are important primary causes. Secondary causes include increased link time, reduced comprehension and increased compile-time.

IEC 61968's specification of component interfaces does not place requirements about how each component should be designed internally. However, design is encouraged to be modular and decoupled from other component designs. That is, components should be largely self contained and have little interdependence.

IEC 61968 requires that a compliant utility inter-application infrastructure shall:

1. allow a subscriber component to be deployed by system administrators independently of the publisher or other subscribers, and there may be any number of other subscribers. Once it is deployed, the system is aware of the subscriber's registration, and it will deliver any that fit the registration.
2. ensure that the system handles all component location transparently so that those components can be relocated in any host without changing the component code.
3. provide initialisation facilities which can synchronize a component start-up in two ways:
 - Deliver the last values of all registrations.
 - Deliver all instances of exchanges which would have been delivered since the component was last active (provided the instances are in the history).
4. provide a component registration that shall be able to be "active" whether or not the component itself is running at the moment. (Thus the system shall be able to hold messages for subscribers who come on line periodically or sporadically, and also for continuous components which can fail and return.)
5. allow components to fail and return without any requirement to re-initialize other components. Components will use Services for this capability. This warm-starting facility can assume that all events which the component would have received while it was down will be available. The component will thus be able to continue to operate in a event driven mode once it has updated its local data store from a previous known (i.e., marked) state.
6. provide notice to all registered components that they must "cold-start" if the utility's IEC 61968 system is down longer than its survival duration, or if there is a failure of the Services, or if for any other reason, the flow of event information cannot be trusted. This requires that components re-initialise themselves without assuming that they have received every event for which they have registered.
7. ensure that a publisher component shall be able to issue a cold-start related to any event type for which it has not been able to guarantee a continuous stream of events.
8. make provision to interface to, as needed, utility standard network management services.
9. support configuration management of the utility's IEC 61968 system. Provision shall be made for the administration and deployment of different versions of the same components within the same utility system.

Annex A (informative)

Distribution Management Domain

In describing integrated systems, it is important to keep in mind the basic meaning of the following words, and how they are presently used:

- Management: Effective regulation and direction
- Automation: Working without human participation
- System: A set of organized operations working to support a particular activity (set of applications). Generally, a system is in the context of this work is a computer based technology.

In the world of integrated systems, systems are also a subset of a system. A system which is built up of many subsystems uses the subsystems to support particular activities better than if the subsystems are operating independently.

Consider the hierarchy of possibilities involving data exchange with some of the examples of their implementation. In figure A.1, the basic building blocks, which have a particular functionality, are the programs or packages or applications. A suite of applications combines together to a system. Several systems may be required to provide the support for a department with a specified responsibility. Thus, data is being exchanged between applications, between systems, and between departments. Finally, each company has commitments for information exchange with other companies with which it is dealing.

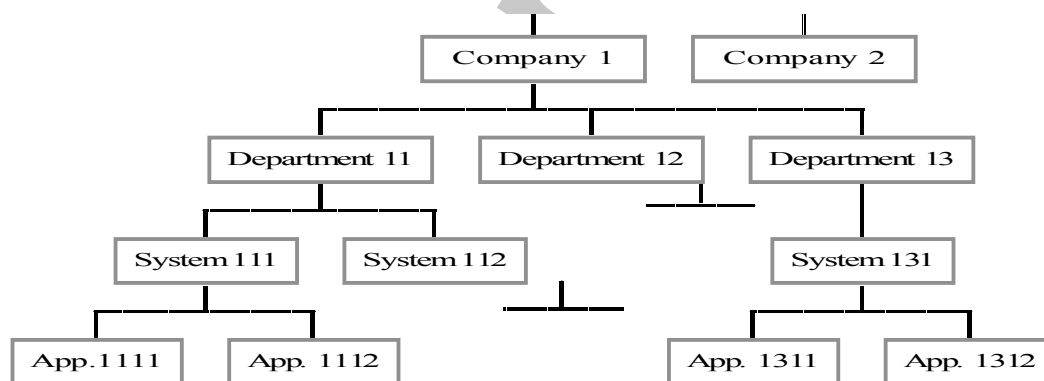


Figure A.1: Hierarchy of complexity in a system environment

As integration and data exchange becomes automated, the systems merge to become themselves sub-systems of the next higher system. Thus, System111 and System112 become subsystems of the Department11 System. At the next level of integration with automated data exchange, the Department11 System and the Department12 System etc. become themselves sub-systems of the Company1 System.

The fact that departments have names, and that some departments or specific responsibilities have become automated earlier than others has led to particular naming conventions being applied to describe the support system. We will continue to use the general names as usually accepted, pointing out the content and limits of the system to provide consistent interface

definition. Within the corporate utility environment, a typical structure which helps to classify the key system interfaces follows from figure A.2.

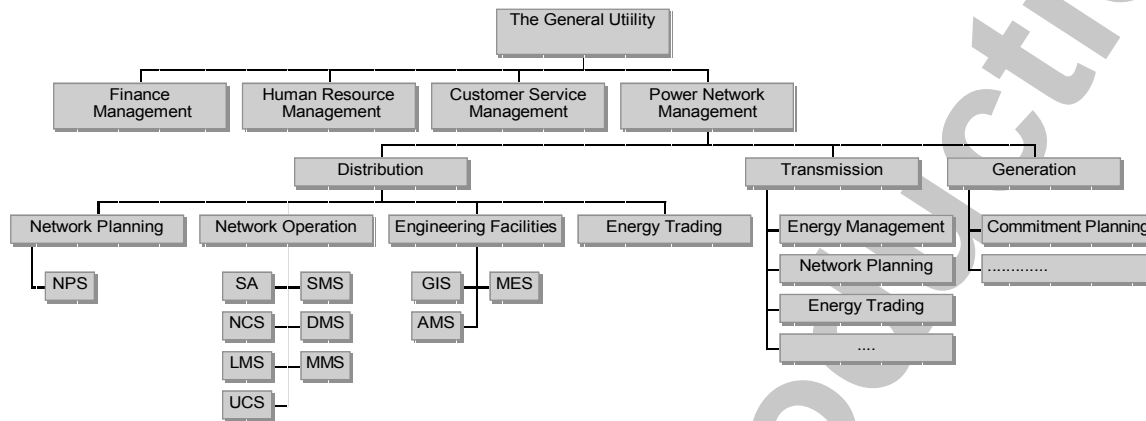


Figure A.2: General utility structure

The Departments involved in Finance Management and Human Resource Management are the internal Corporate services departments whereas the Customer Service Management and Power Network Management Departments are the utility business departments. Note also that a utility for the purposes of this working group has a distribution power network, but need not necessarily have transmission and/or generation.

Information Exchange	Example of Information
Company – Company Utility – Supplier Utility – Utility Utility – Component	Equipment Order Energy exchange statistics Tariffs and billing
Department – Department Network Planning dept - Operations dept. Trading dept – Operations dept Operations dept - Engineering Dept	Network Extensions Load Forecasts Switching statistics
System – System Substation Control Sys. - DMS Power Station Control Sys - EMS	Relay Status Unit Efficiency Statistics
Program – Program State Estimation - Optimal Power Flow Unit Commitment - Economic Dispatch	Network Data Cost Curves

Table A.1: Examples of data exchange in a company environment

The structure of data being exchanged tends to increase with the complexity of the tasks involved on either side of the exchange, as depicted in Table A.1. Furthermore, the deeper the data structure is within the system, e.g. data exchange between two applications, the less transparent it is to the end user.

The type of data that is regularly used by the utility (Table A.2) and the spectrum of users and suppliers of data implies that the basic data must be “owned” by one department, to avoid:

- errors arising from multiple points of data entry
- lack of consistency with software interfaces
- expensive changes with new or upgraded software
- loss of overview of authorised data.

Data Category	Examples of data
Network and Plant	Network description - topology, models, owners Element types, construction data CAD plans
Planning and Analysis	Network expansion data for planning scenarios Historical item data - average, max., min, trends Historical network data - state estimation results
Financial	Energy accounting data Economy data Tariff structures Exchange agreements and contracts Billing and accounts data
Plant Maintenance	Maintenance schedules Work orders Topographical data
System Maintenance	Maintenance Schedules Communications data Measurement cross reference data

Table A.2: Data Categories

The standardisation of data brings with it reduction in errors, reduction in time consuming data entry, and improved process control. On the other hand, together with standardisation, system-wide rules within the utility must be implemented to cover a number of delicate problems such as:

- authorisation of new data
- the right to change data
- main point of storage
- security of data
- handling of non-standard data
- backup of data

- verification of data
- uniqueness and identification of data

©, not for reproduction

Annex B (informative)

IEC 61968 Series Of Standards Development Process

B.1 Introduction

This informative annex summarizes the modeling concepts, work steps, and deliverables of IEC TC57 WG14. It clarifies the purpose and manner of coordinating work with IEC TC57 WG13, the EPRI CCAP1 and UCA projects, the Open Applications Group. This annex is only intended to provide general guidelines for the development of IEC 61968 standards and their use.

B.1.1 Application of IEC61968 by a Utility

Step A of the Utility Application process flow is the installation of suitable infrastructure to enable integration. Steps B to G of the Utility Application process flow are concerned with the analysis of the specific utility requirements leading to a detailed specification of utility specific message types. It is expected that these specifications will be produced as a printed report in a similar manner to Parts 3 to 10 of IEC 61968. However a utility and its suppliers may agree to exchange specifications in an appropriate electronic form, for example as produced by visual modelling tools.

Steps H to N of the Utility Application process flow describe the implementation and deployment of these utility specific message types. In general, an application supplier is expected to be responsible for modifying applications to produce or interpret the utility specific message types. The utility system integrator is expected to be responsible for the configuration of the Information Exchange Model (IEM) within the infrastructure. The IEM may support full or partial automatic configuration from machine-readable data produced by the applications or from electronic copies of the message specifications produced in step G.

There are three parts to the process:

- definition of the interface architecture and the major abstract components;
- definition of interface specifications of message types that describe dynamic changes.
- definition of a static entity model to provide a common way of describing what data may be exchanged;

Development of the static entity model and the messages is an iterative process.

Two process flow are shown below to give an overview of:

1. IEC TC57 Working Group 14 Process For Developing IEC 61968 Parts 3-11
2. An Overview Of An Utility Application Of The IEC 61968 Standard

The steps shown in the first process flow are described in the remaining sections of this informative annex.



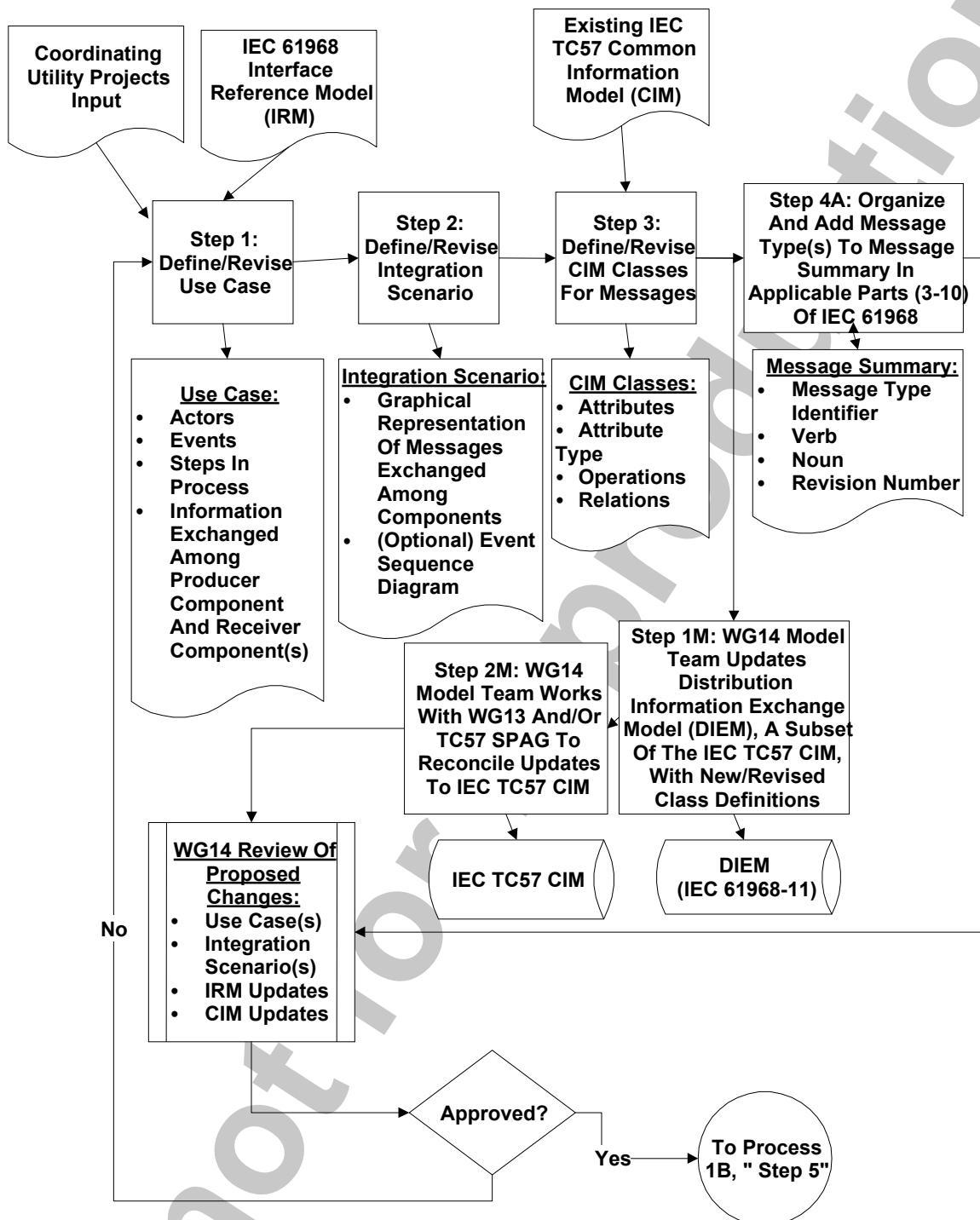


Figure B.1A: Process 1A: IEC TC57 Working Group 14 Process For Developing IEC 61968 Parts 3-11

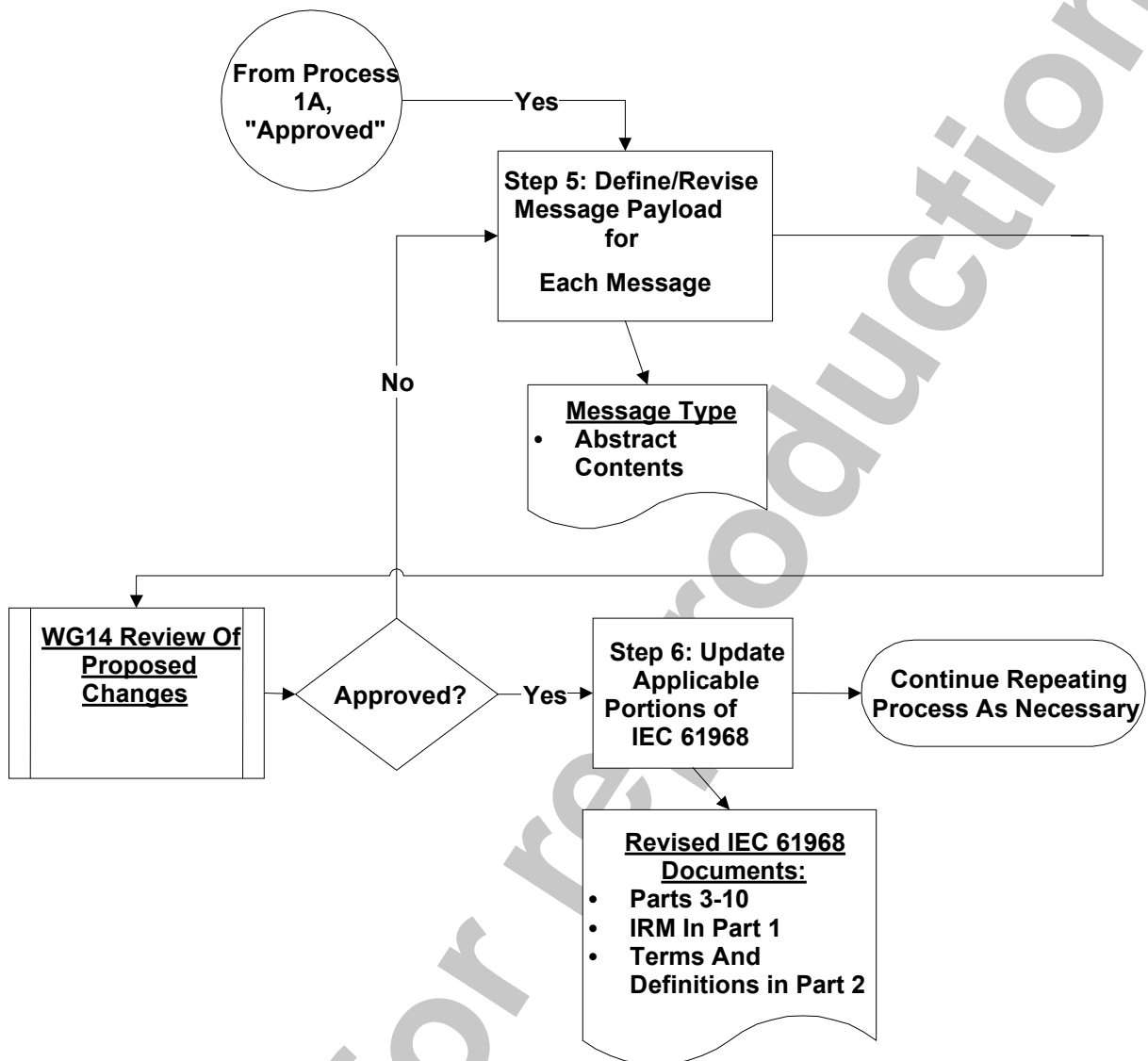


Figure B.1B: Process 1B: (Continuation) IEC TC57 Working Group 14 Process For Developing IEC 61968 Parts 3-11

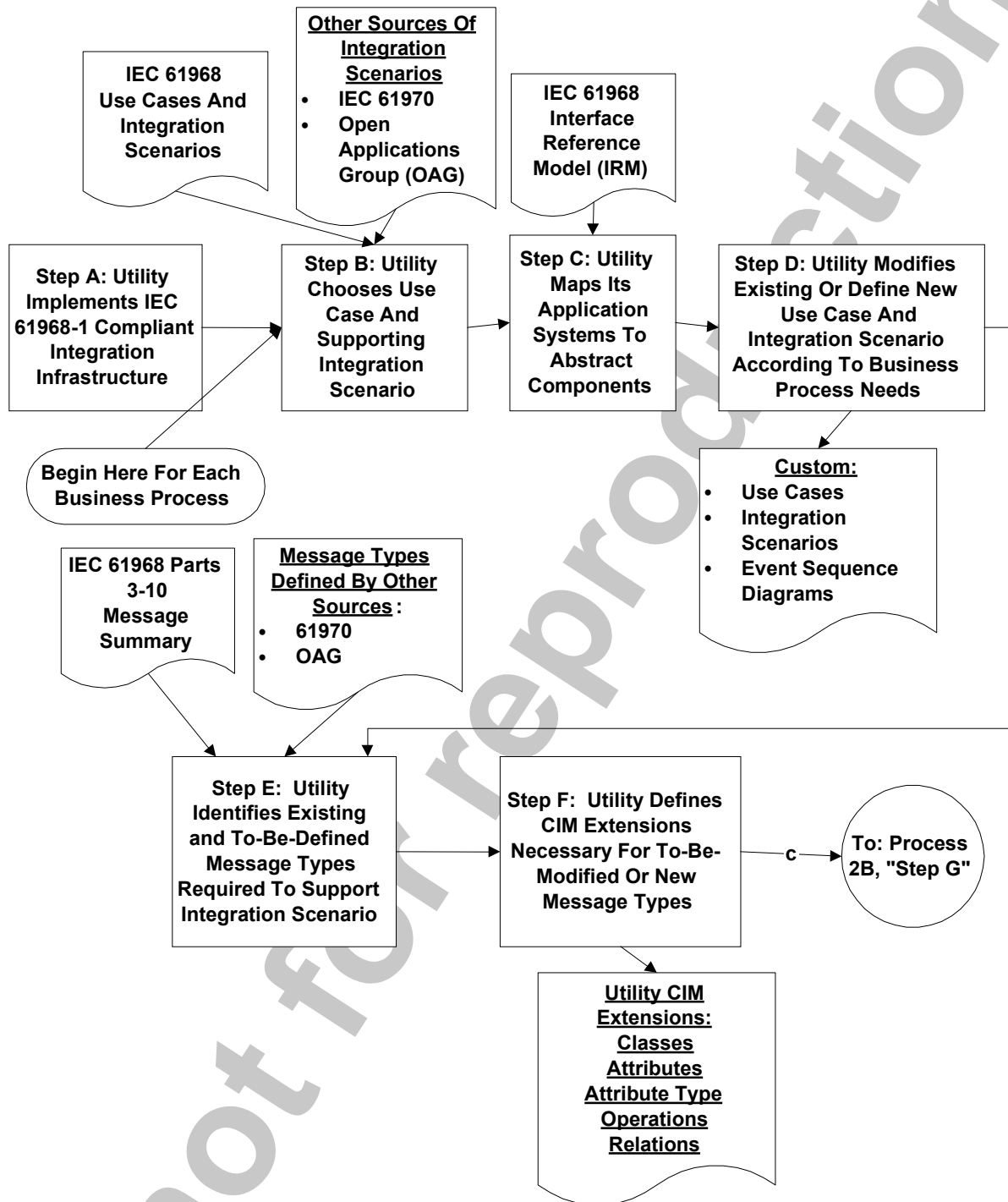


Figure B.2A: Process 2A: Typical business sub-functions of DMS and external systems

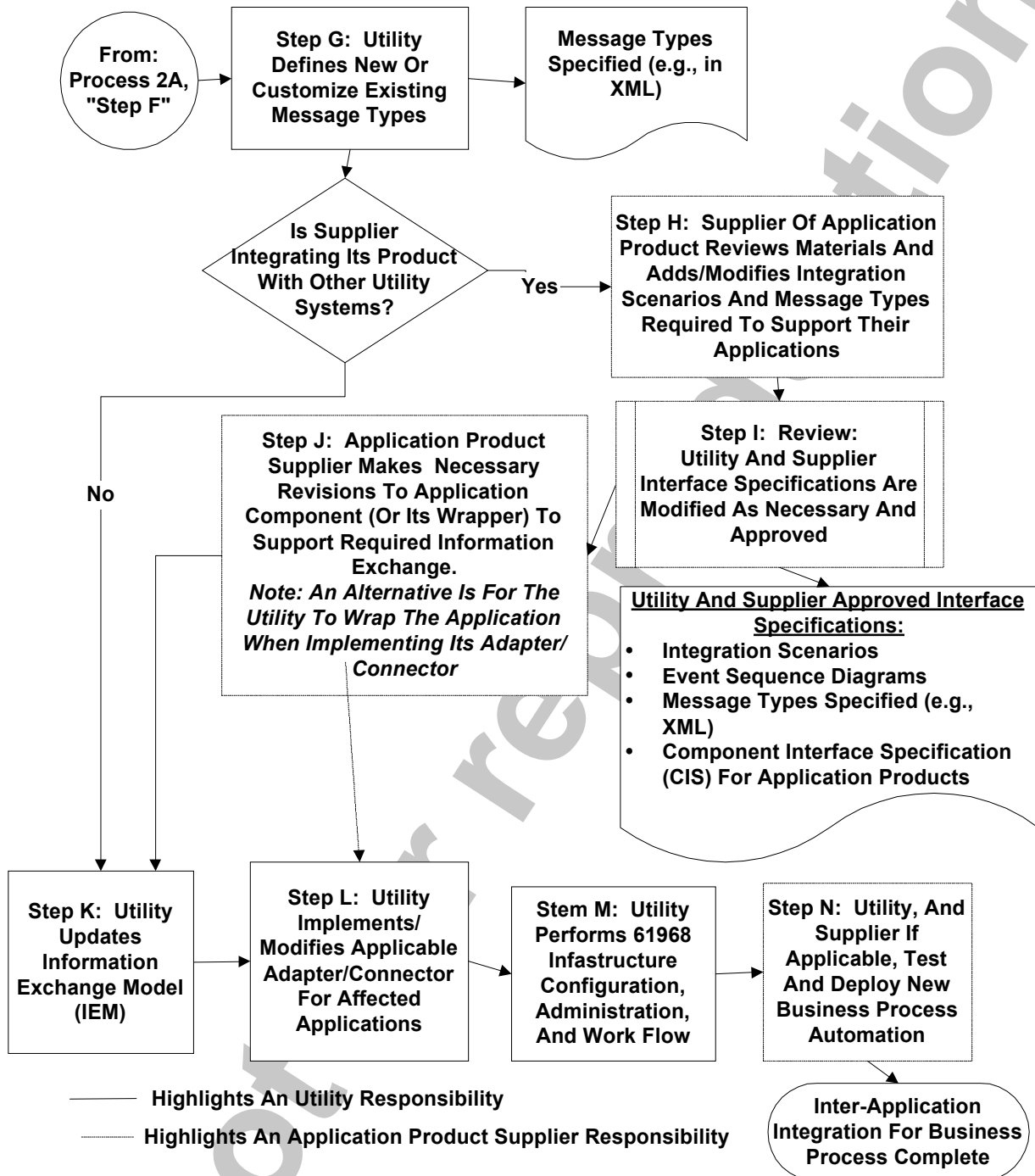


Figure B.2B: Process 2B: (Continuation) An Overview Of An Utility's Application Of The IEC 61968 Standard

B.2 Part 1: Interface Architecture and General Requirements

B.2.1 Establish interface architecture and general requirements in IEC 61968-1, referred to as “Part 1.”

IEC 61968-1 is the first in a series of standards that, taken as a whole, define interfaces for the major elements of an interface architecture for Distribution Management Systems (DMS). This standard, referred to as Part 1, identifies and establishes requirements for standard interfaces based on an interface architecture. Subsequent standards will be developed in accordance with new work item proposals that cover each interface identified in Part 1.

At this stage, use cases, along with other available resources - like those from the CIRED Distribution Automation Working Group, EPRI CCAP and UCA projects and the Open Applications Group (OAG) – will be used to establish general requirements of a utility's inter-application integration infrastructure and to support the definition of the Interface Reference Model (IRM), which is shown in subclause 3.3. It is recognized that the IRM will need to be adjusted as WG14 learns during the development of Parts 3-10. A key objective of Part 1 is to clearly express the “rules of engagement” for information exchange among applications so that work on Parts 3-10 can be performed by separate teams operating in parallel, each team achieving consistent results with other teams. Once the IRM and requirements become relatively stable, Part 1 can move from the “CD” stage into the “CDV” stage.

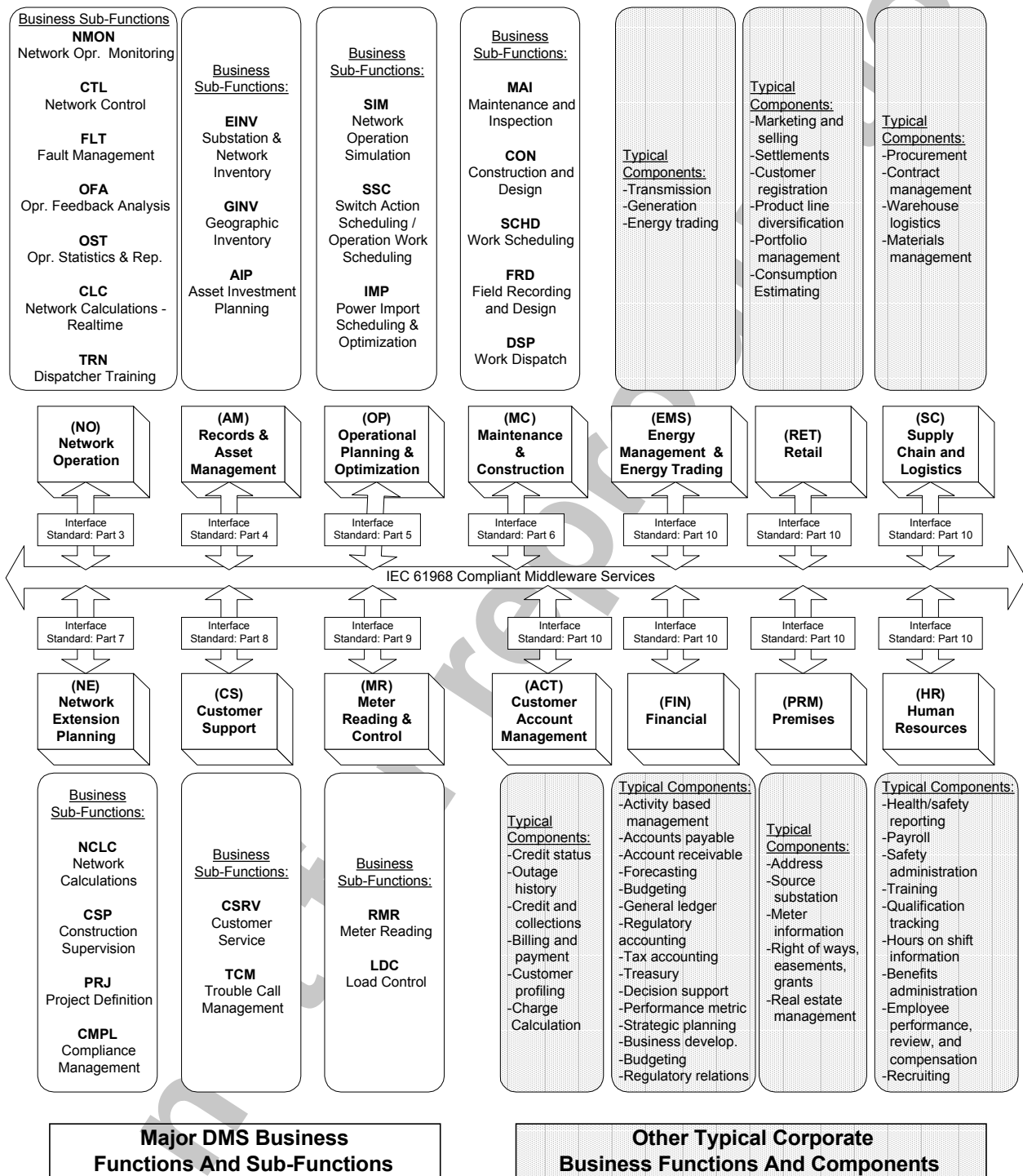
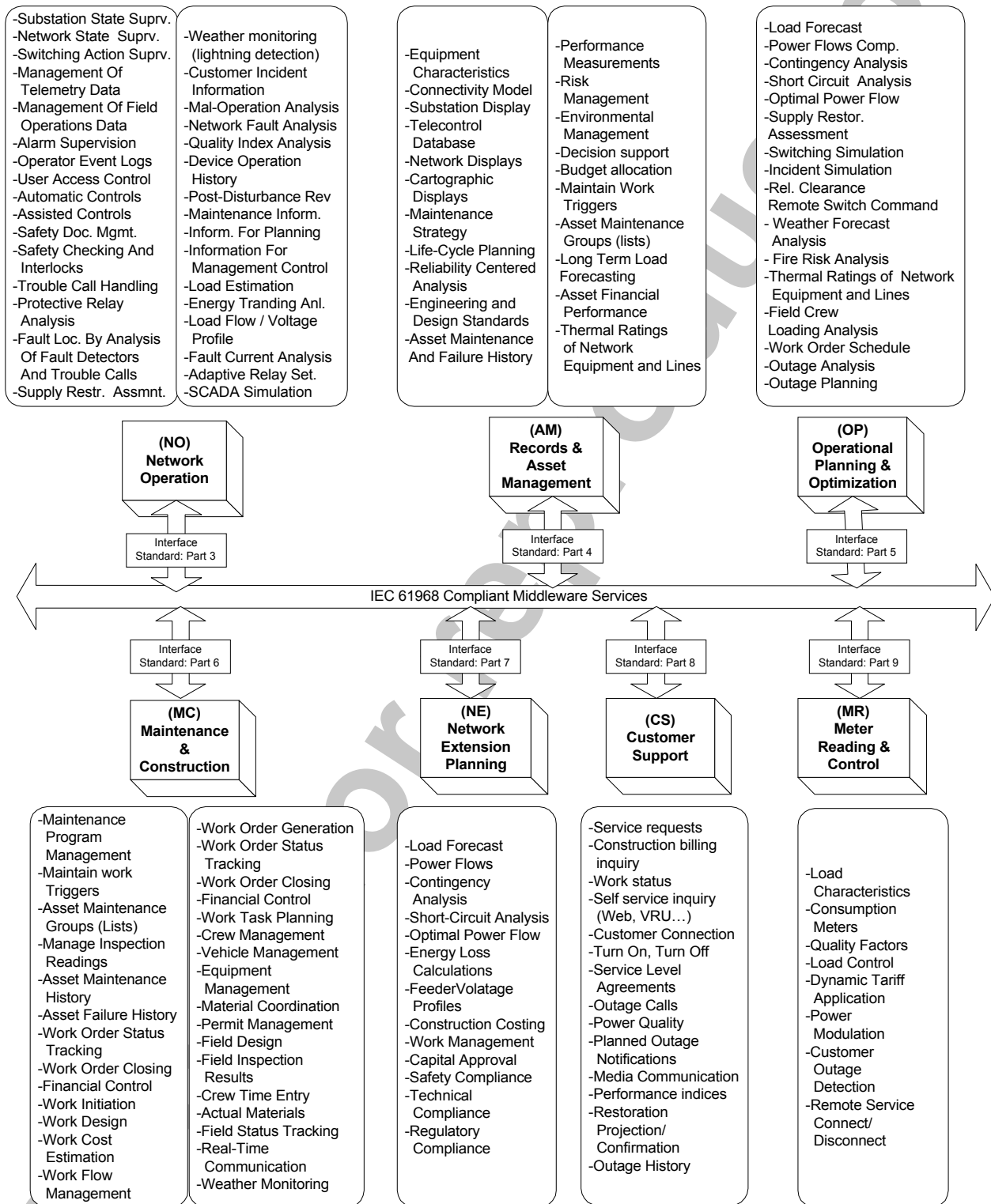


Figure B.3A: Typical Components Of Major DMS Business Functions



Typical Components Of The Major DMS Business Functions

Figure B.3B: Typical Components of the Major DMS Business Functions

B.3 Parts 3-10: Interface Standards For Business Functional Areas

A vertical team is established to develop each Part 3-10 Interface Specification identified in the IRM. The general process followed by each team is described in the following sub-clauses.

B.3.1 Part 3-10 Interface Specification Contents

The deliverables of each team include:

Normative:

- Message Type Table
(e.g., NewOutageRecord, UpdateOutageRecord, CancelOutageRecord)
Columns include: Class Name, Message Type Name, reference to Use Case(s)
- Message Type Definitions
Content (class/attribute pairs included in messages, references to part 11)

Informative:

- Integration Scenarios (and reference to use case) and/or Event Sequence Diagrams
 - Description (text)
 - Normal usage (e.g., request/reply, publish/subscribe, subscription topic, security level)
 - Pre-conditions (for the message type)
 - Post-conditions
 - Error conditions (application level only, not transport or work flow)
- Relevant Common Information Model (CIM) Package(s)

B.3.1.1 Step 1: Define Generic Use Cases

Each vertical team is to modify existing Use Cases and develop new Use Cases that establish typical information exchange requirements to/from the interface for that team's Business Function. Business Functions, one per Part 3-10 of the IRM, are groupings of Abstract Application Components. The purpose of use cases is to identify information to be exchanged among these components. It is not necessary to define the Producer/Consumer and Message Type columns during this step; this is done in step four of the process.

The aim of each Part 3-10 CD is to address 80% of the most commonly needed information exchange requirements.

NOTE Developing standards for information to be exchanged among abstract components within an IRM Business Function (i.e., internal to a vertical team's domain) is beyond the scope of WG14's current work plans. However, if in the team's judgement certain intra-business function information exchanges are commonly needed, the team may elect to define these information exchange message types. During the course of its work, it should also suggest change to the Interface Reference Model to more properly reflect inter-application integration needs of the industry.

When finished with this step for a given business process (use case), we should have the answers for:

- WHY is information exchange required i.e. what are the use cases?
- WHERE is it all happening i.e. what is a typical context?
- WHO are the actors who use the systems and/or applications?

Figure B.4: Use Case Template

Use Case <Number>: <Use Case Name>

Summary:

Actor(s):

Name	Role description

Participating Business Functions:

Acronym	Business Function/Abstract Component	Services or Information Provided

Assumptions / Design Considerations:

Normal Sequence:

Use Case Step	Event	Description Of Process	Information To Be Exchanged	ProducerTo Receiver Abstract Component	Message Type (Verb/Noun)

Integration Scenarios

Information Model for normal sequence:

Class	Class Attributes	Attribute Type	Operations	Relations

Pre-conditions:

Exceptions / Alternate Sequences:

Post-conditions:

Information Model for alternate sequence B: As-Built Update:

Interface Class	Class Attributes	Attribute Type	Operations	Relations

Message Type Table:

Message Type Identifier	Message Type (Verb/Noun)	Message Type Content (Class.Attribute)	Revision Number

References:

Issues:

ID	Description	Status

Revision History:

No	Date	Author	Description
1.			Original.
2			

Table B.1: Example steps in a Use Case (From Use Case 46: Data Acquisition for External EMS)

Use Case Step	Event	Description Of Process	Information To Be Exchanged	ProducerTo Receiver Abstract Component	Message Type (Verb/Noun)
1.1.	External system requests mapping of names to keys	External system sends list of names	Company.name Substation.name Equipment.name Measurement.name	EXT-EMS to AM-EINV (or NO-NMON)	RequestMeasurementIdentities
1.2.	Return numeric keys	looks up names zero or negative key means name(s) not found	As above plus MeasurementUnit.name Measurement.key	AM-EINV (or NO-NMON) to EXT-EMS	ShowMeasurementIdentities
2.	External system subscribes to required measurements	EXT sends list of keys. NMON sets up subscription table.	Measurement.key	EXT-EMS to NO-NMON	SubscribeMeasurementsKeys
3.	NMON system sends current values. This is an implicit acknowledgement to the subscription request	For each entry in each subscription table find most recent value.	Measurement.key MeasurementValue.value MeasurementValue.quality	NO-NMON to EXT-EMS	ShowMeasurementValues
4.	Telemetry system sends measurement event using RTU protocol	NMON Interprets RTU message; stores data in real time database; Calculates alarm states if any; raises alarms as necessary; logs changes as necessary;	Measurement.key MeasurementValue.value MeasurementValue.quality MeasurementValue.timestamp	In terms of IEC61968, this is all internal to NO-NMON	Not applicable

B.3.1.2 Step 2: Define Integration Scenarios

Summarize results of each message exchange among IRM parts in support of the use case with an Integration Scenario Diagram

Coordinate the definition of these scenarios with other vertical teams. UML Class Definitions for the Abstract Components of the IRM are the entities that exchange information in the Integration Scenario Diagrams. Vertical teams work with the Model Development Team (described below) to develop and maintain the WG14 Model. For a more complex interaction, it may be beneficial to first develop an Event Sequence Diagram in UML notation that articulates each type of message used in the sequence of message exchanges among IRM parts in support of the use case.

When finished with this step, we should have the answers for:

- WHEN (due to what events) should producers start data transfers?

This diagram shows the participating components and major information exchanges. The numbers refer to the sequence steps.

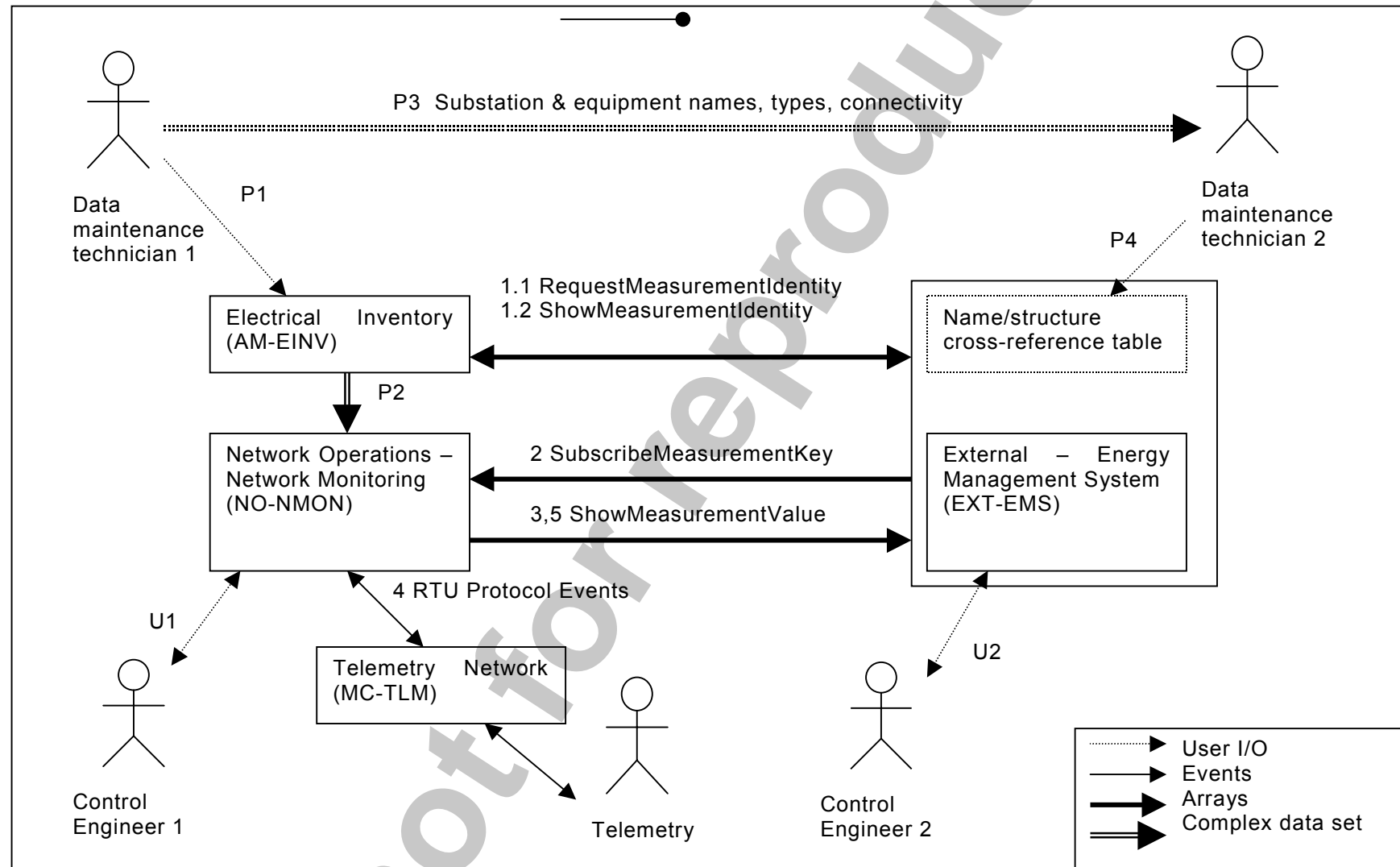


Figure B.5: Integration Scenario Example (From Use Case 46: Data Acquisition for External EMS)

B.3.1.3 Step 3: Identify And/Or Define CIM Class(es)

Referencing the Use Case template (above), this step is performed by defining an information model, as is shown in the example below

Table B.3: Information Model (From Use Case 46: Data Acquisition for External EMS)

Class	Class Attributes	Attribute Type	Domain	Relations
Company	Name	String	Globally unique	Company(1).operates. (1..N)Substations
Substation {isA.PowerSystemResource}	Name	String	Unique within Company	Substation(1).parent. .child(1..N)ConductingEquipment {Inherit from PowerSystemResource}
Equipment ConductingEquipment isA.PowerSystemResource}	Name	String	Unique with Substation	ConductingEquipment(1).has. (1..N)Terminals
Terminal	Name	String	Unique for type of equipment	Terminal(1).has. (1..N)Measurements
PowerSystemResource	Name	String		PowerSystemResource(1).has. (0..N)Measurements
Measurement	Name – Note 1 Key – Note 2	String Long integer		Measurement(1).has. (1)MeasurementUnit Measurement(1).has. (0..N)MeasurementLimit Measurement(1).has. (1..N)MeasurementValue
MeasurementUnit	Name – Note 3	Enumeration or String	kV, MW, MVAR, kA kW, KVAR, V, A etc.	
MeasurementLimit				Internal to NO-NMON system Or could be duplicated in EXT- EMS system
MeasurementValue	Value – Note 4	Double		Value of measured quantity
MeasurementValue	Quality	Bits		As IEC61850
MeasurementValue	TimeStamp – Note 2	Date/time		
MeasurementValue	AlarmState – Notes 2,5	Enumeration or String	NORMAL, HIGH, LOW etc.	

B.3.1.4 Step 4: Organise and add Message Type(s) to Message Summary in each applicable Part of IEC 61968

Organise message types into a Message Type Table.

Referencing the Use Case template (above), this step is performed by defining the Producer/Consumer and Message Type columns for each of the steps in the Use Case. Refer back to example use case steps above.

NOTE: The "verbs" are imperative case while the "nouns" are the objects of the verb.

Nouns are identified in the Distribution Information Exchange Model (IEC 61968-11), which is a subset of the IEC TC57 Common Information Model. In general, the following verbs shall be used unless they are inadequate to properly express the action.

Table B.5: Commonly used verbs

Verb	Meaning	OAG Equivalents
New	This the first time that data for this document ID has been published.	Add, Create
Change	Data has changed for this document ID since it was last published by New or Show.	Change
Show	A publication of data as a result of a Request or Subscribe.	Show, List, Sync
Close	No more data will be published for this document ID due to normal completion of activities e.g. CloseOutageRecord means all affected customers have supply restored.	
Cancel	No more data will be published for this document ID due to some sort of error, e.g. the document was created inadvertently. The message body might include information to assist the receiving components to rollback to a correct state.	Cancel
Delete	Any references to this document ID can be removed. This is the opposite of New. It may be used instead of or in addition to Close or Cancel	
Get Request	A request for data for a given document ID or set of documents. alternative to 'Get'. Request is a more correct term for asynchronous messaging, but Get is shorter and is an existing OAG verb (and used by listserv protocols)	Get, GetList Get, GetList
Ack	an acknowledgement that a document ID or set has been received	Acknowledge
Subscribe	a request for future messages for a set of documents based on some filter criteria	
Unsubscribe	a request to stop receiving messages for a set of documents based on some filter criteria	
	The following are discouraged as they are only applicable to certain document types but are in common usage. They could be defined as a set of standard options for document status.	
Approve	special form of Show status	
Decline	special form of Show status	
UnApprove	special form of Show status	
Lock	special form of Show status	
UnLock	special form of Show status	
Apply	special form of Show	
Issue	special form of Show	
Post	the same as Show followed by Close.	

In order that information may be exchanged with applications other than those included in the IEC 61968 series of standards, verb use is intended to be consistent with the verbs used by the Open Applications Group, which are summarized below:

OAG Verb	Meaning	61968 Equivalent
Add	A request for the receiving component to create a new (internal) document which is a duplicate copy of the information in the message.	replaced by New as that is a standard statement in Windows and C++.
Create	A request for the receiving component to create a new (internal) document based on 0 or more fields in the message.	replaced by New as there is little difference in meaning.
Post	A request for the receiving component to copy the document within its archiving system. The sending component may or may not require an Acknowledge message before deleting its internal version.	Show followed by Close
Change	A request that the receiving component updates its copy of a (internal) document based on the fields in the message. This may trigger additional processing	Change
Update	A notification for the receiving component that an event has occurred. The message need not specify a particular document.	replaced by Show or Change as there is little difference in meaning.
Acknowledge	A generic response to other verbs.	Ack
Getlist	A request for multiple document key information based on selection criteria in the message.	replaced by Get for a collection type of document.
List	The response to Getlist	replaced by Show for a collection type of document.
Get	A request for details of a single document described by the key information in the message	Get
Show	The response to Get	Show
Cancel	A request for the receiving component to cancel the document described in the message. This may mean deleting an instance in a database or simply marking the document as cancelled.	Cancel

Message Type entries for all Integration Scenarios included in an individual IEC 61968 part document will be organized in a single Summary Message Type Table. Each entry in the summary table will be used by at least one integration scenario, but many will be used by multiple integration scenarios. Note that, since each message is either to or from a component in another 61968 part, the identical message will also be shown in one or more other 61968 parts.

B.3.1.5 Step 5: Define/Revise Message Payloads For Each Message

After WG14 has reviewed and accepted the material used for defining Abstract Message Types (i.e., Use Cases, Integration Scenarios, IRM updates, CIM updates), define the message payload for each message. The following is an example of defining a message payload by defining the classes and attributes from the TC57 CIM model to be included in the message.

Message Type

Show Switching Schedule

(e.g. Permit to work, sanction for test, limitation of access, certificate of Isolation)

Document.*

Created By Person.*

Created By Person.Organization.*

Modified By Person.*

Modified By Person. Organization.*

Switching Schedule.*

Requested By Person.*

Requested By Person. Organization.*

Checked By Person.*

Checked By Person.Organization.*

Approved By Person.*

Approved By Person.Organization.*

Has [N] Work Order.ID

Has [N] Safety Document.ID

[N] Schedule Step.Sequence Number

[N] Schedule Step. Power Systems.Resource ID

[N] Schedule Step. Control Action

[N] Schedule Step. Step Status (Ready, Proposed, Instructed, Completed, Skip)

[N] Schedule Step Instructed. Time Stamp

[N] Schedule Step Completed. Time Stamp

Referencing the Use Case template (above), this step is performed by defining the contents of message by either filling Message Type Table. It may be helpful to define a Message Data Model, as shown in the example below:

When finished with this step, we should have the answers for:

- WHICH collections of entity references are required in information exchanges?

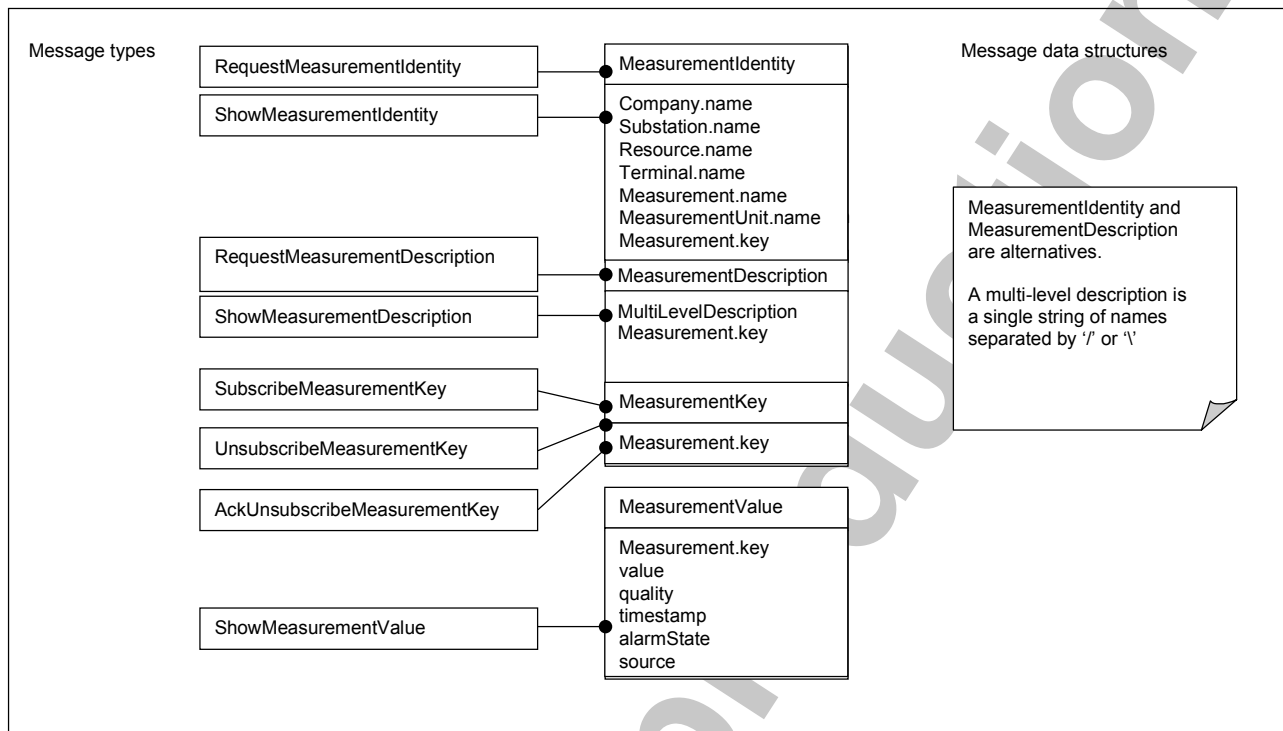


Figure B.6: Message Data Model Example (From Use Case 46: Data Acquisition for External EMS)

B.3.1.6 Step 6: Update Applicable Portions of IEC 61968

Document Editors build and revise appropriate portions of IEC 61968 based on deliverables from this process and input from authors.

B.4 WG14 CIM Model Development

The main purpose of the WG14 CIM Model is to provide a common language for describing exactly what data is being exchanged among Abstract Components of Business Functions (i.e., Part 3-10 Interface Specifications) within Use Cases. The Model Development Team must therefore ensure consistency in the naming and relationships of objects, attributes and elements and also how they are used in Message Type Definitions developed by vertical teams. UML Class Definitions for the Abstract Components of the IRM are the entities that exchange information. Vertical teams (described above) work with the Model Development Team to develop and maintain the WG14 CIM Model. It does this by developing and maintaining a domain object model, using UML notation, that strives for consistency with models used by:

The main purpose of the WG14 Model Development is to provide a common language for describing exactly what data is being exchanged among Abstract Components of Business Sub-Functions (i.e., Part 3-10 Interface Specifications) within Use Cases. The Model Development Team must therefore ensure consistency in the naming and relationships of objects, attributes and elements and also how they are used in Message Type Definitions developed by vertical teams.

The EPRI Control Center API (CCAPI) research project (RP-3654-1) created a Common Information Model (CIM) which provides a comprehensive logical view of Energy Management System information. The CIM is being standardized by WG13 (IEC 61970, Part 301). The CIM is an abstract model that represents all the major objects in an electric utility enterprise typically

contained in an EMS information model. This model includes public classes and attributes for these objects, as well as the relationships between them.

The IEC TC57 CIM is based on this and therefore the CIM has partitioned into subpackages. The Domain package defines datatypes used by the other packages. The following diagram shows the top level packages in the CIM.

NOTE: While packages have been allocated for use by IEC TC57 Working Groups 10 through 12 for IEC 61850, this was only a recommendation at the time this document was released to IEC (decision pending).

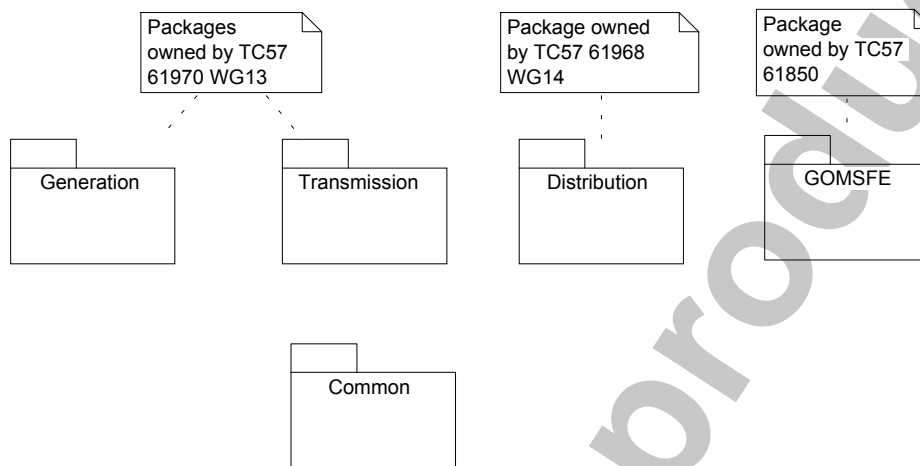


Figure B.7 - CIM Top Level Package

WG14 Vertical teams (described above) work with the Model Development Team to develop and maintain the WG14 Distribution Information Exchange Model (DIEM). Updates needed for the existing the TC57 Common Information Model (CIM) outside of the DIEM are also coordinated with the Model Development Team. The CIM, including the distribution subset (DIEM), is an object model expressed in UML notation.

NOTE: An objective for WG14 modeling is to maintain consistency with the Open Application Group (OAG) model in order to facilitate utility integration with Enterprise Resource Planning (ERP) and Supply Chain applications.

Packages defined by IEC TC57 WG14 are contained in IEC61968-11.

B.4.1 Step 1M: WG14 Model Team updates Distribution Information Exchange Model (DIEM), A Subset of the IEC TC57 CIM, with new/revised Class Definitions

WG14 will use the IEC TC57 CIM (including it's Data Dictionary) as the base for its modeling work.

B.4.2 Step 2M: WG14 Model Team works with WG13 and/or TC57 SPAG to reconcile updates to IEC TC57 CIM

WG14 will help shape plans for and participate in the development of a common TC57 Data Dictionary and Model. For work occurring in packages other than the 61968-11 packages, WG14 will work cooperatively with WG13 and TC57 in general to extend the TC57 CIM as needed for Distribution Management. WG14 will also use XML Namespaces in Message Type Definitions to identify the CIM and other industry models (e.g., OAG).

When finished with this step, we should have the answers for:

- *WHAT are the physical entities modelled in each IRM Business Function for which data may need exchanging?*

Annex C (informative)

Inter-Application Integration Performance Considerations

C.1 Example of Loading Scenarios

Performance is normally defined against three loading scenarios as follows:

- Normal loading
- High loading
- Storm loading

The following typical scenarios assume 2.5 million customers, assume full availability of the distributed servers.

Table C.1: Typical Load Scenario

	Normal	High	Storm
Call Takers	4	40	200
Total calls for all call takers	13/hour	400/hour	7560/hour
Despatchers	4	10	44
Faults despatched for all despatchers	4/hour	50/hour	200/hour
Control Engineers	7	10	20
Telecontrol operations total	1/min	5/min	40/min
Manual operations total	10/min	25/min	100/min
Diagram loading total	10/min	25/min	100/min
Access to plant details total	1/min	2/min	10/min
Combined telecontrol events	300/hour	1000/hour	3000/hour

Testing is normally performed for storm loading conditions. The Normal and High loading figures are provided for information only.

C.2 Transaction Volumes

It is also worth noting the typical transaction volume for DMS.

Table C.2: Example of typical transaction volume for DMS

	Average/Unit	Minimum/Unit	Maximum/Unit	Future Estimates
Customer Calls	300/day	90/day	100 000/day	37600 *
SCADA Alarms / Events	300/hour		3 000/hour	
Limit violation alarms	50/day			
Faults (HV)	5 000/year		1 000/day	
Faults (LV)	6 100/year			
Faults (LV non-reportable)	31 500/year			
Outages (EHV/HV)	19 000/year			
Safety Documents for Primary	10/outage			
Safety Documents for Secondary	3/outage			
Planned switching schedules (HV)	12 000/year			
Unplanned switching schedules (HV)	6 800/year			
Protection setting changes	10/day			
Analysis (load flow)	100/week			
Analysis (short circuit)	100/week			
Analysis (state estimator)	N/A			
Contingency Analysis	N/A			
SCADA Telecontrol operations	700-800/day			
Customer notification of planned outages	261 000/year			
Customer call backs	200/year			
Network dressing operations	600/hour		4 000/hour	
Despatching of staff	200 teams/day	90 teams/day	1 500 teams/day	
Standby list changes	5/day			
Staff changes	4/week			
Severe storms	3/year			
VP messages	4/day			

NOTE: This table assumes that all LV Faults are also reportable.

Annex D (informative)

Views Of Data In A Conventional Electric Utility

The business of the utility is based on its network and plant as the prime structure for operating the generation, transmission or distribution process. With this in mind, the analysis concentrates on plant and equipment definition. By taking a helicopter view of the whole process and zooming in to the software level where the structure defines the exchange of data items related to modelling individual equipment values, it is necessary to indicate some important aspects which are often overlooked when designing applications or systems, and ignoring their imbedding in a broader environment.

D.1 Classification

The dimensions that need to be considered in a company-wide data description are:

- Geography
- Time
- Financial
- Physical

In bringing data together, different views must be accounted in relation to figure D.1:

- The strategic planner has a view of the network for typically many years ahead with forecasts of energy growth, urban expansion and industrial sites, new and decommissioned plant, etc.
- The construction engineer has a view of the network for typically several years ahead with CAD plans, supplier's specifications, commissioning schedules and geographical layouts of construction sites and rights of way.
- The operations engineers have a view of the network today and in the next few months with switching plans, generation schedules, outage schedules, contingency plans and short-term forecasts.
- The contracts department has a view of who is to supply or take power on a contractual basis, and over which lines, and how losses are to be shared.
- The finance department has a view of which plant is owned or shared, who is responsible for the facilities, and the profit/loss statements for the year.

Thus, a consistent way of modelling the data in a Utility Information System (UIS) must classify the different data views expressed above and allow for a smooth passage as one moves along one of the data definition dimensions. Various users have different requirements on the physical model and these change with time. The data must therefore be classified by the areas of interest within the Utility and thus corresponding data management concepts proposed (e.g. - who has responsibility for what, who ensures that the information is in the right place at the right time).

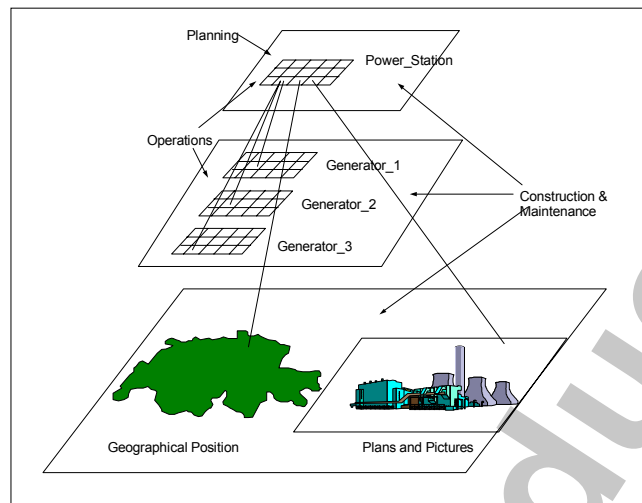


Figure D.1: Database views depend on the time and user

D.2 Identification

Within the business framework, the electricity companies form a geographical block. There is a hierarchical framework that seems to be applicable to all networks with Regions divided into Areas which are operated by a collection of companies.

- A Region is a large geographical networked complex
- Areas are subsets of the region usually with a regulation philosophy exchanging energy with other areas through specific tie lines.
- Companies are the operational entities responsible for their network considering the exchange of energy with other companies in the area and operating with the same regulation philosophy.

Companies operate in an environment where there is responsibility for generation, transmission and distribution. The general trading agreements allow generation to be sold to consumers and the costs of transmission to be covered by the suppliers based on their loading. Losses are covered as part of this cost.

Thus there is a structure in the "**company world**" and another in the "**network world**". In dealing with the data structures, the network elements and companies form a united representation. For example, each element has an owner or owners, each company has contracts with other companies and end users. Connections between the physical process and the business process are modelled in the data structure.

Within this framework, each item has to be uniquely identifiable, thus labelling the network is an important aspect of any classifying structure. In general it is necessary to consider what aspects of data usage and transfer are being covered to ensure that different functions are easily identified. For example:

- For on-line operation and supervision systems, usually the network is mapped by topology, and represents a time slice. Line segments, geographical position and elevation is irrelevant; the line segments and tower types are not considered. Typical identification relates to station name codes and voltage levels.
- Network planning involves in the first instance an analysis of the electrical process and as such involves introduction of new equipment or elements, removal or replacement of existing

equipment. In this activity, the network evolves in time, albeit not continuously, and the time parameter characterises one network layout from another.

- Transforming the planning results to real equipment requires a transformation from a theoretical result based on element type. Each element type has a set of basic physical characteristics, which become concrete with the choice of the equipment.
- The actual choice of equipment relies not only on the technical requirements but also on the geographical position and the terrain. Thus, the geographical co-ordinates represent an integral part of the description of the network when planning is involved.
- the physical characteristics of the elements must include a layer principle so that only relevant data is projected into the application. Thus a line for a load flow calculation depends only on the total length. Whereas for maintenance, or construction, the segment lengths and connection to the tower elements must be apparent.

The financial dimension to the data structure requires that the various elements in the system are labelled by the **owner company/companies**. It is not unusual for elements such as generators or lines to be owned by more than one company. In this case, the evaluation of the generation, transmission rights, losses, etc. is an important aspect in the business of the electrical utility. The **Company Identifier** is also required to label data items such as:

- power contracts
- power efficiency
- load statistics
- environmental credits

Annex E (informative)

Business Functions

Most utilities utilise a variety of systems to assist their staff in DMS work. These may include:

SCADA/NMS	Real-time system to support the control-room operation, including data acquisition and supervisory control utilising RTUs in the substations.
Network calculation	A suite of applications software used to analyse the capacity, efficiency and reliability of the power network.
GIS	Geographical Information System to provide spatial and other information about the power network.
Customer Information	Customer outage management, crew scheduling
Metering and Load management	Remote meter-reading, time-of-use management, service connect/disconnect
Billing system	Electronic billing, customer account enquiries
Work Management	Work order scheduling and tracking, manpower assignment, preparation of Bills of material, cost estimating and monitoring.

A typical profile using IEC 61968 systems by a utility for each business function of the IRM is shown below (figure E.1):

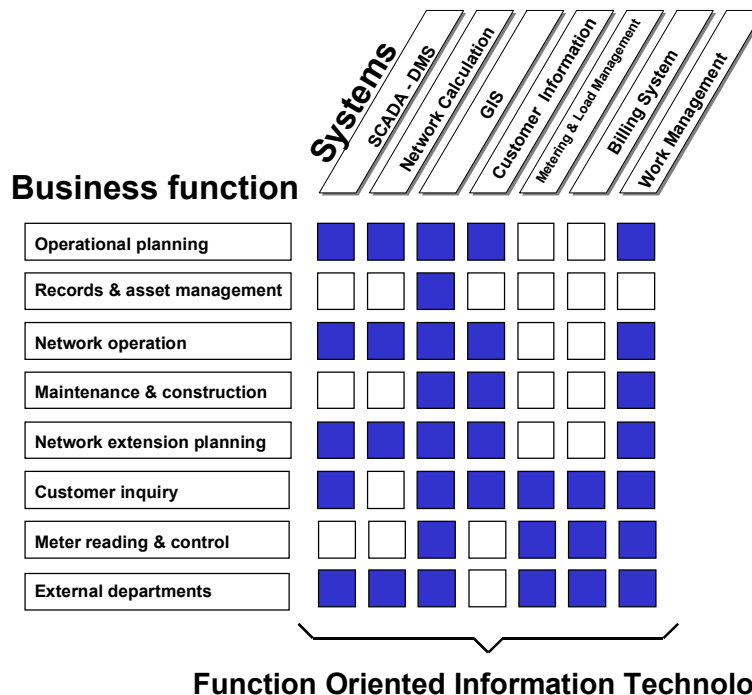


Figure E.1: Map of Typical utility systems to the business functions of the IRM

Information typically exchanged among systems implementing the business functions of the IRM is shown below (table E.1):

Information To Be Exchanged:	Business Functional Areas:													
p = producer; c =consumer	Operational Planning & Optimization	Records & Asset Management	Network Operation	Maintenance & Construction	Network Extension Planning	Customer Inquiry (www, outage ETR, connection, customer data)	Meter Reading & Control	Customer Account Management	Premises (address, source substation, meter information)	EMS Control Centers	Financial	Human Resources	Weather	Energy Trading
Load / Usage Data	p/c		p/c	c	c	c	p			p/c			p	c
Outage Data	c	c	c	c				p		c				c
Trouble Call Records	c	c	p			c	p	c		c	c		p	
Customer Related Emergency Data	c		p/c				p	c		p/c				
Remote Meter Reading Requests						p	c	p	p					
Remote Service Connect / Disconnect Requests			c			p	c	p	p					
Capital Expenditure Requests	p	p	p	p	p						c	p		
New Service Requests	c	c		c	p/c	c	c	p/c	p/c		c			
Line Extension Requests	c	c	p	c	p/c			p			c			
Market Sales Statistics					c			p/c			c			
Meter Theft / Tamper Detection Data						c	p	c						
Meter Customer Outage Detection	c		c			c	p	c		c				
Time-Of-Use Meter Programming Data			c			c	p/c	c						
Real-Time Prices			c			c	c	c			c			p
Electronic Billing						c		p			c			
Updates To Facilities	c	p/c		p/c	c									
Network Model Updates	p/c	p/c	p/c	c	p/c				c					
Network As-Built Updates	c	c	c	p/c						c				
Equipment Characteristics	c	p/c	c	p/c	c					c				
Equipment Drawing Specifications		p		c										
Facilities Map of Service Territory	p/c	p	c	p/c	c	c				c				c
Cartographic Maps	c	p	c	c	c	c	c	c	c	c				
Landbase Maps		p	c	c	c	c		c		c				
Outage Statistics	p		c	c	c			c		c	c			
Equipment operation statistics	c	c	p/c	c						p/c				
Maintenance Requests	c	c		p/c				p/c						
Maintenance Scheduling	p/c	c	c	p						p/c				
Load Survey Requests	c		c		p		c	p						
Load Forecasts Information	p		c	c	p			c		p/c				
Load Shedding	p/c		c							p/c				
Load Control			p/c							p/c				
Outage Schedules	p		p/c	p/c		c		c		p/c				
Requests To Drop Lines	p		p/c	p/c				c						
Protective Relay Settings			p/c	c	c					p/c				
Protective Relay Data	c		p/c	c	c					c				
Fault Locations Estimates	c		p/c	p/c						c				
Network Monitoring Data	c		p/c	p/c	c					p/c				
Release / Clearance Remote Switch Command Scheduling - unvalidated	p		p/c	p						c				
Release / Clearance Remote Switch Command Scheduling - validated	c		p	c						c				
Safety Information	c		p	c	c					c		c		
Interruptible Customer List	c		c	C				p/c			c			
Work & QA Standards		p	c		p					c		c		
Purchase Requests		p/c	c	C	p			p			p/c			
Skills Inventory			c	c						c			p	
Crew Dispatch	c		p/c	p/c		p							c	
Crew Dispatch Schedule	p		c	c		c		c		c			c	
Crew Tracking Reports	c		p	p/c		c		c		c			c	
Time Records By Work Order				c						c		p		
Equipment Tracking Reports		p	p/c	p/c						c				
New Construction Records		c	c	p			c	c		c				

Figure E.2: Typical information exchanged among business functions of the IRM