The Integrated Energy and Communication Systems Architecture

Volume IV:
Technical Analysis

Appendix E:
Environments

EPRI Project Manager

Joe Hughes

Cosponsor

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

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

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

ORGANIZATIONS THAT PREPARED THIS DOCUMENT

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

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

ORDERING INFORMATION

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

CITATIONS

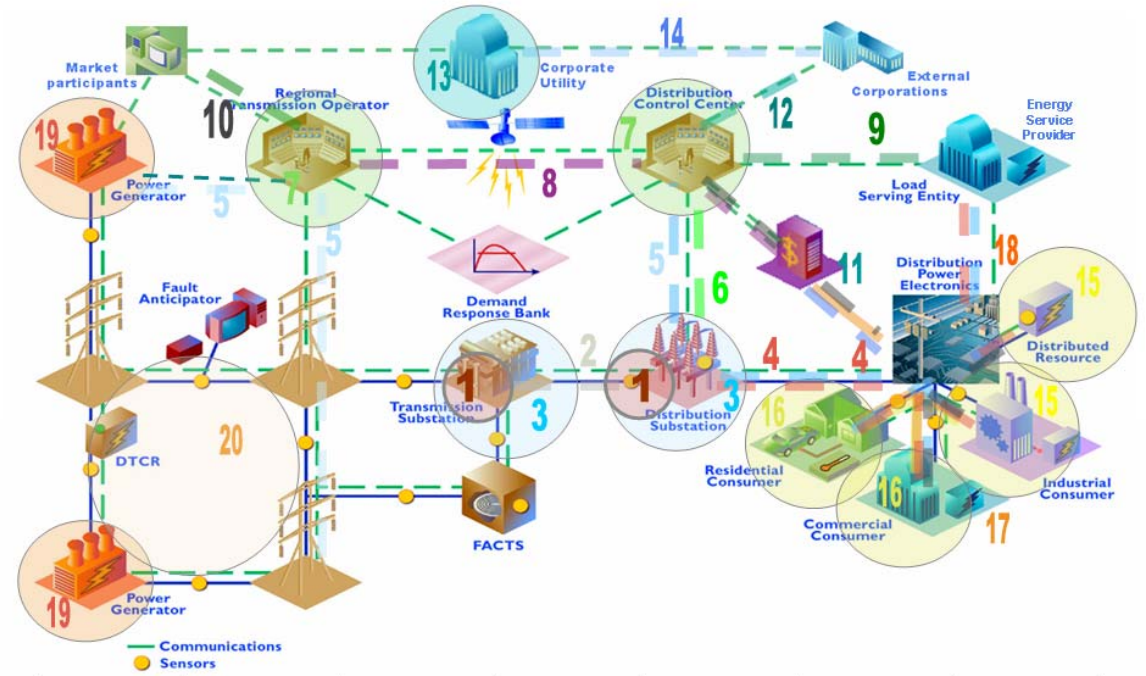
This document describes research sponsored by EPRI and Electricity Innovation Institute. The publication is a corporate document that should be cited in the literature in the following manner:
THE INTEGRATED ENERGY AND COMMUNICATION SYSTEMS ARCHITECTURE, EPRI, Palo Alto, CA and Electricity Innovation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

Table of Contents

This page intentionally left blank.

IECSA Environments

An IECSA Environment is defined as an environment where one or more of the information exchanges of different functions have essentially the same architectural requirements



1 Deterministic Rapid Response Intra-Substation	4 Inter-Field Equipment	7 Intra-Control Center	10 RTOs / Market Participants	13 Intra-Corporation	16 Intra-Customer Site	19 HV Generation Plant
2 Deterministic Rapid Response Inter-Site	5 Critical Operations DAC	8 Inter-Control Center	11 Control Center / Customer Equip	14 Inter-Corporation	17 Inter-Customer Sites	20 Field Equipment Maintenance
3 Critical Operations Intra-Substation	6 Non-Critical Operations DAC:	9 Control Centers / ESPs	12 Control Center / Corporations	15 DER Monitoring and Control	18 Customer / ESP	21 Special

Figure: IECSA Environments in Power System Operations - Click on a number to link to an Environment

What is an IECSA Environment?

IECSA defines an ***Environment*** as a logical grouping of power system requirements that could be addressed by a similar set of distributed computing technologies. Within a particular environment, the information exchanges used to perform power system operational functions have very similar architectural requirements, including their:

- Configuration requirements
- Quality of service requirements
- Security requirements
- Data management requirements

An IECSA environment groups the requirements of the information exchanges, not necessarily the location of the applications or databases (although these may affect the information exchanges and therefore the environment).

The requirements used to define the IECSA environments have been derived from the Use Cases described in Volume II. These Use Cases were in turn developed from industry stakeholder contributions. Since the power system functions defined in these Use Cases may require multiple types of information exchanges, a particular power system function (or Use Case) may cross several environments.

A name and a number represent each environment. The Figure below lists each environment and illustrates how they may be physically located within the power utility. The Table below briefly summarizes the differences between the environments.

It should be noted that locally there may be some valid "sub-environments" within what is defined here as a single IECSA environment. Consumer sites, for instance are shown as single "Intra-Customer" environment. Consumer sites, however, may have separate networks for building automation and controls that coexist with corporate office networking environments.

The sections that follow describe each environment. Each section first describes the environment generally in terms of history, typical applications, characteristics, and what makes it distinct from the other environments. This description is followed by a more rigorous list of requirements that defines each environment. This set of requirements is derived from the "architectural issues" that were gathered during stakeholder engagement.

No.	Name	Security	QoS	Config	Data Mgmt	Sub	CC	Field	Cust	Bus
1	Deterministic Rapid Response Intra-Sub		H	H		Y				
2	Deterministic Rapid Response Inter-Site	M	H	H	H	Y	Y	Y		
3	Critical Operations Intra-Substation	H	M	H		Y				
4	Inter-Field Equipment			M				Y		
5	Critical Operations DAC	H	M	H	H	Y	Y	Y		
6	Non-Critical Operations DAC		M			Y	Y	Y		
7	Intra-CC		M		H		Y			
8	Inter-CC	H		M	H		Y			

9	CC to ESP	H		M	H		Y			Y
10	RTO to Market Participant	H		M	H					Y
11	CC to Customer Equipment	M	M	H	H		Y		Y	
12	CC to External Corporations	H			H		Y			Y
13	Intra-Corporation	M		H	H		Y			Y
14	Inter-Corporation	H		M	H					Y
15	DER Monitoring and Control	H	M	H	H		Y		Y	
16	Intra-Customer Site	M	H						Y	
17	Inter-Customer Site	H		H				Y	Y	
18	Customer to ESP	H		H					Y	Y
19	HV Generation Plant	H	M	H		Y				
20	Field Equipment and Maintenance	M		H	H	Y		Y	Y	

Table Summary of IECSA Environment Requirements

General ratings for Security, Quality of Service (QoS), Configuration (Config) and Data Management (Data Mgmt)

H = high level of requirements; M= medium level of requirements; blank = low level of requirements

Indications of physical locations: Substation (Sub), Control Center (CC), Field Devices (Field), Customer site (Cust), Business (Bus)

Y= Yes, involves communication with that physical location.

Basic IECSA Environments

- **1. Deterministic Intra-Substation:** High speed intra-substation environment (e.g. protective relaying, direct monitoring of power system parameters by CTs and PTs)
- **2. Deterministic Inter-Site:** High speed inter-site (e.g. distance protective relaying, FSM)
- **3. Critical Operations Intra-Substation:** High security intra-substation environment (e.g. monitoring and control of IEDs, setting protective relay and other substation equipment parameters, …)
- **4. Inter-Field Equipment:** Inter-field devices environment (e.g. monitoring and control of IEDs on feeders, …)
- **5. Critical Operations DAC:** High security between control center and field equipment environment (e.g. monitoring and control by SCADA of substation and DA

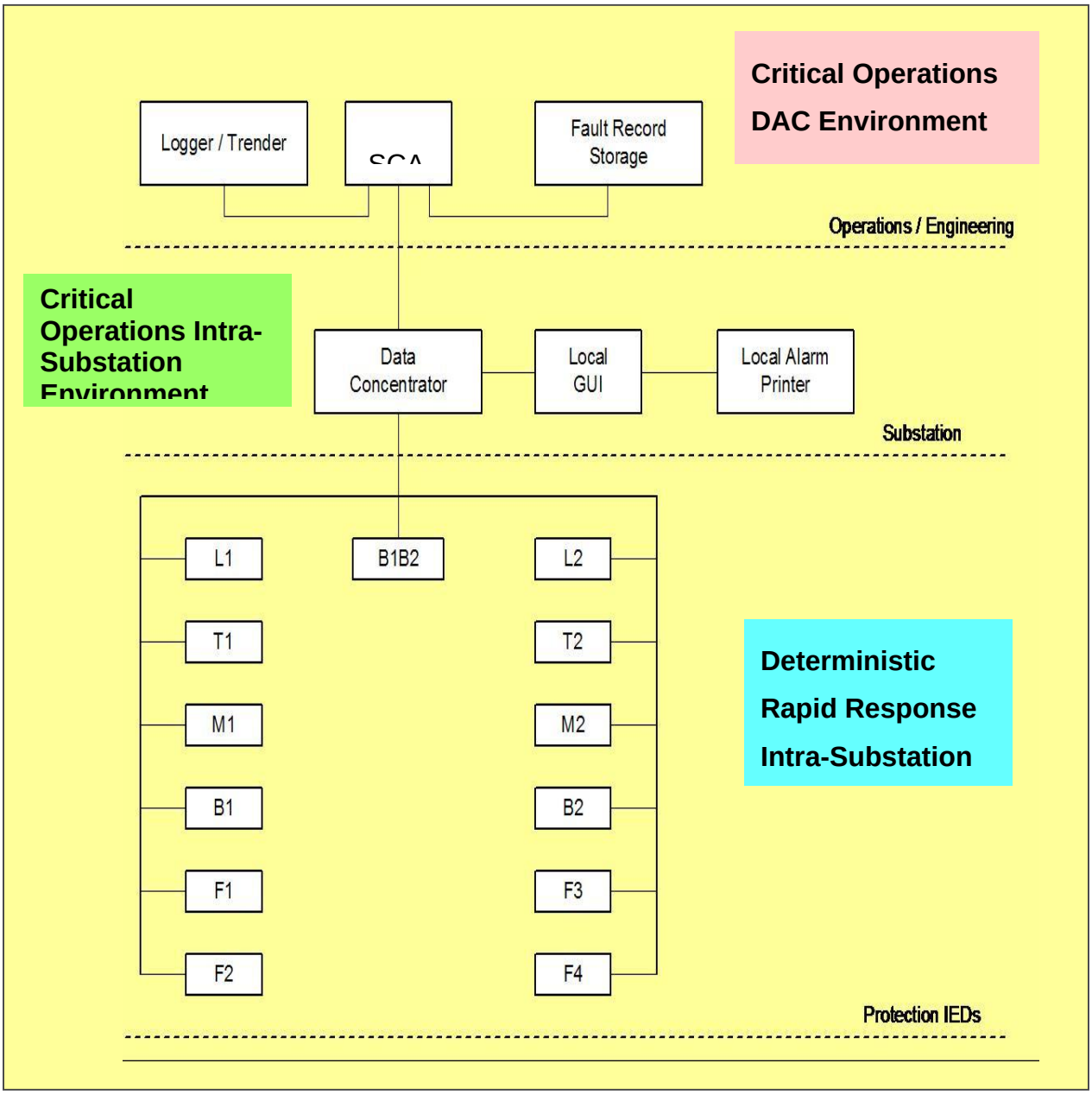
equipment, monitoring and control of DER devices, monitoring of security-sensitive customer meters, monitoring and control of generation units)

- **6. Non-Critical Operations DAC:** Lower security interactions among control center, substation, field equipment, customer sites environment (e.g. monitoring non-power system equipment, less security-sensitive substations, customer site PQ monitoring, customer metering)
- **7. Intra-Control Center:** Within one control center (e.g. SCADA system, EMS system, ADA functions, real-time operations)
- **8. Inter-Control Center:** Among control centers (e.g. between utility control centers, between RTOs, between remote subsidiary or supervisory centers)
- **9. Control Centers to ESPs:** Between utility control centers and ESPs/Aggregators (e.g. RTP, metering and settlements, market operations)
- **10. RTOs to Market Participants:** Between utility/RTO/ISO control centers and Market Participants (e.g. market operations)
- **11. Control Center to Customers:** Between customer equipment and utility control centers (e.g. customer metering, demand response interactions, DER management)
- **12. Control Center to Corporations:** Between control centers and external corporations (e.g. weather data, regulators, auditors, vendors)
- **13. Intra-Corporation:** Within corporate utility (e.g. planning, engineering, ADA access to AM/FM and customer information systems, arena addressed by TC57 WG14)
- **14. Inter-Corporation:** Between corporate utility and external corporations (e.g. e-business)
- **15. DER Monitoring and Control:** Between DER and ESP (e.g. ESP as Aggregator performing monitoring and control)
- **16. Intra-Customer Site:** Within a customer site (e.g. building management systems, DER management)
- **17. Inter-Customer Sites:** Between customer sites (e.g. microgrid management)
- **18. Customer to ESP:** Between customers and ESPs, Aggregators, MDMAs (e.g. DER management, customer metering, RTP, demand response)
- **19. HV Generation Plant:** Within an HV Generation Plant site (e.g. within the electrical and physical site of the generating plant up to the point of common coupling with the area power system)
- **20. Field Equipment Maintenance:** Maintenance of field equipment

- **User Interface:** User Interfaces and Person-to-person interactions (not technical environments)
- **Special:** Special environments ...

Example of IECSA Environments

An example of three IECSA environments is shown below



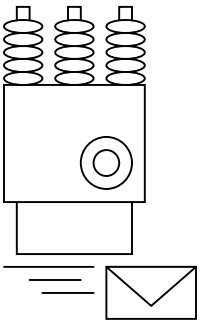
Generic List of Requirements with Recommended Technologies, Services, and Best Practices

- **Provide point-to-point interactions between two entities**
- **Support interactions between a few "clients" and many "servers"**
- **Support interactions between a few "servers" and many "clients"**
- **Support peer to peer interactions**
- **Support interactions within a contained environment (e.g. substation or control center)**
- **Support interactions across widely distributed sites**
- **Support multi-cast or broadcast capabilities**
- **Support the frequent change of configuration and/or location of end devices or sites**
- **Support mandatory mobile communications**
- **Support compute-constrained and/or media constrained communications**
- **Provide ultra high speed messaging (short latency) of less than 4 milliseconds**
- **Provide very high speed messaging of less than 10 milliseconds**
- **Provide high speed messaging of less than 1 second**
- **Provide medium speed messaging on the order of 10 seconds**
- **Support contractual timeliness (data must be available at a specific time or within a specific window of time)**
- **Support ultra high availability of information flows of 99.9999+ (~1/2 second)**
- **Support extremely high availability of information flows of 99.999+ (~5 minutes)**
- **Support very high availability of information flows of 99.99+ (~1 hour)**
- **Support high availability of information flows of 99.9+ (~9 hours)**
- **Support medium availability of information flows of 99.0+ (~3.5 days)**
- **Support high precision of data (< 0.5 variance)**
- **Support time synchronization of data for age and time-skew information**
- **Support high frequency of data exchanges**
- **Provide Identity Establishment Service (you are who you say you are)**
- **Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)**
- **Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)**
- **Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)**
- **Provide Security Against Denial-of-Service Service (unimpeded access to data to avoid denial of service)**
- **Provide Inter-Domain Security Service (support security requirements across organizational boundaries)**
- **Provide Non-repudiation Service (cannot deny that interaction took place)**
- **Provide Security Assurance Service (determine the level of security provided by another environment)**
- **Provide Audit Service (responsible for producing records, which track security relevant events)**

- **Provide Identity Mapping Service (capability of transforming an identity which exists in one identity domain into an identity within another identity domain)**
- **Provide Credential Conversion Service (provides credential conversion between one type of credential to another type or form of credential)**
- **Provide Credential Renewal Service (notify users prior to expiration of their credentials)**
- **Provide Security Policy Service (concerned with the management of security policies)**
- **Provide Policy Exchange Service (allow service requestors and providers to exchange dynamically security (among other) policy information to establish a negotiated security context between them)**
- **Provide Single Sign-On Service (relieve an entity having successfully completed the act of authentication once from the need to participate in re-authentications upon subsequent accesses to managed resources for some reasonable period of time)**
- **Provide Trust Establishment Security Service (security verification across multiple organizations)**
- **Provide Path and Routing Quality of Security (being able to determine a secure communication path)**
- **Provide Firewall Transversal**
- **Provide Privacy Service (the ability to ensure person information is not disclosed)**
- **Provide User Profile and User Management (combination of several other security services)**
- **Provide Security Protocol mapping (the ability to convert from one protocol to another)**
- **Provide Quality of Identity (the ability to determine the merit of converted credentials)**
- **Provide Security Discovery (the ability to determine what security services are available for use)**
- **Provide Delegation Service (delegation of access rights from requestors to services, as well as to allow for delegation policies to be specified)**
- **Provide Network Management (management of media, transport, and communication nodes)**
- **Provide System Management (management of end devices and applications)**
- **Support the management of large volumes of data flows**
- **Support keeping the data up-to-date**
- **Support extensive data validation procedures**
- **Support keeping data consistent and synchronized across systems and/or databases**
- **Support timely access to data by multiple different users**
- **Support frequent changes in types of data exchanged**
- **Support management of data whose types can vary significantly in different implementations**
- **Support specific standardized or de facto object models of data**

- **Support the exchange of unstructured or special-format data (e.g. text, documents, oscillographic data)**
- **Support transaction integrity (consistency and rollback capability)**
- **Provide discovery service (discovering available services and their characteristics)**
- **Provide services for spontaneously finding and joining a community**
- **Provide protocol conversion and mapping**

Deterministic Rapid Response Intra-Substation Environment - #1



The two Deterministic Rapid Response environments carry data exchanges that were previously considered too fast, too high volume, or too deterministic to carry on a generalized network. These data exchanges traditionally took place either within a single device or on dedicated lines.

Typical applications: Advances in technology have now made it possible to exchange data over LANs and WANs:

- Between protective relays to coordinate protection schemes
- Between those devices sampling measurements (e.g. smart current or voltage transformers) and those processing the data
- Between multiple devices that are distributing other real-time processes that previously took place on a single device, e.g. process control. Another name that has been used for Deterministic Rapid Response Intra-Substation is “process bus”.

Characteristics: The Deterministic Rapid Response environments require extremely high speed, high volume, or both, with timing requirements measured in milliseconds or lower. Violation of these requirements might cause equipment damage or safety issues.

Similar Environments: The Deterministic Rapid Response Intra-Substation environment is limited within the physical boundaries of the substation. Its security requirements can therefore be somewhat lower, and its timing requirements somewhat stricter, than Deterministic Rapid Response Inter-Site. Data management is not a major concern because of its limited scope.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Provide point-to-point interactions between two entities
- Support interactions within a contained environment (e.g. substation or control center)

Quality of Service Requirements

- Provide ultra high speed messaging (short latency) of less than 4 milliseconds
- Support extremely high availability of information flows of 99.999+ (~5 minutes)
- Support high precision of data (< 0.5 variance)

- Support time synchronization of data for age and time-skew information

Security Requirements

- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Security Policy Service (concerned with the management of security policies)

Data Management Requirements

- Support keeping data consistent and synchronized across systems and/or databases
- Support specific standardized or de facto object models of data

---

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Part 7-2 – GSE (GOOSE and GSSE** - Configuration, Quality of Service,
- **IEC61850 Part 7-2 – SMV (Sampled Measured Values)** - Configuration,
- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Quality of Service, Data Management
- **IEEE C37.94 - Standard for N x 64 kbps Optical Fiber Interfaces between Teleprotection and Multiplexer Equipment** - Quality of Service,

Communications Industry Technologies

Link Layer and Physical Technologies

- **Ethernet** - Quality of Service,
- **Bridges/Switches** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration, Quality of Service,

Wireless Technologies

- **Global Positioning System (GPS)** - Quality of Service, Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,

General Security Technologies

- **Role-Based Access Control** - Security,
- **Service Level Agreements (SLA)** - Security,

Application Layer Security Technologies

- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **IEC 62351-7 Objects for Network Management** - Quality of Service, Data Management

---

Recommended Common Services

Security Services

Common Security Services

- **Authorization for Access Control** - Security,
- **Security Policies** - Security,

Network and System Management Services

Enterprise Management Services

- **System/Network Health-Check Analysis** - Quality of Service,
- **System/Network Fault Diagnosis** - Quality of Service,
- **System/Network Performance Analysis** - Quality of Service,

Data Management Common Services

Data Management Services

- **Address and Naming Management** - Data Management
- **Network Time** - Data Management

Common Platform Services

Recommended Best Practices

Data Management Best Practices

Data Management

- **Alternate Communication Channels** - Quality of Service,
- **Backup Data Sources** - Quality of Service,
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Quality of Service, Data Management
- **Time Stamping** - Quality of Service, Data Management
- **Data Update Management** - Data Management
- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Quality of Service, Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Quality of Service,

Security Best Practices

Security Technology Documents

Alternative Best Practices

Data Management

- **Data Backup and Logging** - Quality of Service,

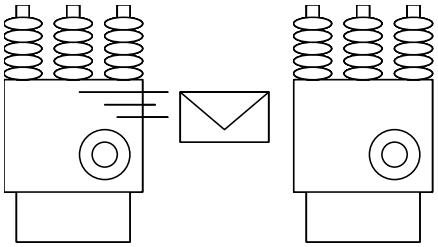
IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service,

Other Security Technologies

- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,

Deterministic Rapid Response Inter-Site Environment - #2



The Deterministic Rapid Response Inter-Site environment represents a set of requirements primarily concerned with the system-wide stability and reliability of the power grid. When implemented on general networks rather than dedicated lines, it is even newer than its Intra-Substation counterpart, with only a few pilot projects currently underway.

Typical Applications: Sending protection, samples, phasor measurements, and process control information between sites in real-time enables applications that can coordinate functions at a grid level and anticipate problems rather than just reacting to them. The simplest use of this environment may be transmission line protection, while more complex applications might involve real-time contingency analysis. These applications may be coordinated between field equipment, between multiple substations, or between substations and other sites such as control centers.

Characteristics, and Similar Environments: The Deterministic Rapid Response Inter-Site environment has higher security requirements and lower timing requirements than Deterministic Rapid Response Intra-Substation. However, violations of its timing requirements might still cause equipment damage, safety concerns, or network instability issues. Volumes of this type of data exchange are small so far but have the potential to be enormous if the quest for grid stability causes data to be directly measured that previously was only estimated. This could make data management concerns for this environment much greater than its Intra-Substation counterpart.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions across widely distributed sites

Quality of Service Requirements

- Provide ultra high speed messaging (short latency) of less than 4 milliseconds
- Support high precision of data (< 0.5 variance)
- Support time synchronization of data for age and time-skew information

Security Requirements

- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Security Policy Service (concerned with the management of security policies)

Data Management Requirements

- Support keeping data consistent and synchronized across systems and/or databases
- Support specific standardized or de facto object models of data

---

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Part 7-2 – GSE (GOOSE and GSSE** - Configuration, Quality of Service,
- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Quality of Service, Data Management
- **IEC61850 Power Quality Object Models** - Quality of Service, Data Management
- **IEEE C37.94 - Standard for N x 64 kbps Optical Fiber Interfaces between Teleprotection and Multiplexer Equipment** - Quality of Service,

Communications Industry Technologies

Link Layer and Physical Technologies

- **Ethernet** - Quality of Service,
- **Bridges/Switches** - Configuration,
- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration, Quality of Service,

Wireless Technologies

- **Global Positioning System (GPS)** - Quality of Service, Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,

General Security Technologies

- **Role-Based Access Control** - Security,
- **Service Level Agreements (SLA)** - Security,

Application Layer Security Technologies

- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **IEC 62351-7 Objects for Network Management** - Data Management

---

Recommended Common Services

Security Services

Common Security Services

- **Authorization for Access Control** - Security,
- **Security Policies** - Security,

Network and System Management Services

Enterprise Management Services

- **System/Network Health-Check Analysis** - Quality of Service,
- **System/Network Fault Diagnosis** - Quality of Service,
- **System/Network Performance Analysis** - Quality of Service,

Data Management Common Services

Data Management Services

- **Address and Naming Management** - Data Management

- **Network Time** - Data Management

Common Platform Services

Recommended Best Practices

Data Management Best Practices

Data Management

- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Quality of Service, Data Management
- **Time Stamping** - Quality of Service, Data Management
- **Data Update Management** - Data Management
- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Quality of Service, Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Quality of Service,

Security Best Practices

Security Technology Documents

Alternative Technologies

Link Layer and Physical Technologies

- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Alternative Best Practices

Data Management

- **Alternate Communication Channels** - Configuration,
- **Backup Data Sources** - Configuration,

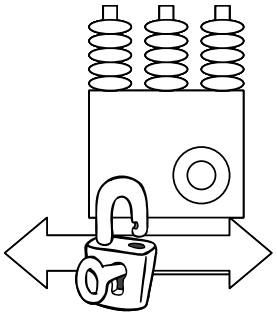
IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service,

Possible Technologies

Utility Field Device Related Data Exchange Technologies

Critical Operations Intra-Substation Environment - #3



This environment encompasses the set of requirements traditionally known as “substation automation” and involve information exchanges within a substation that are critical to legal, safe, and reliable power system operations. Devices within the substation coordinate with each other to ensure the safety of equipment and personnel while optimizing the operation of the network and permitting operators to respond to emergencies.

Typical applications: Uses of this environment may include voltage/VAR control, interlocking, removing equipment for maintenance, updating configurations and settings, responding to faults, load shedding, and manually or automatically restoring service. These tasks were traditionally performed by individual devices but are now are commonly distributed over local area networks.

Characteristics: This environment requires a high level of security because outages, equipment damage or safety concerns can result from misoperated controls, either manually or automatically generated. Similarly, maintenance of equipment by unauthorized personnel could be disastrous.

Similar Environments: Quality of service requirements are not as strict as with the Rapid Deterministic environments, but response generally must be better than human reaction time.

This environment differs from Critical Operations DAC because it is limited to the substation. Some utilities may find physical security adequate within the substation, while electronic security is vital outside the substation. Quality of service requirements may also be less vital between substation and control center than within the substation itself, since the substation automates many critical functions locally.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Provide point-to-point interactions between two entities
- Support peer to peer interactions
- Support interactions within a contained environment (e.g. substation or control center)

Quality of Service Requirements

- Provide high speed messaging of less than 1 second
- Support very high availability of information flows of 99.99+ (~1 hour)
- Support time synchronization of data for age and time-skew information

Security Requirements

- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Credential Renewal Service (notify users prior to expiration of their credentials)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Single Sign-On Service (relieve an entity having successfully completed the act of authentication once from the need to participate in re-authentications upon subsequent accesses to managed resources for some reasonable period of time)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support the management of large volumes of data flows
- Support keeping the data up-to-date
- Support extensive data validation procedures
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **ISO 9506 MMS – Manufacturing Messaging Specification** - Configuration, Quality of Service,
- **IEC61850 – Substation Automation Communications** - Configuration,
- **IEC61850 Part 7-2 – GSE (GOOSE and GSSE** - Configuration, Quality of Service,
- **IEC61850 Part 7-2 – SMV (Sampled Measured Values)** - Configuration,
- **IEC61850 Part 7-2 – Abstract Common Services Interface (ACSI)** - Configuration, Quality of Service, Data Management
- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Network Management, Data Management
- **IEC61850 Part 6 – Substation Configuration Language** - Network Management, Data Management
- **IEC61850 Power Quality Object Models** - Data Management
- **IEC62350 – Object Models for Distributed Energy Resources (DER)** - Network Management, Data Management
- **IEC62349 – Hydro Power Plant Object Models** - Network Management, Data Management
- **IEC61400-25 for Wind Power Object Models** - Network Management, Data Management

Communications Industry Technologies

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Application Layer Protocols

- **SNTP (Network Time Protocol)** - Quality of Service,

Link Layer and Physical Technologies

- **IEEE 802 MAC Addresses** - Configuration,
- **Ethernet** - Configuration,
- **Bridges/Switches** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Wireless Technologies

- **Global Positioning System (GPS)** - Quality of Service,

Computer Systems Related Technologies

- **Universal Description, Discovery, and Integration (UDDI)** - Data Management

- **IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems** - Quality of Service,

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Quality of Service, Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **Role-Based Access Control** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Transport Layer Security Technologies

- **Transport Layer Security (TLS)/Secure Sockets Layer (SSL)** - Security,

Application Layer Security Technologies

- **SNMP Security** - Security, Network Management,

- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service, Security,
- **IEC 62351-3 Security for Profiles including TCP/IP** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,
- **IEC 62351-7 Objects for Network Management** - Quality of Service, Network Management, Data Management

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Credential Renewal Service** - Security,
- **Information Integrity Service** - Security,
- **Security Policies** - Security,
- **Security Service Availability Discovery Service** - Security,
- **Single Sign On Service** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,
- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,

- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,
- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management, Data Management
- **Alarm Detection/Reporting** - Network Management, Data Management
- **Instrumentation and Monitoring Service** - Network Management, Data Management
- **Measurement Data Logging Service** - Security, Network Management,
- **Remote Control** - Network Management,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management
- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Alternate Communication Channels** - Quality of Service,
- **Backup Data Sources** - Quality of Service,
- **Metadata Files and Databases** - Network Management, Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Quality of Service, Network Management, Data Management
- **Time Stamping** - Quality of Service, Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Data Update Management** - Data Management

- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Quality of Service,
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Data Storage and Access Management** - Data Management
- **Database Maintenance Management** - Data Management
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 10164-8:1993 Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function** - Quality of Service,
- **ISO/IEC 18014-1:2002 Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework** - Quality of Service,
- **ISO/IEC 18014-2:2002 Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens** - Quality of Service,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 101 – Serial Telecontrol Protocol** - Configuration, Quality of Service,
- **IEC60870-5 Part 104 – Telecontrol Protocol over TCP/IP** - Configuration, Quality of Service,
- **DNP Serial Protocol** - Configuration, Quality of Service,
- **DNP3 Protocol over TCP/IP** - Configuration, Quality of Service,

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Multicast Routing** - Configuration,

IP-based Transport Protocols

- **User Datagram Protocol (UDP)** - Configuration,

Wireless Technologies

- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

Computer Systems Related Technologies

- **GUID** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Alternative Best Practices

Data Management

- **Backup Databases** - Quality of Service,
- **Backup Sites** - Quality of Service,
- **Data Backup and Logging** - Quality of Service,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,

Federal Documents on Security Technologies

- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,

- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 2986 PKCS #10: Certification Request Syntax Specification Version 1.7** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

Possible Technologies

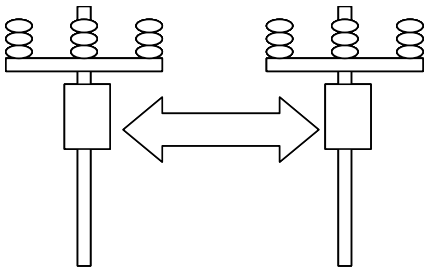
Utility Field Device Related Data Exchange Technologies

- **Fieldbus** - Configuration, Quality of Service,
- **PROFIBUS** - Configuration, Quality of Service,
- **Modbus** - Configuration, Quality of Service,
- **Modbus TCP/IP** - Configuration, Quality of Service,
- **Modbus Plus** - Configuration, Quality of Service,

Link Layer and Physical Technologies

- **Point-to-Point Protocol (PPP)** - Configuration,

Inter-Field Equipment Environment - #4



This environment represents communications that take place between devices outside control centers. This environment tends to be concerned with the optimization of the network rather than operations that are critical to safety or reliability.

Typical applications: Uses of this environment might include a data concentrator gathering primary equipment monitoring data. Another possibility would be two pole-top automated switches exchanging of non-protection-related loading data. This data might later be forwarded to different masters for load-sharing purposes.

Characteristics: Low security needed, but there are a lot of remote devices that can only be reached via wireless or low-bandwidth links.

Similar Environments: Not as critical as Critical Oprations Intra-Site, nor requiring as high a quality of service.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support peer to peer interactions
- Support interactions across widely distributed sites
- Support multi-cast or broadcast capabilities
- Support compute-constrained and/or media constrained communications

Quality of Service Requirements

- Provide high speed messaging of less than 1 second
- Support high availability of information flows of 99.9+ (~9 hours)
- Support time synchronization of data for age and time-skew information

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)

- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support keeping the data up-to-date
- Support extensive data validation procedures
- Support timely access to data by multiple different users
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **ISO 9506 MMS – Manufacturing Messaging Specification** - Configuration, Quality of Service,
- **IEC61850 Part 7-2 – GSE (GOOSE and GSSE** - Configuration, Quality of Service,
- **IEC61850 Part 7-2 – Abstract Common Services Interface (ACSI)** - Configuration, Quality of Service, Data Management
- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Network Management, Data Management
- **IEC61850 Part 6 – Substation Configuration Language** - Network Management, Data Management
- **IEC61850 Power Quality Object Models** - Data Management
- **IEC62350 – Object Models for Distributed Energy Resources (DER)** - Network Management, Data Management
- **IEC62349 – Hydro Power Plant Object Models** - Network Management, Data Management

- **IEC61400-25 for Wind Power Object Models** - Network Management, Data Management

Utility Control Center Related Data Management Technologies

- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management

Communications Industry Technologies

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Application Layer Protocols

- **SNTP (Network Time Protocol)** - Quality of Service, Data Management

Link Layer and Physical Technologies

- **IEEE 802 MAC Addresses** - Configuration,
- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Wireless Technologies

- **Global Positioning System (GPS)** - Quality of Service,
- **Multiple Address (MAS) Radio** - Configuration,
- **Spread Spectrum Radio System** - Configuration,

Computer Systems Related Technologies

- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems** - Quality of Service,

General Internet and De Facto Data Management Technologies

- **XML Schema (xls)** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Quality of Service, Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service, Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,
- **IEC 62351-7 Objects for Network Management** - Quality of Service, Network Management, Data Management

Web-based Network Management

- **Web-based Enterprise Management (WBEM)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Security Policies** - Security,
- **Quality of Identity Service** - Security,
- **Security Service Availability Discovery Service** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,
- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,

- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management, Data Management
- **Alarm Detection/Reporting** - Network Management, Data Management
- **Instrumentation and Monitoring Service** - Network Management, Data Management
- **Measurement Data Logging Service** - Security, Network Management,
- **Remote Control** - Network Management,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management
- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Network Management, Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Quality of Service, Network Management, Data Management
- **Time Stamping** - Quality of Service, Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Data Update Management** - Data Management
- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Quality of Service, Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Data Storage and Access Management** - Data Management

- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Quality of Service, Security, Data Management
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 10164-8:1993 Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function** - Quality of Service,
- **ISO/IEC 18014-1:2002 Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework** - Quality of Service,
- **ISO/IEC 18014-2:2002 Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens** - Quality of Service,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 104 – Telecontrol Protocol over TCP/IP** - Configuration, Quality of Service,
- **DNP3 Protocol over TCP/IP** - Configuration, Quality of Service,

Access Technologies

- **Public Internet** - Configuration,

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Multicast Routing** - Configuration,

Link Layer and Physical Technologies

- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **Trunked Mobile Radio (TMR, TETRA, Project25)** - Configuration,
- **Satellite Leased Channels and VSAT** - Configuration,
- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

Computer Systems Related Technologies

- **GUID** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

Alternative Best Practices

Data Management

- **Backup Data Sources** - Quality of Service,

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,

- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,
- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,

- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,

- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,

- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

---

Possible Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 101 – Serial Telecontrol Protocol** - Configuration,
- **DNP Serial Protocol** - Configuration,
- **Fieldbus** - Quality of Service,
- **PROFIBUS** - Quality of Service,
- **Modbus** - Quality of Service,
- **Modbus TCP/IP** - Quality of Service,
- **Modbus Plus** - Quality of Service,

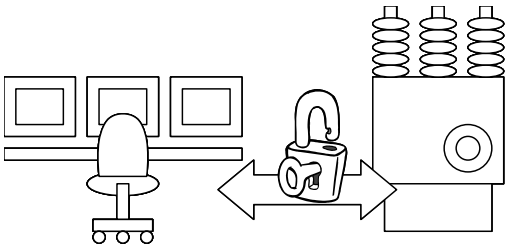
Access Technologies

- **Data over Voice Lines** - Configuration,
- **Fiber in the Loop (FITL)** - Configuration,
- **Hybrid Fiber Coax (HFC)** - Configuration,

Wireless Technologies

- **TDMA Cellular Wireless – IS-136** - Configuration,
- **CDMA Cellular Wireless – IS-95** - Configuration,
- **Cellular Digital Packet Data (CDPD)** - Configuration,
- **Paging Systems** - Configuration,

Critical Operations DAC and SCADA Environment - #5



Critical Operations-related Data Acquisition and Control is the environment most resembling what has been traditionally called Supervisory Control and Data Acquisition (SCADA). It represents those messages between a substation and control center that are critical to legal, safe, and reliable power system operations.

Typical applications: Include monitoring and control of substations, pole-top devices, generation plants or distributed energy resources. These are the functions performed by operators in the daily operation or emergency recovery of the power system.

Characteristics: It is vital that these message exchanges not be tampered, monitored, or interfered with by unauthorized persons. Quality of service requirements are based around human reaction times. Configuration of the network changes often, and may vary widely. Could also include transfer of data that is high-volume and critical, such as configuration files or fault recordings.

Similar Environments: Critical Operations Data Acquisition and Control is very similar to Critical Operations Intra-Substation except that these exchanges take place between control centers and field equipment, rather than between substations.

Requirements for Defining this Environment

Configuration Requirements

- Support interactions between a few "clients" and many "servers"
- Support interactions across widely distributed sites
- Support compute-constrained and/or media constrained communications

Quality of Service Requirements

- Provide high speed messaging of less than 1 second
- Support high availability of information flows of 99.9+ (~9 hours)
- Support time synchronization of data for age and time-skew information

Security Requirements

- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Credential Renewal Service (notify users prior to expiration of their credentials)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Single Sign-On Service (relieve an entity having successfully completed the act of authentication once from the need to participate in re-authentications upon subsequent accesses to managed resources for some reasonable period of time)
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support the management of large volumes of data flows
- Support keeping the data up-to-date
- Support extensive data validation procedures
- Support timely access to data by multiple different users
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **ISO 9506 MMS – Manufacturing Messaging Specification** - Configuration, Quality of Service,
- **IEC61850 Part 7-2 – Abstract Common Services Interface (ACSI)** - Configuration, Quality of Service, Data Management
- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Network Management, Data Management
- **IEC61850 Part 6 – Substation Configuration Language** - Network Management, Data Management
- **IEC61850 Power Quality Object Models** - Data Management
- **IEC62350 – Object Models for Distributed Energy Resources (DER)** - Network Management, Data Management
- **IEC62349 – Hydro Power Plant Object Models** - Network Management, Data Management
- **IEC61400-25 for Wind Power Object Models** - Network Management, Data Management

Utility Control Center Related Data Management Technologies

- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **CIM Extensions for Market Operations** - Data Management

Communications Industry Technologies

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Application Layer Protocols

- **SNTP (Network Time Protocol)** - Quality of Service, Data Management

Link Layer and Physical Technologies

- **LAN/MAN Technologies** - Configuration,
- **IEEE 802 MAC Addresses** - Configuration,
- **Ethernet** - Configuration,
- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Wireless Technologies

- **Global Positioning System (GPS)** - Quality of Service,

Computer Systems Related Technologies

- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems** - Quality of Service,

General Internet and De Facto Data Management Technologies

- **XML Schema (xls)** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Quality of Service, Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **Role-Based Access Control** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,

- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Transport Layer Security Technologies

- **Transport Layer Security (TLS)/Secure Sockets Layer (SSL)** - Security,

Application Layer Security Technologies

- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service, Security,
- **IEC 62351-3 Security for Profiles including TCP/IP** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,
- **IEC 62351-7 Objects for Network Management** - Quality of Service, Network Management, Data Management

Web-based Network Management

- **Web-based Enterprise Management (WBEM)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Credential Renewal Service** - Security,
- **Information Integrity Service** - Security,
- **Security Policies** - Security,

- **Security Service Availability Discovery Service** - Security,
- **Single Sign On Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,
- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,
- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management, Data Management
- **Alarm Detection/Reporting** - Network Management, Data Management
- **Instrumentation and Monitoring Service** - Network Management, Data Management
- **Measurement Data Logging Service** - Security, Network Management,
- **Remote Control** - Network Management,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management
- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Backup Databases** - Quality of Service,
- **Metadata Files and Databases** - Network Management, Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Quality of Service, Network Management, Data Management
- **Time Stamping** - Quality of Service, Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Data Update Management** - Data Management
- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Quality of Service, Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Data Storage and Access Management** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Quality of Service, Security, Data Management
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 10164-8:1993 Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function** - Quality of Service,
- **ISO/IEC 18014-1:2002 Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework** - Quality of Service,
- **ISO/IEC 18014-2:2002 Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens** - Quality of Service,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,

- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 104 – Telecontrol Protocol over TCP/IP** - Configuration, Quality of Service,
- **DNP3 Protocol over TCP/IP** - Configuration, Quality of Service,

Utility Control Center Related Data Management Technologies

- **IEC 60870-6 (ICCP)** - Configuration,

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,
- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Hubs/Repeaters** - Configuration,

- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **IEEE 802.16 Broadband Wireless Access Standards** - Configuration,
- **Multiple Address (MAS) Radio** - Configuration,
- **Spread Spectrum Radio System** - Configuration,
- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

---

Alternative Best Practices

Data Management

- **Alternate Communication Channels** - Quality of Service,
- **Backup Data Sources** - Quality of Service,
- **Backup Sites** - Quality of Service,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,

- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,

Federal Documents on Security Technologies

- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,

- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 2986 PKCS #10: Certification Request Syntax Specification Version 1.7** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,

- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

---

Possible Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 101 – Serial Telecontrol Protocol** - Configuration,
- **DNP Serial Protocol** - Configuration,
- **Fieldbus** - Configuration, Quality of Service,
- **PROFIBUS** - Configuration, Quality of Service,

- **Modbus** - Quality of Service,
- **Modbus TCP/IP** - Configuration, Quality of Service,
- **Modbus Plus** - Configuration, Quality of Service,

Access Technologies

- **Data over Voice Lines** - Configuration,
- **Fiber in the Loop (FITL)** - Configuration,
- **Hybrid Fiber Coax (HFC)** - Configuration,

Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

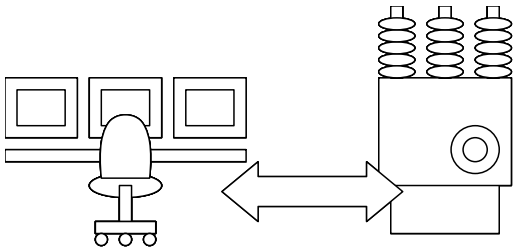
IP-based Transport Protocols

- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Wireless Technologies

- **Trunked Mobile Radio (TMR, TETRA, Project25)** - Configuration,
- **Satellite Leased Channels and VSAT** - Configuration,

Non-Critical Operations DAC Data Acquisition Environment - #6



Non-Critical Operations Data Acquisition and Control environment represents the set of requirements for gathering less-vital data to the control center, usually for the purposes of optimizing the power network rather than for safety, legality or reliability reasons.

Typical applications: Monitoring non-power system equipment, power quality monitoring, primary equipment monitoring, some kinds of customer metering.

Characteristics: Since this environment does not involve critical information exchanges, impacts from security breaches are minimal, and therefore extensive security measures are not mandatory. Data may be required in hours or days rather than seconds.

Similar Environments: Unlike Inter-Field Equipment, this information goes directly to and from the control center, similar to High-Security DAC but not as critical.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions between a few "clients" and many "servers"
- Support interactions across widely distributed sites
- Support compute-constrained and/or media constrained communications

Quality of Service Requirements

- Provide medium speed messaging on the order of 10 seconds
- Support high availability of information flows of 99.9+ (~9 hours)

Security Requirements

- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Audit Service (responsible for producing records, which track security relevant events)

- Provide Security Policy Service (concerned with the management of security policies)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support keeping the data up-to-date
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **ISO 9506 MMS – Manufacturing Messaging Specification** - Configuration, Quality of Service,
- **IEC61850 Part 7-2 – GSE (GOOSE and GSSE** - Configuration,
- **IEC61850 Part 7-2 – Abstract Common Services Interface (ACSI)** - Configuration, Quality of Service, Data Management
- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Network Management, Data Management
- **IEC61850 Part 6 – Substation Configuration Language** - Network Management, Data Management
- **IEC61850 Power Quality Object Models** - Data Management
- **IEC62350 – Object Models for Distributed Energy Resources (DER)** - Network Management, Data Management
- **IEC62349 – Hydro Power Plant Object Models** - Network Management, Data Management
- **IEC61400-25 for Wind Power Object Models** - Network Management, Data Management

Utility Control Center Related Data Management Technologies

- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management

Communications Industry Technologies

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Link Layer and Physical Technologies

- **LAN/MAN Technologies** - Configuration,
- **IEEE 802 MAC Addresses** - Configuration,
- **Ethernet** - Configuration,
- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Computer Systems Related Technologies

- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management

General Internet and De Facto Data Management Technologies

- **XML Schema (xls)** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security,
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **Role-Based Access Control** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Transport Layer Security Technologies

- **Transport Layer Security (TLS)/Secure Sockets Layer (SSL)** - Security,

Application Layer Security Technologies

- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,
- **IEC 62351-7 Objects for Network Management** - Quality of Service, Network Management, Data Management

Web-based Network Management

- **Web-based Enterprise Management (WBEM)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Security Policies** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,
- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,
- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management,
- **Alarm Detection/Reporting** - Network Management,
- **Instrumentation and Monitoring Service** - Network Management,
- **Measurement Data Logging Service** - Security, Network Management,
- **Remote Control** - Network Management,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management
- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Backup Databases** - Quality of Service,
- **Metadata Files and Databases** - Network Management, Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Network Management, Data Management
- **Time Stamping** - Security, Network Management, Data Management
- **Data Update Management** - Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Quality of Service, Security,
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Network Management,
- **RFC 2518** - Network Management,

- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 104 – Telecontrol Protocol over TCP/IP** - Configuration,
- **DNP3 Protocol over TCP/IP** - Configuration,

Utility Control Center Related Data Management Technologies

- **IEC 60870-6 (ICCP)** - Configuration,

Access Technologies

- **Public Internet** - Configuration,

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

Link Layer and Physical Technologies

- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **Multiple Address (MAS) Radio** - Configuration,
- **Spread Spectrum Radio System** - Configuration,
- **Satellite Leased Channels and VSAT** - Configuration,
- **Radio Frequency Identification (RFID)** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

---

Alternative Best Practices

Data Management

- **Backup Sites** - Quality of Service,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,

- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Network Management,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,

- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,

Possible Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 101 – Serial Telecontrol Protocol** - Configuration,
- **DNP Serial Protocol** - Configuration,
- **Fieldbus** - Configuration,
- **PROFIBUS** - Configuration,
- **Modbus TCP/IP** - Configuration,
- **Modbus Plus** - Configuration,

Access Technologies

- **Data over Voice Lines** - Configuration,
- **Fiber in the Loop (FITL)** - Configuration,
- **Hybrid Fiber Coax (HFC)** - Configuration,

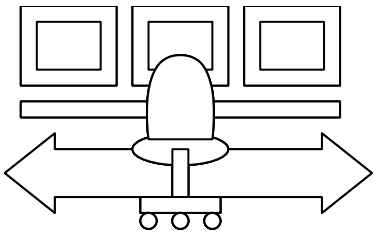
Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Wireless Technologies

- **TDMA Cellular Wireless – IS-136** - Configuration,
- **CDMA Cellular Wireless – IS-95** - Configuration,
- **Cellular Digital Packet Data (CDPD)** - Configuration,
- **Global System for Mobile Communication (GSM)** - Configuration,
- **Trunked Mobile Radio (TMR, TETRA, Project25)** - Configuration,
- **Paging Systems** - Configuration,

Intra-Control Center Environment - #7



This environment represents communications between modules of a single control center, typically over a local area network within a single physical building.

Typical Applications: Updating databases and human-machine interfaces with data gathered from the "front-end processors" within Energy Management Systems (EMSs) or Distribution Management Systems (DMSs).

Characteristics: Located in a very secure and reliable physical environment, but with a huge amount of data to manage and distribute between a variety of platforms and database technologies. Updates must happen in at least human response times for some data.

Similar Environments: This environment carries ALL the data brought in via High Security DAC or Low Security DAC, but need not be transmitted in as reliable a format. Carries similar types of data as when the control center communicates with other businesses (CC/ESP, CC/Customer Equipment, or CC/corporations). However, the real-time requirements are tighter, security is nowhere near as important, and data formats tend to be proprietary for performance reasons.

Definition: This environment is defined by the following requirements:

.

Requirements for Defining this Environment

Configuration Requirements

- Support peer to peer interactions
- Support interactions within a contained environment (e.g. substation or control center)

Quality of Service Requirements

- Support high availability of information flows of 99.9+ (~9 hours)
- Support time synchronization of data for age and time-skew information

Security Requirements

- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)

- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide User Profile and User Management (combination of several other security services)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support the management of large volumes of data flows
- Support keeping the data up-to-date
- Support extensive data validation procedures
- Support keeping data consistent and synchronized across systems and/or databases
- Support timely access to data by multiple different users
- Support frequent changes in types of data exchanged
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Support the exchange of unstructured or special-format data (e.g. text, documents, oscillographic data)
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Part 6 – Substation Configuration Language** - Network Management, Data Management

Utility Control Center Related Data Management Technologies

- **IEC 60870-6 (ICCP)** - Configuration,
- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **CIM Extensions for Market Operations** - Data Management

- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration, Quality of Service, Data Management
- **IEC61968 SIDM System Interfaces for Distribution Management** - Data Management
- **OPEN GIS** - Data Management

Communications Industry Technologies

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Application Layer Protocols

- **SNTP (Network Time Protocol)** - Quality of Service, Data Management

Link Layer and Physical Technologies

- **IEEE 802 MAC Addresses** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Wireless Technologies

- **Global Positioning System (GPS)** - Quality of Service, Data Management

Computer Systems Related Technologies

- **CORBA and CORBA Services** - Data Management
- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **Enterprise Java Beans (EJB)** - Data Management
- **IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems** - Quality of Service,
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ANSI/ISO/IEC 8632-1, 2, 3, 4 – Computer Graphics Metafile (CGM)** - Data Management

- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management
- **XSLT** - Data Management
- **XQuery** - Data Management
- **ANSI/ISO/IEC 9075 – Structured Query Language (SQL)** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Quality of Service, Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **Role-Based Access Control** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Transport Layer Security Technologies

- **Transport Layer Security (TLS)/Secure Sockets Layer (SSL)** - Security,

Application Layer Security Technologies

- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service, Security, Data Management
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,

Web-based Network Management

- **Web-based Enterprise Management (WBEM)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Security Policies** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,
- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,

- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,
- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Distributed Data Management Service** - Data Management
- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management, Data Management
- **Alarm Detection/Reporting** - Network Management, Data Management
- **Instrumentation and Monitoring Service** - Network Management, Data Management
- **Measurement Data Logging Service** - Security, Network Management,
- **Remote Control** - Network Management,
- **Network Time** - Data Management
- **File Transfer** - Data Management

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management
- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,
- **Checkpoint and Recovery** - Network Management,
- **Workflow Service** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Backup Data Sources** - Quality of Service,
- **Backup Databases** - Quality of Service,
- **Metadata Files and Databases** - Network Management, Data Management

- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Quality of Service, Network Management, Data Management
- **Time Stamping** - Quality of Service, Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Data Update Management** - Data Management
- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Quality of Service, Data Management
- **Management of Data Consistency and Synchronization across Systems** - Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Data Storage and Access Management** - Data Management
- **Data Consistency across Multiple Systems** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Quality of Service, Security, Data Management
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 10164-8:1993 Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function** - Quality of Service, Data Management
- **ISO/IEC 18014-1:2002 Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework** - Quality of Service,
- **ISO/IEC 18014-2:2002 Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens** - Quality of Service,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,

- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Network Management,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **C37.111-1999 IEEE COMTRADE Standard (Common Format for Transient Data Exchange) for Power Systems** - Data Management
- **IEEE 1159.3 - Power Quality Data Interchange Format (PQDIF)** - Data Management

Utility Control Center Related Data Management Technologies

- **MultiSpeak** - Data Management

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

Application Layer Protocols

- **Microsoft COM+** - Data Management

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,
- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Hubs/Repeaters** - Configuration,

- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,

Wireless Technologies

- **IEEE 802.11 Wireless Local Area Network (WLAN)** - Configuration,
- **IEEE 802.15 Wireless Personal Area Network (PAN)** - Configuration,
- **Bluetooth Special** - Configuration,
- **Radio Frequency Identification (RFID)** - Data Management

Computer Systems Related Technologies

- **Web Services Description Language (WSDL)** - Data Management

General Internet and De Facto Data Management Technologies

- **Common Warehouse Model (CWM)** - Data Management
- **American Standard Code for Information Interchange (ASCII)** - Data Management
- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

eCommerce Related Data Management Technologies

- **EAN.UCC Identification Numbers** - Data Management
- **EAN.UCC Universal Bar Codes** - Data Management
- **10303 Standard Exchange for Product Data (STEP)** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

Alternative Best Practices

Data Management

- **Backup Sites** - Quality of Service,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Network Management,

- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,

Possible Technologies

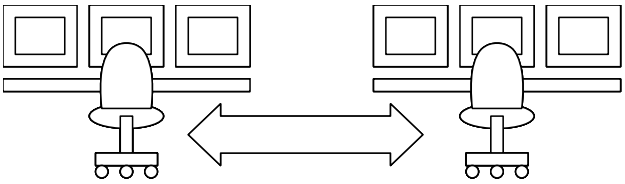
Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Application Layer Protocols

- **CSV files** - Data Management

Inter-Control Center Environment - #8



This environment represents the requirements for exchanging data among control centers. Until recently, such links were the only formal links between power system businesses. For this reason, considerable effort has already been made in standardizing protocols for this environment

Typical Applications: Exchanging fault information for contingency analysis and emergency operations. Exchanging metering information from territorial boundaries to initialize state estimation or load distribution applications. Sometimes includes text messaging between operators, or tariff information. May take place between levels of control centers within a utility, or between RTOs.

Characteristics: Often, but not always, business-to-business. Usually based on wide-area networks. Extremely high security requirements because exchanges usually cross organizational boundaries, the data may be critical to network stability, and the security environment at the other end cannot be guaranteed. Networks are usually private so denial-of-service is not a primary concern; however non-repudiation is vital because mistakes may cause inter-organizational conflict. Control centers exchange relatively small amounts of data, mostly already in standard format, in time periods measured in seconds.

Similar Environments: Technologically very similar to other business-to-business environments, and with similar security requirements. However, the data carried tends to be critical for operational rather than economic reasons. Carries only a subset of the Intra-Control Center information.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support peer to peer interactions
- Support interactions across widely distributed sites

Quality of Service Requirements

- Provide medium speed messaging on the order of 10 seconds
- Support high availability of information flows of 99.9+ (~9 hours)

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)
- Provide Inter-Domain Security Service (support security requirements across organizational boundaries)
- Provide Non-repudiation Service (cannot deny that interaction took place)
- Provide Security Assurance Service (determine the level of security provided by another environment)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Path and Routing Quality of Security (being able to determine a secure communication path)
- Provide Firewall Transversal
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Protocol mapping (the ability to convert from one protocol to another)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support keeping the data up-to-date
- Support extensive data validation procedures
- Support keeping data consistent and synchronized across systems and/or databases
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping
- Support the management of data across organizational boundaries

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Part 6 – Substation Configuration Language** - Network Management, Data Management

Utility Control Center Related Data Management Technologies

- **IEC 60870-6 (ICCP)** - Configuration,
- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **CIM Extensions for Market Operations** - Data Management
- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration, Quality of Service, Data Management
- **IEC61968 SIDM System Interfaces for Distribution Management** - Data Management
- **OPEN GIS** - Data Management

Communications Industry Technologies

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Application Layer Protocols

- **SNTP (Network Time Protocol)** - Data Management

Link Layer and Physical Technologies

- **IEEE 802 MAC Addresses** - Configuration,
- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Synchronous Optical Network (SONET)** - Configuration,

- **Asynchronous Transfer Mode (ATM)** - Configuration,

Wireless Technologies

- **Global Positioning System (GPS)** - Data Management

Computer Systems Related Technologies

- **CORBA and CORBA Services** - Data Management
- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **Enterprise Java Beans (EJB)** - Data Management
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ANSI/ISO/IEC 8632-1, 2, 3, 4 – Computer Graphics Metafile (CGM)** - Data Management
- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management

eCommerce Related Data Management Technologies

- **ebXML** - Data Management
- **ebXML Collaboration Protocol Profiles (CPPA)** - Data Management
- **ebXML Messaging** - Data Management
- **ebXML Registry** - Data Management
- **ISO/IEC JTC 1 SC32 - ISO/IEC 15944-1:2002 Information technology -- Business agreement semantic descriptive techniques -- Part 1: Operational aspects of Open-EDI for implementation** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,

- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security, Data Management
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **OASIS Extensible Access Control Markup Language (XACML** - Security,
- **XML Key Management Specification (XKMS** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,

Web-based Network Management

- **Web-based Enterprise Management (WBEM)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Confidentiality** - Security,
- **Firewall Traversal** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Inter-Domain Security** - Security,
- **Non-repudiation** - Security,
- **Path Routing and QOS Service** - Security,
- **Security Policies** - Security,
- **Quality of Identity Service** - Security,
- **Security Assurance Management** - Security,
- **Security Protocol Mapping** - Security,
- **Security Service Availability Discovery Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,
- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,
- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Distributed Data Management Service** - Data Management
- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management, Data Management
- **Alarm Detection/Reporting** - Network Management, Data Management
- **Instrumentation and Monitoring Service** - Network Management, Data Management
- **Measurement Data Logging Service** - Security, Network Management,
- **Remote Control** - Network Management,
- **Network Time** - Data Management

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management
- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,
- **Checkpoint and Recovery** - Network Management,
- **Workflow Service** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Alternate Communication Channels** - Quality of Service,
- **Backup Data Sources** - Quality of Service,
- **Backup Databases** - Quality of Service,
- **Metadata Files and Databases** - Network Management, Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Network Management, Data Management
- **Time Stamping** - Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Data Update Management** - Data Management
- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Data Management
- **Management of Data Consistency and Synchronization across Systems** - Data Management
- **Management of Data and Object Naming** - Data Management

- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Data Consistency across Multiple Systems** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Quality of Service, Security, Data Management
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 10164-8:1993 Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function** - Data Management
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2350 Expectations for Computer Security Incident Response** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Security, Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Control Center Related Data Management Technologies

- **MultiSpeak** - Data Management

Access Technologies

- **Public Internet** - Configuration,

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

Application Layer Protocols

- **Microsoft COM+** - Data Management

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,
- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

General Internet and De Facto Data Management Technologies

- **Common Warehouse Model (CWM)** - Data Management
- **American Standard Code for Information Interchange (ASCII)** - Data Management
- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

---

Alternative Best Practices

Data Management

- **Backup Sites** - Quality of Service,

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,

- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,
- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO 9735-9:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 9: Security key** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO/IEC 10181-4:1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,

- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General** - Security,
- **ISO/IEC 13888-2:1998 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques** - Security,
- **ISO/IEC 13888-3:1997 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,
- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,

- **RFC 1579 Firewall-Friendly FTP** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,

- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2888 Secure Remote Access with L2TP** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2979 Behavior of and Requirements for Internet Firewalls** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,

- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

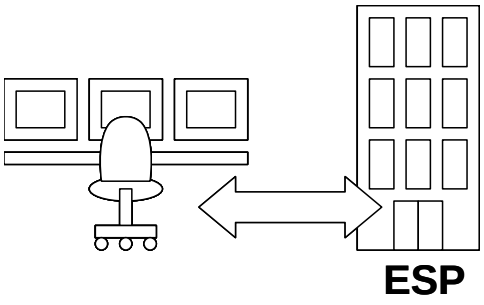
---

Possible Technologies

Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Control Centers to ESPs Environment - #9



This environment encompasses the requirements for communications between utility control centers and Energy Service Providers (ESPs) or "aggregators".

Typical Applications: Real-time pricing negotiations, aggregated customer metering and settlements. May provide data later used for market operations.

Characteristics: A business-to-business environment, therefore having very strict requirements for security, a contractual level of timeliness and record-keeping. ESPs are a volatile business environment, so the data may need to be reconfigured on a monthly basis. Any metering data is usually aggregated and sent in infrequent "batches", so it does not carry data at high volumes or speeds.

Similar Environments: Technologically very similar to other business-to-business environments, but connections and associations change frequently.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support peer to peer interactions
- Support interactions across widely distributed sites
- Support the frequent change of configuration and/or location of end devices or sites

Quality of Service Requirements

- Provide medium speed messaging on the order of 10 seconds
- Support contractual timeliness (data must be available at a specific time or within a specific window of time)
- Support medium availability of information flows of 99.0+ (~3.5 days)

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)

- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)
- Provide Inter-Domain Security Service (support security requirements across organizational boundaries)
- Provide Non-repudiation Service (cannot deny that interaction took place)
- Provide Security Assurance Service (determine the level of security provided by another environment)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Path and Routing Quality of Security (being able to determine a secure communication path)
- Provide Firewall Transversal
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Protocol mapping (the ability to convert from one protocol to another)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Support extensive data validation procedures

Data Management Requirements

- Support timely access to data by multiple different users
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping
- Support the management of data across organizational boundaries

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Network Management, Data Management
- **IEC61850 Power Quality Object Models** - Data Management
- **IEC62350 – Object Models for Distributed Energy Resources (DER)** - Network Management, Data Management
- **IEC62349 – Hydro Power Plant Object Models** - Network Management, Data Management
- **IEC61400-25 for Wind Power Object Models** - Network Management, Data Management

Utility Control Center Related Data Management Technologies

- **IEC 60870-6 (ICCP)** - Configuration,
- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **CIM Extensions for Market Operations** - Data Management
- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration, Quality of Service, Data Management
- **IEC61968 SIDM System Interfaces for Distribution Management** - Data Management
- **IEC62325 on Framework for Energy Market Communications** - Data Management
- **NERC e-tagging** - Data Management
- **NAESB OASIS for Market Transactions** - Data Management

Customer Interface Data Management Technologies

- **IEC62056 – Data Exchange for Meter Reading, Tariff, and Load Control** - Data Management
- **ANSI C12.19 (Meter Tables)** - Data Management
- **AEIC Guidelines** - Data Management

Communications Industry Technologies

Access Technologies

- **Public Internet** - Configuration,
- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Application Layer Protocols

- **SNTP (Network Time Protocol)** - Data Management

Link Layer and Physical Technologies

- **IEEE 802 MAC Addresses** - Configuration,
- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Wireless Technologies

- **Global Positioning System (GPS)** - Quality of Service,

Computer Systems Related Technologies

- **CORBA and CORBA Services** - Data Management
- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **Enterprise Java Beans (EJB)** - Data Management
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management
- **XQuery** - Data Management
- **ANSI/ISO/IEC 9075 – Structured Query Language (SQL)** - Data Management

eCommerce Related Data Management Technologies

- **ebXML** - Data Management
- **ebXML Collaboration Protocol Profiles (CPPA)** - Data Management
- **ebXML Messaging** - Data Management
- **ebXML Registry** - Data Management
- **ISO/IEC JTC 1 SC32 - ISO/IEC 15944-1:2002 Information technology -- Business agreement semantic descriptive techniques -- Part 1: Operational aspects of Open-EDI for implementation** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,

- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security, Network Management,
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **OASIS Extensible Access Control Markup Language (XACML** - Security,
- **XML Key Management Specification (XKMS** - Security,

- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Confidentiality** - Security,
- **Firewall Traversal** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Inter-Domain Security** - Security,
- **Non-repudiation** - Security,
- **Path Routing and QOS Service** - Security,
- **Security Policies** - Security,
- **Quality of Identity Service** - Security,
- **Security Assurance Management** - Security,
- **Security Protocol Mapping** - Security,
- **Security Service Availability Discovery Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Data Management
- **Generic Eventing And Subscription** - Data Management
- **Alarm Detection/Reporting** - Network Management,
- **Instrumentation and Monitoring Service** - Network Management,
- **Measurement Data Logging Service** - Security,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Network Management, Data Management
- **Time Stamping** - Quality of Service, Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Network Management,
- **Data Update Management** - Data Management
- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Quality of Service, Data Management
- **Management of Data Consistency and Synchronization across Systems** - Quality of Service, Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Network Management,
- **Management of Data Acquisition** - Network Management, Data Management
- **Management of Manual Data Entry** - Network Management,
- **Data Storage and Access Management** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Quality of Service, Security, Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2350 Expectations for Computer Security Incident Response** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Security, Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Control Center Related Data Management Technologies

- **MultiSpeak** - Data Management

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,

- **Core-Based Tree (CBT) multicast routing** - Configuration,

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,
- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **Radio Frequency Identification (RFID)** - Network Management, Data Management

Quality-of-Service-enabling Technologies

- **Multi-Protocol Label Switching (MPLS)** - Quality of Service,
- **Differentiated Services (DiffServ)** - Quality of Service,
- **Integrated Services (IntServ)** - Quality of Service,

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

General Internet and De Facto Data Management Technologies

- **Common Warehouse Model (CWM)** - Data Management
- **American Standard Code for Information Interchange (ASCII)** - Data Management
- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

Alternative Best Practices

Data Management

- **Alternate Communication Channels** - Quality of Service,
- **Backup Data Sources** - Quality of Service,
- **Backup Databases** - Quality of Service,
- **Backup Sites** - Quality of Service,

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,

- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,
- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO 9735-9:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 9: Security key** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO/IEC 10181-4:1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,

- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General** - Security,
- **ISO/IEC 13888-2:1998 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques** - Security,
- **ISO/IEC 13888-3:1997 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,
- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1579 Firewall-Friendly FTP** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,

- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2888 Secure Remote Access with L2TP** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,

- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2979 Behavior of and Requirements for Internet Firewalls** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,

- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

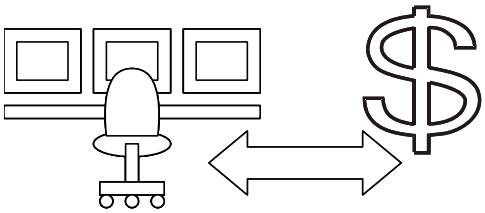
---

Possible Technologies

Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

RTOs/ISOs to Market Participants Environment - #10



This environment represents the communications requirements for control centers to pass metering data to energy market participants.

Typical Applications: Providing raw data from utility, RTO or ISO control centers for use in energy trading and marketing operations.

Characteristics: A business-to-business environment in which volumes and speeds of data are not great, but the data is critical to large sums of money being exchanged, and there may be many users of the data. Exchanges may take place over public networks, so all types of attacks including denial-of-service are therefore a possibility.

Similar Environments: Technologically very similar to other business-to-business environments, but with the strictest security requirements, and most likely to adopt modern technology.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions between a few "servers" and many "clients"
- Support interactions across widely distributed sites
- Support the frequent change of configuration and/or location of end devices or sites

Quality of Service Requirements

- Provide medium speed messaging on the order of 10 seconds
- Support contractual timeliness (data must be available at a specific time or within a specific window of time)
- Support high availability of information flows of 99.9+ (~9 hours)

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)

- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)
- Provide Security Against Denial-of-Service Service (unimpeded access to data to avoid denial of service)
- Provide Inter-Domain Security Service (support security requirements across organizational boundaries)
- Provide Non-repudiation Service (cannot deny that interaction took place)
- Provide Security Assurance Service (determine the level of security provided by another environment)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Path and Routing Quality of Security (being able to determine a secure communication path)
- Provide Firewall Transversal
- Provide Privacy Service (the ability to ensure person information is not disclosed)
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Protocol mapping (the ability to convert from one protocol to another)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)

Data Management Requirements

- Support extensive data validation procedures
- Support timely access to data by multiple different users
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping
- Support the management of data across organizational boundaries

---

Recommended Technologies

Energy Industry-Specific Technologies

Utility Control Center Related Data Management Technologies

- **IEC 60870-6 (ICCP)** - Configuration,
- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **CIM Extensions for Market Operations** - Data Management
- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration, Quality of Service, Data Management
- **IEC62325 on Framework for Energy Market Communications** - Data Management
- **NERC e-tagging** - Data Management
- **NAESB OASIS for Market Transactions** - Data Management

Communications Industry Technologies

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Application Layer Protocols

- **Hypertext Transfer Protocol (HTTP)** - Configuration,
- **Web Browser** - Configuration,
- **SNTP (Network Time Protocol)** - Data Management

Link Layer and Physical Technologies

- **LAN/MAN Technologies** - Configuration,
- **IEEE 802 MAC Addresses** - Configuration,
- **Ethernet** - Configuration,
- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Wireless Technologies

- **Global Positioning System (GPS)** - Quality of Service,

Computer Systems Related Technologies

- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management

- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **Enterprise Java Beans (EJB)** - Data Management
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management
- **ANSI/ISO/IEC 9075 – Structured Query Language (SQL)** - Data Management

eCommerce Related Data Management Technologies

- **ebXML** - Data Management
- **ebXML Collaboration Protocol Profiles (CPPA)** - Data Management
- **ebXML Messaging** - Data Management
- **ebXML Registry** - Data Management
- **ISO/IEC JTC 1 SC32 - ISO/IEC 15944-1:2002 Information technology -- Business agreement semantic descriptive techniques -- Part 1: Operational aspects of Open-EDI for implementation** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,

- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **OASIS Extensible Access Control Markup Language (XACML** - Security,
- **XML Key Management Specification (XKMS** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,

- **Authorization for Access Control** - Security,
- **Confidentiality** - Security,
- **Firewall Traversal** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Inter-Domain Security** - Security,
- **Non-repudiation** - Security,
- **Path Routing and QOS Service** - Security,
- **Security Policies** - Security,
- **Privacy Service** - Security,
- **Quality of Identity Service** - Security,
- **Security against Denial-of-Service** - Security,
- **Security Assurance Management** - Security,
- **Security Protocol Mapping** - Security,
- **Security Service Availability Discovery Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Data Management
- **Generic Eventing And Subscription** - Data Management
- **Alarm Detection/Reporting** - Data Management
- **Instrumentation and Monitoring Service** - Data Management
- **Measurement Data Logging Service** - Security,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Data Management
- **Time Stamping** - Quality of Service, Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Data Update Management** - Data Management
- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Quality of Service, Data Management
- **Management of Data Consistency and Synchronization across Systems** - Quality of Service, Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Data Storage and Access Management** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Quality of Service, Security, Data Management

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,

- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2350 Expectations for Computer Security Incident Response** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Security, Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Access Technologies

- **Public Internet** - Configuration,

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

IP-based Transport Protocols

- **Stream Control Transmission Protocol (SCTP)** - Configuration,
- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,
- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Hubs/Repeaters** - Configuration,

- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **Radio Frequency Identification (RFID)** - Data Management

Quality-of-Service-enabling Technologies

- **Multi-Protocol Label Switching (MPLS)** - Quality of Service,
- **Differentiated Services (DiffServ)** - Quality of Service,
- **Integrated Services (IntServ)** - Quality of Service,

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

General Internet and De Facto Data Management Technologies

- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

---

Alternative Best Practices

Data Management

- **Alternate Communication Channels** - Quality of Service,
- **Backup Data Sources** - Quality of Service,
- **Backup Databases** - Quality of Service,
- **Backup Sites** - Quality of Service,

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,
- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO 9735-9:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 9: Security key** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks** - Security,

- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO/IEC 10181-4:1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General** - Security,
- **ISO/IEC 13888-2:1998 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques** - Security,
- **ISO/IEC 13888-3:1997 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,

- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,
- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1040 Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication** - Security,
- **RFC 1423 Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers** - Security,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1579 Firewall-Friendly FTP** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,

- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2888 Secure Remote Access with L2TP** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2979 Behavior of and Requirements for Internet Firewalls** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,

- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

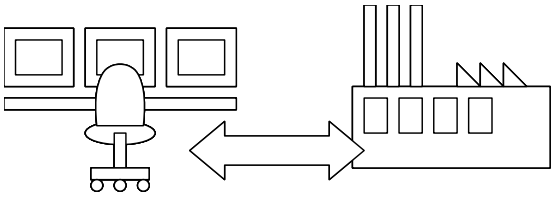
- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **W3C The Platform for Privacy Preferences 1.1 (P3P1.1) SpecificationW3C Working Draft** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

Possible Technologies

Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Control Center to Customers Environment - #11



This environment encompasses the requirements for what has traditionally been called commercial or industrial metering. It includes the requirements for any data exchange that travels directly to the control center from a customer site, without involving substations or data aggregators.

Typical Applications: Metering of large customers, control of distributed energy resources, limiting demand under heavy loads by requesting customers drop off.

Characteristics: Business-to-business communications, but involving operational rather than monetary data. Medium to high volumes of data coming from many sources, but only moderately high security requirements because of the nature of the data. Configuration may change significantly on a monthly basis.

Similar Environments: Similar in requirements to Critical Operations DAC except attackers could not do as much damage by controlling this environment, and the quality of service need not be as quite as high. It is otherwise similar, technologically, to other business-to-business environments.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions between a few "clients" and many "servers"
- Support interactions across widely distributed sites
- Support multi-cast or broadcast capabilities
- Support the frequent change of configuration and/or location of end devices or sites

Quality of Service Requirements

- Support medium availability of information flows of 99.0+ (~3.5 days)

Security Requirements

- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)

- Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)
- Provide Inter-Domain Security Service (support security requirements across organizational boundaries)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Firewall Transversal
- Provide Privacy Service (the ability to ensure person information is not disclosed)
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Protocol mapping (the ability to convert from one protocol to another)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support the management of large volumes of data flows
- Support extensive data validation procedures
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping
- Support the management of data across organizational boundaries

---

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Part 7-2 – Abstract Common Services Interface (ACSI)** - Configuration, Data Management

Utility Control Center Related Data Management Technologies

- **IEC 60870-6 (ICCP)** - Configuration,
- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **CIM Extensions for Market Operations** - Data Management
- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration, Data Management
- **IEC62325 on Framework for Energy Market Communications** - Data Management

Customer Interface Data Management Technologies

- **IEC62056 – Data Exchange for Meter Reading, Tariff, and Load Control** - Data Management
- **ANSI C12.19 (Meter Tables)** - Data Management
- **AEIC Guidelines** - Data Management

Communications Industry Technologies

Access Technologies

- **Public Internet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Link Layer and Physical Technologies

- **LAN/MAN Technologies** - Configuration,
- **IEEE 802 MAC Addresses** - Configuration,
- **Ethernet** - Configuration,
- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Computer Systems Related Technologies

- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management

- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management

eCommerce Related Data Management Technologies

- **ebXML** - Data Management
- **ebXML Collaboration Protocol Profiles (CPPA)** - Data Management
- **ebXML Messaging** - Data Management
- **ebXML Registry** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **PKI – Public Key Infrastructure (X.509)** - Security,
- **Kerberos** - Security,
- **FIPS 140-2 Security Requirements for Cryptographic Modules** - Security,
- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **Role-Based Access Control** - Security,
- **PKCS** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,

- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Transport Layer Security Technologies

- **Transport Layer Security (TLS)/Secure Sockets Layer (SSL)** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security,
- **IEC 62351-3 Security for Profiles including TCP/IP** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **OASIS Extensible Access Control Markup Language (XACML** - Security,
- **XML Key Management Specification (XKMS** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,
- **IEC 62351-7 Objects for Network Management** - Quality of Service, Network Management, Data Management

Web-based Network Management

- **Web-based Enterprise Management (WBEM)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Confidentiality** - Security,
- **Firewall Traversal** - Security,
- **Inter-Domain Security** - Security,
- **Security Policies** - Security,
- **Privacy Service** - Security,
- **Security Protocol Mapping** - Security,
- **Security Service Availability Discovery Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,
- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,
- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management, Data Management
- **Alarm Detection/Reporting** - Network Management, Data Management
- **Instrumentation and Monitoring Service** - Network Management, Data Management
- **Measurement Data Logging Service** - Security, Network Management,
- **Remote Control** - Network Management,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management

- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management
- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,
- **Checkpoint and Recovery** - Network Management,
- **Workflow Service** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Network Management, Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Network Management, Data Management
- **Time Stamping** - Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Management of Data Consistency and Synchronization across Systems** - Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Data Storage and Access Management** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Quality of Service, Security, Data Management
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,

- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Security, Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 104 – Telecontrol Protocol over TCP/IP** - Configuration,
- **DNP3 Protocol over TCP/IP** - Configuration,
- **ISO 9506 MMS – Manufacturing Messaging Specification** - Configuration,

Customer Interface Data Management Technologies

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Host extensions for IP multicasting** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

IP-based Transport Protocols

- **Stream Control Transmission Protocol (SCTP)** - Configuration,
- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,
- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **Code-Division Multiple Access 2000 (CDMA-2000)** - Configuration,
- **TDMA Cellular Wireless – IS-136** - Configuration,
- **CDMA Cellular Wireless – IS-95** - Configuration,
- **Cellular Digital Packet Data (CDPD)** - Configuration,
- **Global System for Mobile Communication (GSM)** - Configuration,
- **Short Message Service (SMS)** - Configuration,
- **Trunked Mobile Radio (TMR, TETRA, Project25)** - Configuration,
- **IEEE 802.16 Broadband Wireless Access Standards** - Configuration,
- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

General Internet and De Facto Data Management Technologies

- **Common Warehouse Model (CWM)** - Data Management
- **American Standard Code for Information Interchange (ASCII)** - Data Management
- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

---

Alternative Best Practices

Data Management

- **Backup Databases** - Quality of Service,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,

- **ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,

Federal Documents on Security Technologies

- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1040 Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication** - Security,
- **RFC 1423 Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers** - Security,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1579 Firewall-Friendly FTP** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,

- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2888 Secure Remote Access with L2TP** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2979 Behavior of and Requirements for Internet Firewalls** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,

- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **W3C The Platform for Privacy Preferences 1.1 (P3P1.1) SpecificationW3C Working Draft** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,

Possible Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61334 – Distribution PLC** - Configuration,

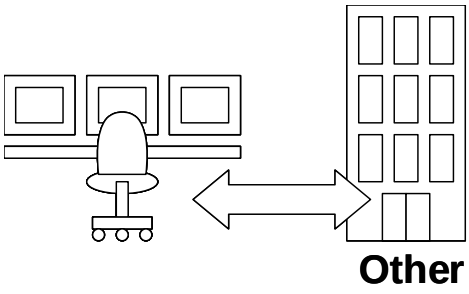
Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Wireless Technologies

- **Paging Systems** - Configuration,

Control Centers to Corporate Environment - #12



This environment captures the requirements for passing data between control centers and external corporations.

Typical Applications: Gathering weather data, communicating with regulators, auditors and vendors. May include passing historical data, specifications, network topologies, configuration files, debug traces. Possibly remote login by trusted vendors.

Characteristics: A business-to-business environment; security is therefore important, but data rarely involves safety or reliability issues. Speed, volume and quality of service requirements are very low. Data tends to be transferred in file format rather than real-time updates.

Similar Environments: Similar technologically to the other business-to-business environments, but does not involve real-time operational, contractual, or marketing information.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions across widely distributed sites

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)
- Provide Inter-Domain Security Service (support security requirements across organizational boundaries)
- Provide Security Assurance Service (determine the level of security provided by another environment)
- Provide Audit Service (responsible for producing records, which track security relevant events)

- Provide Security Policy Service (concerned with the management of security policies)
- Provide Firewall Transversal
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Protocol mapping (the ability to convert from one protocol to another)
- Provide Security Discovery (the ability to determine what security services are available for use)

Data Management Requirements

- Support extensive data validation procedures
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping
- Support the management of data across organizational boundaries

---

Recommended Technologies

Energy Industry-Specific Technologies

Utility Control Center Related Data Management Technologies

- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **CIM Extensions for Market Operations** - Data Management
- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration, Data Management
- **IEC61968 SIDM System Interfaces for Distribution Management** - Data Management

Customer Interface Data Management Technologies

- **IEC62056 – Data Exchange for Meter Reading, Tariff, and Load Control** - Data Management
- **ANSI C12.19 (Meter Tables)** - Data Management
- **AEIC Guidelines** - Data Management

Communications Industry Technologies

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Link Layer and Physical Technologies

- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Computer Systems Related Technologies

- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ANSI/ISO/IEC 8632-1, 2, 3, 4 – Computer Graphics Metafile (CGM)** - Data Management
- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management
- **ANSI/ISO/IEC 9075 – Structured Query Language (SQL)** - Data Management

eCommerce Related Data Management Technologies

- **ebXML** - Data Management
- **ebXML Collaboration Protocol Profiles (CPPA)** - Data Management
- **ebXML Messaging** - Data Management
- **ebXML Registry** - Data Management
- **ISO/IEC JTC 1 SC32 - ISO/IEC 15944-1:2002 Information technology -- Business agreement semantic descriptive techniques -- Part 1: Operational aspects of Open-EDI for implementation** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,

- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security,
- **Intrusion Prevention Systems (IPS)** - Security,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **OASIS Extensible Access Control Markup Language (XACML** - Security,
- **XML Key Management Specification (XKMS** - Security,

- **Secure XML** - Security,

Network and Enterprise Management Technologies

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Confidentiality** - Security,
- **Firewall Traversal** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Inter-Domain Security** - Security,
- **Security Policies** - Security,
- **Quality of Identity Service** - Security,
- **Security Assurance Management** - Security,
- **Security Protocol Mapping** - Security,
- **Security Service Availability Discovery Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Data Management
- **Alarm Detection/Reporting** - Data Management
- **Instrumentation and Monitoring Service** - Data Management
- **Measurement Data Logging Service** - Security,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Data Management
- **Time Stamping** - Security, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Management of Data Consistency and Synchronization across Systems** - Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Security, Data Management

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Security,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,

Security Technology Documents

Alternative Technologies

Utility Control Center Related Data Management Technologies

- **MultiSpeak** - Data Management

Access Technologies

- **Public Internet** - Configuration,

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

IP-based Transport Protocols

- **Stream Control Transmission Protocol (SCTP)** - Configuration,
- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Link Layer and Physical Technologies

- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

General Internet and De Facto Data Management Technologies

- **Common Warehouse Model (CWM)** - Data Management
- **American Standard Code for Information Interchange (ASCII)** - Data Management
- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

Alternative Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,
- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO 9735-9:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 9: Security key** - Security,

- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,

- **ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,
- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1579 Firewall-Friendly FTP** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,

- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2888 Secure Remote Access with L2TP** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2979 Behavior of and Requirements for Internet Firewalls** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,

- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

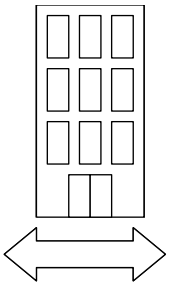
---

Possible Technologies

Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Intra-Corporation Environment - #13



This environment includes the requirements for exchanging data between what was traditionally called the “Control Network”, or the “Energy Management Network”, and the rest of the organization. The usual point of contact between the corporation and this data is the Energy Management System, although links from corporate networks to other types of equipment are increasing.

Typical Applications: Long term network planning, protection engineering, asset management, facilities management, graphical information systems, and operator training.

Characteristics: Security is important, but several types of attacks need not be addressed because the data travels within the corporate network. A huge variety of formats and volumes of data must be exchanged, very specific to particular applications. The data may be considered “real-time” but for these purposes, response times of minutes or hours are typically adequate.

Similar environments: Similar to Control Center / ESP or Control Center / External Corporations, but the amount and variety of data is much greater.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions within a contained environment (e.g. substation or control center)

Quality of Service Requirements

- Provide medium speed messaging on the order of 10 seconds
- Support time synchronization of data for age and time-skew information

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Audit Service (responsible for producing records, which track security relevant events)

- Provide Security Policy Service (concerned with the management of security policies)
- Provide Firewall Transversal
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support the management of large volumes of data flows
- Support keeping the data up-to-date
- Support extensive data validation procedures
- Support keeping data consistent and synchronized across systems and/or databases
- Support timely access to data by multiple different users
- Support frequent changes in types of data exchanged
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Support the exchange of unstructured or special-format data (e.g. text, documents, oscillographic data)
- Support transaction integrity (consistency and rollback capability)
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping

Recommended Technologies

Energy Industry-Specific Technologies

Utility Control Center Related Data Management Technologies

- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration, Quality of Service, Data Management
- **IEC61968 SIDM System Interfaces for Distribution Management** - Data Management
- **OPEN GIS** - Data Management

Communications Industry Technologies

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Application Layer Protocols

- **SNTP (Network Time Protocol)** - Quality of Service, Data Management

Link Layer and Physical Technologies

- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Wireless Technologies

- **Global Positioning System (GPS)** - Quality of Service, Data Management

Computer Systems Related Technologies

- **CORBA and CORBA Services** - Data Management
- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **Enterprise Java Beans (EJB)** - Data Management
- **IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems** - Quality of Service,
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ANSI/ISO/IEC 8632-1, 2, 3, 4 – Computer Graphics Metafile (CGM)** - Data Management
- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management
- **ANSI/ISO/IEC 9075 – Structured Query Language (SQL)** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Quality of Service, Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service, Security, Data Management
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,

Web-based Network Management

- **Web-based Enterprise Management (WBEM)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Firewall Traversal** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Security Policies** - Security,
- **Quality of Identity Service** - Security,
- **Security Service Availability Discovery Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,
- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,

- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,
- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Distributed Data Management Service** - Data Management
- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management, Data Management
- **Alarm Detection/Reporting** - Network Management, Data Management
- **Instrumentation and Monitoring Service** - Network Management, Data Management
- **Measurement Data Logging Service** - Security, Network Management,
- **Remote Control** - Network Management,
- **Network Time** - Data Management
- **File Transfer** - Data Management

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management
- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,
- **Transactions** - Data Management
- **Checkpoint and Recovery** - Network Management, Data Management
- **Workflow Service** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Network Management, Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Quality of Service, Network Management, Data Management
- **Time Stamping** - Quality of Service, Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Data Update Management** - Data Management

- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Quality of Service, Data Management
- **Management of Data Consistency and Synchronization across Systems** - Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Transaction Integrity (backup and rollback capability)** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Data Storage and Access Management** - Data Management
- **Data Consistency across Multiple Systems** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Security, Data Management
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 10164-8:1993 Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function** - Quality of Service, Data Management
- **ISO/IEC 18014-1:2002 Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework** - Quality of Service,
- **ISO/IEC 18014-2:2002 Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens** - Quality of Service,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,

- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **C37.111-1999 IEEE COMTRADE Standard (Common Format for Transient Data Exchange) for Power Systems** - Data Management
- **IEEE 1159.3 - Power Quality Data Interchange Format (PQDIF)** - Data Management

Utility Control Center Related Data Management Technologies

- **MultiSpeak** - Data Management

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

IP-based Transport Protocols

- **Stream Control Transmission Protocol (SCTP)** - Configuration,
- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Application Layer Protocols

- **Microsoft COM+** - Data Management

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,
- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **IEEE 802.11 Wireless Local Area Network (WLAN)** - Configuration,
- **IEEE 802.15 Wireless Personal Area Network (PAN)** - Configuration,
- **Bluetooth Special** - Configuration,
- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

Computer Systems Related Technologies

- **Web Services Description Language (WSDL)** - Data Management

General Internet and De Facto Data Management Technologies

- **Common Warehouse Model (CWM)** - Data Management
- **American Standard Code for Information Interchange (ASCII)** - Data Management
- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

eCommerce Related Data Management Technologies

- **EAN.UCC Identification Numbers** - Data Management
- **EAN.UCC Universal Bar Codes** - Data Management
- **10303 Standard Exchange for Product Data (STEP)** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

---

Alternative Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,
- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,

- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,
- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,

- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Quality of Service,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1579 Firewall-Friendly FTP** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,

- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2979 Behavior of and Requirements for Internet Firewalls** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,

- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

---

Possible Technologies

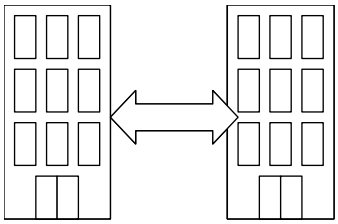
Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Application Layer Protocols

- **CSV files** - Data Management

Inter-Corporation Environment - #14



This environment consists of the requirements for standard business communications between power system organizations and others.

Typical Applications: Contracts, email, regulations, sales, marketing, orders and invoices.

Characteristics: Business-to-business, relatively small volumes of traffic, typically file-oriented but a variety of file types, with acceptable response times in hours or days.

Similar Environments: Similar technologically to other business-to-business environments, but not related to operational, safety or reliability issues in real-time.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions across widely distributed sites

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)
- Provide Inter-Domain Security Service (support security requirements across organizational boundaries)
- Provide Non-repudiation Service (cannot deny that interaction took place)
- Provide Security Assurance Service (determine the level of security provided by another environment)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Trust Establishment Security Service (security verification across multiple organizations)

- Provide Path and Routing Quality of Security (being able to determine a secure communication path)
- Provide Firewall Transversal
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Protocol mapping (the ability to convert from one protocol to another)
- Provide Security Discovery (the ability to determine what security services are available for use)

Data Management Requirements

- Support extensive data validation procedures
- Support frequent changes in types of data exchanged
- Support management of data whose types can vary significantly in different implementations
- Provide discovery service (discovering available services and their characteristics)
- Provide services for spontaneously finding and joining a community
- Provide conversion and protocol mapping
- Support the management of data across organizational boundaries

---

Recommended Technologies

Energy Industry-Specific Technologies

Utility Control Center Related Data Management Technologies

- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **CIM Extensions for Market Operations** - Data Management
- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration, Data Management

Communications Industry Technologies

Access Technologies

- **Public Internet** - Configuration,
- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Link Layer and Physical Technologies

- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Computer Systems Related Technologies

- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management
- **ANSI/ISO/IEC 9075 – Structured Query Language (SQL)** - Data Management

eCommerce Related Data Management Technologies

- **ebXML** - Data Management
- **ebXML Collaboration Protocol Profiles (CPPA)** - Data Management
- **ebXML Messaging** - Data Management
- **ebXML Registry** - Data Management
- **ISO/IEC JTC 1 SC32 - ISO/IEC 15944-1:2002 Information technology -- Business agreement semantic descriptive techniques -- Part 1: Operational aspects of Open-EDI for implementation** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,

- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security,
- **Intrusion Prevention Systems (IPS)** - Security,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **OASIS Extensible Access Control Markup Language (XACML** - Security,
- **XML Key Management Specification (XKMS** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Confidentiality** - Security,
- **Firewall Traversal** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Inter-Domain Security** - Security,
- **Non-repudiation** - Security,
- **Path Routing and QOS Service** - Security,
- **Security Policies** - Security,
- **Quality of Identity Service** - Security,
- **Security Assurance Management** - Security,
- **Security Protocol Mapping** - Security,
- **Security Service Availability Discovery Service** - Security,
- **Trust Establishment Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Data Management
- **Alarm Detection/Reporting** - Data Management
- **Instrumentation and Monitoring Service** - Data Management
- **Measurement Data Logging Service** - Security,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Data Management

- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Data Management
- **Time Stamping** - Security, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Management of Data Consistency and Synchronization across Systems** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Security, Data Management

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2350 Expectations for Computer Security Incident Response** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Security,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,

Security Technology Documents

Alternative Technologies

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

IP-based Transport Protocols

- **Stream Control Transmission Protocol (SCTP)** - Configuration,
- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Link Layer and Physical Technologies

- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

Computer Systems Related Technologies

- **CORBA and CORBA Services** - Data Management
- **Web Services Description Language (WSDL)** - Data Management
- **Enterprise Java Beans (EJB)** - Data Management

General Internet and De Facto Data Management Technologies

- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

Alternative Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,
- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO 9735-9:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 9: Security key** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,

- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO/IEC 10181-4:1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General** - Security,
- **ISO/IEC 13888-2:1998 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques** - Security,
- **ISO/IEC 13888-3:1997 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,

- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1579 Firewall-Friendly FTP** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,

- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2888 Secure Remote Access with L2TP** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2979 Behavior of and Requirements for Internet Firewalls** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,

- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

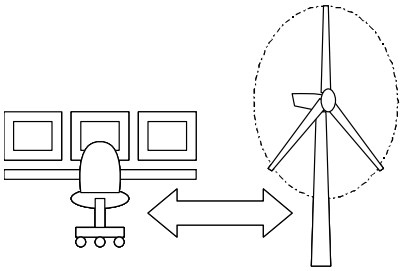
---

Possible Technologies

Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

DER Monitoring and Control Environment - #15



This environment encompasses the communications between distributed energy resources and the organizations that must monitor and operate them.

Typical Applications: Energy Service Provider aggregating data from multiple small generators, including renewable power, small hydro, co-generation; or operating the distributed resources as a service to a utility. Uses include demand response and adjustment of power quality.

Characteristics: It is vital that these message exchanges not be tampered, monitored, or interfered with by unauthorized persons. Quality of service requirements are based around human reaction times. Configuration of the network changes frequently. Could also include transfer of data that is high-volume and critical, such as configuration files or fault recordings.

Similar Environments: Very similar to Critical Operations DAC, except that the volume of traffic may be lower and that communications links to DER sites may be higher bandwidth.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions between a few "clients" and many "servers"
- Support interactions across widely distributed sites
- Support multi-cast or broadcast capabilities

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)
- Provide Inter-Domain Security Service (support security requirements across organizational boundaries)
- Provide Non-repudiation Service (cannot deny that interaction took place)

- Provide Security Assurance Service (determine the level of security provided by another environment)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Firewall Transversal
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Protocol mapping (the ability to convert from one protocol to another)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support extensive data validation procedures
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping
- Support the management of data across organizational boundaries

---

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Part 7-2 – Abstract Common Services Interface (ACSI)** - Configuration,
- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Network Management, Data Management
- **IEC61850 Power Quality Object Models** - Data Management
- **IEC62350 – Object Models for Distributed Energy Resources (DER)** - Network Management, Data Management
- **IEC62349 – Hydro Power Plant Object Models** - Network Management, Data Management

- **IEC61400-25 for Wind Power Object Models** - Network Management, Data Management

Utility Control Center Related Data Management Technologies

- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **CIM Extensions for Market Operations** - Data Management
- **NERC e-tagging** - Data Management
- **NAESB OASIS for Market Transactions** - Data Management

Customer Interface Data Management Technologies

- **IEC62056 – Data Exchange for Meter Reading, Tariff, and Load Control** - Data Management
- **ANSI C12.19 (Meter Tables)** - Data Management
- **AEIC Guidelines** - Data Management

Communications Industry Technologies

Access Technologies

- **Public Internet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Link Layer and Physical Technologies

- **LAN/MAN Technologies** - Configuration,
- **IEEE 802 MAC Addresses** - Configuration,
- **Ethernet** - Configuration,
- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Computer Systems Related Technologies

- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management
- **ANSI/ISO/IEC 9075 – Structured Query Language (SQL)** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,

- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **OASIS Extensible Access Control Markup Language (XACML** - Security,
- **XML Key Management Specification (XKMS** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,
- **IEC 62351-7 Objects for Network Management** - Network Management, Data Management

Web-based Network Management

- **Web-based Enterprise Management (WBEM)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Confidentiality** - Security,
- **Firewall Traversal** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Inter-Domain Security** - Security,
- **Non-repudiation** - Security,
- **Security Policies** - Security,
- **Quality of Identity Service** - Security,
- **Security Assurance Management** - Security,

- **Security Protocol Mapping** - Security,
- **Security Service Availability Discovery Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,
- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,
- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management,
- **Alarm Detection/Reporting** - Network Management, Data Management
- **Instrumentation and Monitoring Service** - Network Management, Data Management
- **Measurement Data Logging Service** - Security, Network Management,
- **Remote Control** - Network Management,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management
- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,
- **Checkpoint and Recovery** - Network Management,
- **Workflow Service** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Network Management, Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Network Management, Data Management
- **Time Stamping** - Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Management of Data Consistency and Synchronization across Systems** - Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Security, Data Management
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,

- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Security, Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 104 – Telecontrol Protocol over TCP/IP** - Configuration,
- **DNP3 Protocol over TCP/IP** - Configuration,
- **ISO 9506 MMS – Manufacturing Messaging Specification** - Configuration,

Utility Control Center Related Data Management Technologies

- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration,

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Host extensions for IP multicasting** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

IP-based Transport Protocols

- **Stream Control Transmission Protocol (SCTP)** - Configuration,
- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,

- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

Computer Systems Related Technologies

- **Enterprise Java Beans (EJB)** - Data Management

General Internet and De Facto Data Management Technologies

- **American Standard Code for Information Interchange (ASCII)** - Data Management
- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

---

Alternative Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,
- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO 9735-9:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 9: Security key** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,

- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO/IEC 10181-4:1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General** - Security,
- **ISO/IEC 13888-2:1998 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques** - Security,
- **ISO/IEC 13888-3:1997 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,

- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1579 Firewall-Friendly FTP** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,

- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2888 Secure Remote Access with L2TP** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2979 Behavior of and Requirements for Internet Firewalls** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

---

Possible Technologies

Utility Field Device Related Data Exchange Technologies

Utility Control Center Related Data Management Technologies

- **IEC 60870-6 (ICCP)** - Configuration,

Customer Automated Meter Reading (AMR) Technologies

- **Broadband over Power Line (BPL)** - Configuration,

Networking Technologies

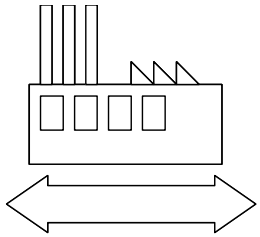
- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,

- **Routing Information Protocol (RIP)** - Configuration,

Wireless Technologies

- **TDMA Cellular Wireless – IS-136** - Configuration,
- **CDMA Cellular Wireless – IS-95** - Configuration,
- **Cellular Digital Packet Data (CDPD)** - Configuration,
- **Global System for Mobile Communication (GSM)** - Configuration,

Intra-Customer Site Environment - #16



This environment encompasses communications that are local to customer sites.

Typical Applications: A customer bringing processes online or offline in response to real-time pricing decisions; A customer locally managing distributed energy resources in response to emissions, environmental conditions, fuel availability, or regulations; building automation for environmental control.

Characteristics: Critical data, but with a local scope and limited impact on the overall grid. Types of possible security attacks somewhat limited thanks to physical security. Data is real-time, possibly peer-to-peer, with response times potentially measured in milliseconds if process control is involved. Available communications technologies and devices tend to be less "hardened" or redundant because of a less harsh physical environment and have corresponding lower quality of service requirements.

Similar Environments: This environment is similar to Critical Operations Intra-Substation or the Deterministic Rapid Response environments. However, failures in this environment have a more limited range of effect on the overall power network, and it is generally a less harsh physical environment with lower required quality of service.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions within a contained environment (e.g. substation or control center)

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)

- Provide User Profile and User Management (combination of several other security services)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support extensive data validation procedures
- Support keeping data consistent and synchronized across systems and/or databases
- Support frequent changes in types of data exchanged
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Provide conversion and protocol mapping

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Part 7-2 – Abstract Common Services Interface (ACSI)** - Configuration,
- **IEC61850 Power Quality Object Models** - Data Management
- **IEC62350 – Object Models for Distributed Energy Resources (DER)** - Network Management, Data Management
- **IEC61400-25 for Wind Power Object Models** - Network Management, Data Management

Utility Control Center Related Data Management Technologies

- **NERC e-tagging** - Data Management
- **NAESB OASIS for Market Transactions** - Data Management
- **OPEN GIS** - Data Management
- **OAG** - Data Management
- **MultiSpeak** - Data Management

Customer Interface Data Management Technologies

- **IEC62056 – Data Exchange for Meter Reading, Tariff, and Load Control** - Data Management

- **ANSI C12.19 (Meter Tables)** - Data Management
- **AEIC Guidelines** - Data Management

Communications Industry Technologies

Access Technologies

- **Private Intranet** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Application Layer Protocols

- **SNTP (Network Time Protocol)** - Data Management

Link Layer and Physical Technologies

- **Asynchronous Transfer Mode (ATM)** - Configuration,

Wireless Technologies

- **Global Positioning System (GPS)** - Data Management

Computer Systems Related Technologies

- **CORBA and CORBA Services** - Data Management
- **Web Services** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **Enterprise Java Beans (EJB)** - Data Management
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ANSI/ISO/IEC 8632-1, 2, 3, 4 – Computer Graphics Metafile (CGM)** - Data Management
- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security, Data Management
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,
- **IEC 62351-7 Objects for Network Management** - Network Management, Data Management

Web-based Network Management

- **Web-based Enterprise Management (WBEM)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Security Policies** - Security,
- **Quality of Identity Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,
- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,

- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Distributed Data Management Service** - Data Management
- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management, Data Management
- **Alarm Detection/Reporting** - Network Management, Data Management
- **Instrumentation and Monitoring Service** - Network Management, Data Management
- **Measurement Data Logging Service** - Security, Network Management,
- **Remote Control** - Network Management,
- **Network Time** - Data Management

Common Platform Services

Platform Services

- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,
- **Checkpoint and Recovery** - Network Management,
- **Workflow Service** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Network Management, Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Network Management, Data Management
- **Time Stamping** - Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Data Update Management** - Data Management
- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Data Management
- **Management of Data Consistency and Synchronization across Systems** - Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management

- **Management of Manual Data Entry** - Data Management
- **Data Consistency across Multiple Systems** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Security, Data Management
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 10164-8:1993 Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function** - Data Management
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Part 7-2 – GSE (GOOSE and GSSE** - Configuration,

Customer Interface Data Management Technologies

- **ASHRAE SSPC135 BACnet** - Configuration,
- **GPC-20 XML Modeling for HVAC** - Configuration, Data Management
- **CEBus based on EIA 600** - Configuration,
- **UPnP** - Configuration,

Networking Technologies

- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

IP-based Transport Protocols

- **Stream Control Transmission Protocol (SCTP)** - Configuration,
- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Application Layer Protocols

- **Microsoft COM+** - Data Management

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,
- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,

Wireless Technologies

- **IEEE 802.11 Wireless Local Area Network (WLAN)** - Configuration,
- **IEEE 802.15 Wireless Personal Area Network (PAN)** - Configuration,
- **Bluetooth Special** - Configuration,
- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

Computer Systems Related Technologies

- **Web Services Description Language (WSDL)** - Data Management

General Internet and De Facto Data Management Technologies

- **Common Warehouse Model (CWM)** - Data Management
- **American Standard Code for Information Interchange (ASCII)** - Data Management
- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

---

Alternative Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,

- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,
- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,

- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,
- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,

- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,

- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

---

Possible Technologies

Utility Field Device Related Data Exchange Technologies

- **Fieldbus** - Configuration,
- **PROFIBUS** - Configuration,
- **Modbus** - Configuration,
- **Modbus TCP/IP** - Configuration,
- **Modbus Plus** - Configuration,

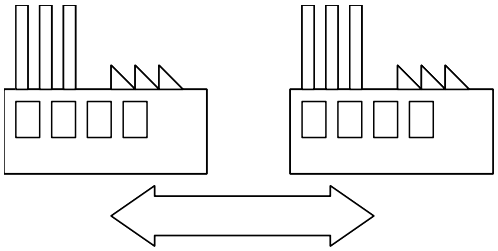
Customer Site In-Building Technologies

- **Home PNA** - Configuration,
- **HomePlug** - Configuration,
- **Zigbee Spec** - Configuration,

Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Inter-Customer Sites Environment - #17



This environment captures requirements for communications between customer sites. This is a relatively new environment, not widely deployed yet.

Typical Applications: Management of micro-grids between customers.

Characteristics: High security requirements because of data crossing organizational boundaries, but relatively few, simple messages.

Similar Environments: Similar to Inter-Control Center, but with much lower volumes and variety of data, and less potential impact on the grid.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions across widely distributed sites

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)
- Provide Inter-Domain Security Service (support security requirements across organizational boundaries)
- Provide Non-repudiation Service (cannot deny that interaction took place)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Firewall Transversal
- Provide Privacy Service (the ability to ensure person information is not disclosed)
- Provide User Profile and User Management (combination of several other security services)

- Provide Security Protocol mapping (the ability to convert from one protocol to another)
- Provide Security Discovery (the ability to determine what security services are available for use)

Data Management Requirements

- Support extensive data validation procedures
- Support frequent changes in types of data exchanged
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping
- Support the management of data across organizational boundaries

---

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Part 7-2 – Abstract Common Services Interface (ACSI)** - Configuration,
- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Security, Data Management
- **IEC61850 Part 6 – Substation Configuration Language** - Security, Data Management
- **IEC61850 Power Quality Object Models** - Data Management
- **IEC62350 – Object Models for Distributed Energy Resources (DER)** - Security, Data Management
- **IEC62349 – Hydro Power Plant Object Models** - Security, Data Management
- **IEC61400-25 for Wind Power Object Models** - Security, Data Management

Utility Control Center Related Data Management Technologies

- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration, Data Management

Communications Industry Technologies

Access Technologies

- **Public Internet** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Link Layer and Physical Technologies

- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Computer Systems Related Technologies

- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management

eCommerce Related Data Management Technologies

- **ebXML** - Data Management
- **ebXML Collaboration Protocol Profiles (CPPA)** - Data Management
- **ebXML Messaging** - Data Management
- **ebXML Registry** - Data Management
- **ISO/IEC JTC 1 SC32 - ISO/IEC 15944-1:2002 Information technology -- Business agreement semantic descriptive techniques -- Part 1: Operational aspects of Open-EDI for implementation** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,

- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security,
- **Intrusion Prevention Systems (IPS)** - Security,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **OASIS Extensible Access Control Markup Language (XACML** - Security,
- **XML Key Management Specification (XKMS** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **IEC 62351-7 Objects for Network Management** - Data Management

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Confidentiality** - Security,
- **Firewall Traversal** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Inter-Domain Security** - Security,
- **Non-repudiation** - Security,
- **Security Policies** - Security,
- **Privacy Service** - Security,
- **Quality of Identity Service** - Security,
- **Security Protocol Mapping** - Security,
- **Security Service Availability Discovery Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Data Management
- **Alarm Detection/Reporting** - Data Management
- **Instrumentation and Monitoring Service** - Data Management
- **Measurement Data Logging Service** - Security,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Data Management
- **Time Stamping** - Security, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Management of Data Consistency and Synchronization across Systems** - Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Security, Data Management

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Security,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,

Security Technology Documents

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 104 – Telecontrol Protocol over TCP/IP** - Configuration,
- **DNP3 Protocol over TCP/IP** - Configuration,
- **ISO 9506 MMS – Manufacturing Messaging Specification** - Configuration,

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

IP-based Transport Protocols

- **Stream Control Transmission Protocol (SCTP)** - Configuration,
- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Link Layer and Physical Technologies

- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

Computer Systems Related Technologies

- **CORBA and CORBA Services** - Data Management
- **Web Services Description Language (WSDL)** - Data Management
- **Enterprise Java Beans (EJB)** - Data Management

General Internet and De Facto Data Management Technologies

- **Common Warehouse Model (CWM)** - Data Management

- **American Standard Code for Information Interchange (ASCII)** - Data Management
- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

Alternative Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,

- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO/IEC 10181-4:1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General** - Security,
- **ISO/IEC 13888-2:1998 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques** - Security,

- **ISO/IEC 13888-3:1997 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,
- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1040 Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication** - Security,
- **RFC 1423 Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers** - Security,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1579 Firewall-Friendly FTP** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,

- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2888 Secure Remote Access with L2TP** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2979 Behavior of and Requirements for Internet Firewalls** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,

- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **W3C The Platform for Privacy Preferences 1.1 (P3P1.1) SpecificationW3C Working Draft** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

---

Possible Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 101 – Serial Telecontrol Protocol** - Configuration,

- **DNP Serial Protocol** - Configuration,

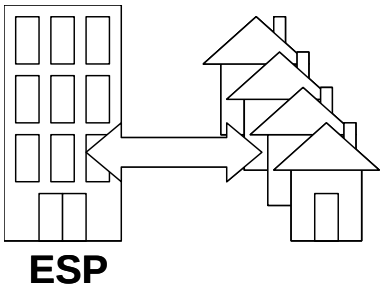
Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Wireless Technologies

- **TDMA Cellular Wireless – IS-136** - Configuration,
- **CDMA Cellular Wireless – IS-95** - Configuration,
- **Cellular Digital Packet Data (CDPD)** - Configuration,
- **Global System for Mobile Communication (GSM)** - Configuration,

Customer to ESP Environment - #18



This environment encompasses communications between end customers and the utility, aggregator, or Energy Service Provider (ESP) to which they are connected. This environment includes the requirements for what is traditionally known as Automatic Meter Reading (AMR).

Typical applications: Customer metering, management of distributed energy resources on customer sites, real-time pricing and demand response.

Characteristics: Extremely large volumes of data are transferred, and there are frequent configuration and topology changes. Commands are often broadcast due to the large number of end users. Data is critical due to the potential for fraud and the impact on generation. Ease of use and low cost of technologies at the customer end is critical.

Similar Environments: Similar to Control Center to Customer Equipment, or Critical Operations DAC, but the volume of data is much larger.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions between a few "clients" and many "servers"
- Support interactions across widely distributed sites
- Support multi-cast or broadcast capabilities
- Support the frequent change of configuration and/or location of end devices or sites

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)

- Provide Inter-Domain Security Service (support security requirements across organizational boundaries)
- Provide Non-repudiation Service (cannot deny that interaction took place)
- Provide Security Assurance Service (determine the level of security provided by another environment)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Firewall Transversal
- Provide Privacy Service (the ability to ensure person information is not disclosed)
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Protocol mapping (the ability to convert from one protocol to another)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)

Data Management Requirements

- Support the management of large volumes of data flows
- Support extensive data validation procedures
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping
- Support the management of data across organizational boundaries

---

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Part 7-2 – Abstract Common Services Interface (ACSI)** - Configuration, Data Management
- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Data Management
- **IEC61850 Part 6 – Substation Configuration Language** - Data Management

- **IEC61850 Power Quality Object Models** - Data Management
- **IEC62350 – Object Models for Distributed Energy Resources (DER)** - Data Management
- **IEC62349 – Hydro Power Plant Object Models** - Data Management
- **IEC61400-25 for Wind Power Object Models** - Data Management

Customer Interface Data Management Technologies

- **IEC62056 – Data Exchange for Meter Reading, Tariff, and Load Control** - Data Management
- **ANSI C12.19 (Meter Tables)** - Data Management
- **AEIC Guidelines** - Data Management

Customer Automated Meter Reading (AMR) Technologies

- **1390.3-1999** - Configuration,

Communications Industry Technologies

Access Technologies

- **Public Internet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Link Layer and Physical Technologies

- **LAN/MAN Technologies** - Configuration,
- **IEEE 802 MAC Addresses** - Configuration,
- **Ethernet** - Configuration,
- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Computer Systems Related Technologies

- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management

eCommerce Related Data Management Technologies

- **ebXML** - Data Management
- **ebXML Collaboration Protocol Profiles (CPPA)** - Data Management
- **ebXML Messaging** - Data Management
- **ebXML Registry** - Data Management
- **ISO/IEC JTC 1 SC32 - ISO/IEC 15944-1:2002 Information technology -- Business agreement semantic descriptive techniques -- Part 1: Operational aspects of Open-EDI for implementation** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security, Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,

- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **OASIS Extensible Access Control Markup Language (XACML** - Security,
- **XML Key Management Specification (XKMS** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,
- **IEC 62351-7 Objects for Network Management** - Data Management

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Confidentiality** - Security,
- **Firewall Traversal** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Inter-Domain Security** - Security,

- **Non-repudiation** - Security,
- **Security Policies** - Security,
- **Privacy Service** - Security,
- **Quality of Identity Service** - Security,
- **Security Assurance Management** - Security,
- **Security Protocol Mapping** - Security,
- **Security Service Availability Discovery Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Data Management
- **Generic Eventing And Subscription** - Data Management
- **Alarm Detection/Reporting** - Data Management
- **Instrumentation and Monitoring Service** - Data Management
- **Measurement Data Logging Service** - Security,

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Data Management
- **Time Stamping** - Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Management of Data Consistency and Synchronization across Systems** - Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Data Storage and Access Management** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Security, Data Management

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Security, Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,

- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **ISO 9506 MMS – Manufacturing Messaging Specification** - Configuration,

Customer Interface Data Management Technologies

- **ASHRAE SSPC135 BACnet** - Configuration,
- **GPC-20 XML Modeling for HVAC** - Data Management
- **CEBus based on EIA 600** - Configuration,

Customer Automated Meter Reading (AMR) Technologies

- **ANSI C12.21 (POTS)** - Configuration,
- **ANSI C12.22 (EPSEM)** - Configuration,

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Host extensions for IP multicasting** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

IP-based Transport Protocols

- **Stream Control Transmission Protocol (SCTP)** - Configuration,
- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,
- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

General Internet and De Facto Data Management Technologies

- **American Standard Code for Information Interchange (ASCII)** - Data Management
- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

---

Alternative Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,
- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO 9735-9:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 9: Security key** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,

- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO/IEC 10181-4:1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General** - Security,
- **ISO/IEC 13888-2:1998 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques** - Security,
- **ISO/IEC 13888-3:1997 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,

- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1040 Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication** - Security,
- **RFC 1423 Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers** - Security,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1579 Firewall-Friendly FTP** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,

- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2888 Secure Remote Access with L2TP** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2979 Behavior of and Requirements for Internet Firewalls** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,

- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **W3C The Platform for Privacy Preferences 1.1 (P3P1.1) SpecificationW3C Working Draft** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

---

Possible Technologies

Customer Automated Meter Reading (AMR) Technologies

- **Broadband over Power Line (BPL)** - Configuration,

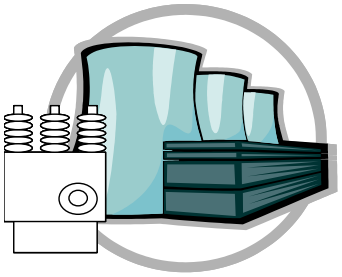
Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Wireless Technologies

- **TDMA Cellular Wireless – IS-136** - Configuration,
- **CDMA Cellular Wireless – IS-95** - Configuration,
- **Cellular Digital Packet Data (CDPD)** - Configuration,
- **Global System for Mobile Communication (GSM)** - Configuration,

HV Generation Plant Environment - #19



This environment captures the requirements for communications within the electrical and physical site of the generating plant up to the point of common coupling with the area power system.

Typical Applications: Frequency and Volt/VAR control, load shedding under emergency conditions, cold start of generation, local displays on graphical user interfaces. Also involves plant management systems for other plant equipment, such as fuel systems, burners, boilers, turbines, cooling systems, historical records, market operations, etc.

Characteristics: Critical data in a real-time, process-control environment, but security attacks may be limited by very strong physical security.

Similar Environments: Very similar to Critical Operations Intra-Substation, with slightly lower quality of service and security requirements due to a more secure and stable physical environment.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions within a contained environment (e.g. substation or control center)

Quality of Service Requirements

- Provide high speed messaging of less than 1 second
- Support high availability of information flows of 99.9+ (~9 hours)

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Audit Service (responsible for producing records, which track security relevant events)

- Provide Security Policy Service (concerned with the management of security policies)
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support extensive data validation procedures
- Support keeping data consistent and synchronized across systems and/or databases
- Support the exchange of unstructured or special-format data (e.g. text, documents, oscillographic data)
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Part 7-2 – Abstract Common Services Interface (ACSI)** - Configuration, Quality of Service, Data Management
- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Network Management, Data Management
- **IEC61850 Part 6 – Substation Configuration Language** - Network Management, Data Management
- **IEC61850 Power Quality Object Models** - Data Management
- **IEC62350 – Object Models for Distributed Energy Resources (DER)** - Network Management, Data Management
- **IEC62349 – Hydro Power Plant Object Models** - Network Management, Data Management
- **IEC61400-25 for Wind Power Object Models** - Network Management, Data Management

Utility Control Center Related Data Management Technologies

- **IEC 60870-6 (ICCP)** - Quality of Service,
- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration, Quality of Service, Data Management

Communications Industry Technologies

Access Technologies

- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Application Layer Protocols

- **SNTP (Network Time Protocol)** - Data Management

Link Layer and Physical Technologies

- **Asynchronous Transfer Mode (ATM)** - Configuration,

Wireless Technologies

- **Global Positioning System (GPS)** - Data Management

Computer Systems Related Technologies

- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ANSI/ISO/IEC 9075 – Structured Query Language (SQL)** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Security, Data Management

- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Security, Network Management,
- **Intrusion Prevention Systems (IPS)** - Security, Network Management,
- **Service Level Agreements (SLA)** - Security,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security, Data Management
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,
- **Secure XML** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,
- **IEC 62351-7 Objects for Network Management** - Quality of Service, Network Management,

Web-based Network Management

- **Web-based Enterprise Management (WBEM)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Audit Common Service** - Security,
- **Authorization for Access Control** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Security Policies** - Security,
- **Quality of Identity Service** - Security,
- **Security Service Availability Discovery Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,
- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,
- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Distributed Data Management Service** - Data Management
- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management, Data Management
- **Alarm Detection/Reporting** - Network Management, Data Management
- **Instrumentation and Monitoring Service** - Network Management, Data Management
- **Measurement Data Logging Service** - Security, Network Management,
- **Remote Control** - Network Management,
- **Network Time** - Data Management
- **File Transfer** - Data Management

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management
- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,
- **Checkpoint and Recovery** - Network Management,
- **Workflow Service** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Backup Databases** - Quality of Service,
- **Metadata Files and Databases** - Network Management, Data Management
- **Quality Flagging** - Network Management, Data Management
- **Time Stamping** - Security, Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Data Update Management** - Data Management
- **Management of Time-Sensitive Data Flows and Timely Access to Data by Multiple Different Users** - Quality of Service, Data Management
- **Management of Data Consistency and Synchronization across Systems** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Data Consistency across Multiple Systems** - Data Management

- **Data Backup and Logging** - Quality of Service, Security, Data Management
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC Security Best Practices** - Security,
- **ISO/IEC 10164-8:1993 Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function** - Data Management
- **ISO/IEC 18014-3:2004 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens** - Security,
- **Federal Security Best Practices** - Security,
- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2276 Architectural Principles of Uniform Resource Name Resolution** - Security,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC60870-5 Part 104 – Telecontrol Protocol over TCP/IP** - Configuration, Quality of Service,
- **DNP3 Protocol over TCP/IP** - Configuration, Quality of Service,

- **ISO 9506 MMS – Manufacturing Messaging Specification** - Configuration, Quality of Service,
- **C37.111-1999 IEEE COMTRADE Standard (Common Format for Transient Data Exchange) for Power Systems** - Data Management
- **IEEE 1159.3 - Power Quality Data Interchange Format (PQDIF)** - Data Management

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

IP-based Transport Protocols

- **Stream Control Transmission Protocol (SCTP)** - Configuration,
- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Application Layer Protocols

- **Microsoft COM+** - Data Management

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,
- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,

Wireless Technologies

- **IEEE 802.11 Wireless Local Area Network (WLAN)** - Configuration,
- **IEEE 802.15 Wireless Personal Area Network (PAN)** - Configuration,
- **Bluetooth Special** - Configuration,
- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,

- **PPTP** - Security,

Computer Systems Related Technologies

- **CORBA and CORBA Services** - Data Management
- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management

eCommerce Related Data Management Technologies

- **EAN.UCC Identification Numbers** - Data Management
- **EAN.UCC Universal Bar Codes** - Data Management
- **10303 Standard Exchange for Product Data (STEP)** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

---

Alternative Best Practices

Data Management

- **Backup Sites** - Quality of Service,

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,

- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,
- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,
- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,

- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security** - Security,
- **ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security** - Security,
- **ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security** - Security,
- **ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general mode** - Security,
- **ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements** - Security,
- **ISO/IEC 17799:2000 Information technology -- Code of practice for information security management** - Security,
- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,

- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,
- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2797 Certificate Management Messages over CMS** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,

- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **WC3 XML Key Management Specification (XKMS 2.0) Bindings** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NERC Certificate Policy for the Energy Market Access and Reliability Certificate (e MARC) Program Version 2.4** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,

- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

---

Possible Technologies

Utility Field Device Related Data Exchange Technologies

- **Fieldbus** - Configuration, Quality of Service,
- **PROFIBUS** - Configuration, Quality of Service,
- **Modbus** - Configuration, Quality of Service,
- **Modbus TCP/IP** - Configuration, Quality of Service,
- **Modbus Plus** - Configuration, Quality of Service,

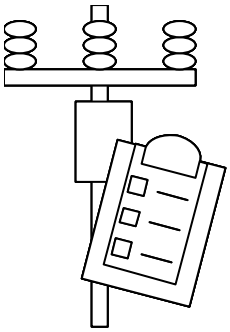
Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Application Layer Protocols

- **CSV files** - Data Management

Field Equipment Maintenance Environment - #20



This environment represents all communications with field crews.

Typical Applications: Asset management, primary equipment monitoring and maintenance, planned outages, statistics gathering, testing, diagnostics, protection engineering, trouble call management, updating of schematics and drawings, emergency (fire, earthquake, flood) response.

Characteristics: Extremely mobile workforce and frequent configuration changes makes wireless communications, ease of use and self-discovery a necessity. Response times in seconds are required due to human reaction times. Data is critical to safe and reliable operation of the grid, and must be keyed to role-based access, i.e. only certain employees have access to certain data.

Similar Environments: Similar to both Critical Operations DAC and Non-Critical Operations DAC, but with an emphasis on mobile access.

Definition: This environment is defined by the following requirements:

Requirements for Defining this Environment

Configuration Requirements

- Support interactions between a few "clients" and many "servers"
- Support interactions across widely distributed sites
- Support mandatory mobile communications

Quality of Service Requirements

- Provide medium speed messaging on the order of 10 seconds
- Support medium availability of information flows of 99.0+ (~3.5 days)

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Firewall Transversal
- Provide User Profile and User Management (combination of several other security services)

- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)

Data Management Requirements

- Support extensive data validation procedures
- Support frequent changes in types of data exchanged
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Support the exchange of unstructured or special-format data (e.g. text, documents, oscillographic data)
- Support transaction integrity (consistency and rollback capability)
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping

Recommended Technologies

Energy Industry-Specific Technologies

Utility Field Device Related Data Exchange Technologies

- **IEC61850 Parts 7-3 and 7-4 – Substation Object Modeling** - Network Management, Data Management
- **IEC61850 Part 6 – Substation Configuration Language** - Network Management, Data Management
- **IEC61850 Power Quality Object Models** - Data Management
- **IEC62350 – Object Models for Distributed Energy Resources (DER)** - Network Management, Data Management
- **IEC62349 – Hydro Power Plant Object Models** - Network Management, Data Management
- **IEC61400-25 for Wind Power Object Models** - Network Management, Data Management

Utility Control Center Related Data Management Technologies

- **IEC 61970 Part 3 - Common Information Model (CIM)** - Data Management
- **CIM Extensions for Market Operations** - Data Management

- **IEC 61970 Part 4 - Generic Interface Definition (GID)** - Configuration, Quality of Service, Data Management
- **IEC61968 SIDM System Interfaces for Distribution Management** - Data Management
- **OPEN GIS** - Data Management

Customer Interface Data Management Technologies

- **IEC62056 – Data Exchange for Meter Reading, Tariff, and Load Control** - Data Management
- **ANSI C12.19 (Meter Tables)** - Data Management
- **AEIC Guidelines** - Data Management

Communications Industry Technologies

Access Technologies

- **Public Internet** - Configuration,
- **Private Intranet** - Configuration,

Networking Technologies

- **Internet Protocol Version V4 (IPV4)** - Configuration,

IP-based Transport Protocols

- **Transmission Control Protocol (TCP)** - Configuration,

Link Layer and Physical Technologies

- **LAN/MAN Technologies** - Configuration,
- **IEEE 802 MAC Addresses** - Configuration,
- **Ethernet** - Configuration,
- **Synchronous Optical Network (SONET)** - Configuration,
- **Asynchronous Transfer Mode (ATM)** - Configuration,

Wireless Technologies

- **Global System for Mobile Communication (GSM)** - Configuration,

Computer Systems Related Technologies

- **Web Services** - Data Management
- **Universal Description, Discovery, and Integration (UDDI)** - Data Management
- **XML Protocol/Simple Object Access Protocol (SOAP)** - Data Management
- **Enterprise Java Beans (EJB)** - Data Management
- **GUID** - Data Management

General Internet and De Facto Data Management Technologies

- **ANSI/ISO/IEC 8632-1, 2, 3, 4 – Computer Graphics Metafile (CGM)** - Data Management
- **ISO/IEC 11179 Parts 1 - 6 Metadata Registries** - Data Management
- **Meta Object Facility (MOF)** - Data Management
- **XML Metadata Interchange (XMI)** - Data Management
- **eXtensible Markup Language (XML)** - Data Management
- **XML Schema (xls)** - Data Management
- **ANSI/ISO/IEC 9075 – Structured Query Language (SQL)** - Data Management

Security Technologies

Policy and Framework Related Technologies

- **ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management** - Security,
- **ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework** - Data Management
- **ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **FIPS PUB 113 Computer Data Authentication** - Security,
- **RFC 2196 Site Security Handbook** - Security,
- **RFC 2401 Security Architecture for the Internet Protocol** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

General Security Technologies

- **FIPS 197 for Advanced Encryption Standard (AES)** - Security,
- **FIPS 186 Digital Signatures Standard (DSS)** - Security,
- **Intrusion Detection Technologies** - Network Management,
- **Intrusion Prevention Systems (IPS)** - Network Management,

Media and Network Layer Technologies

- **Secure IP Architecture (IPSec)** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **Remote Authentication Dial In User Service (RADIUS)** - Security,
- **ATM Security** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations** - Security,

Application Layer Security Technologies

- **RFC 2228 FTP Security Extensions** - Security,
- **Internet Mail Extensions** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **SNMP Security** - Security, Network Management,
- **RFC 1305 Network Time Protocol (Version 3) Specification, Implementation** - Security,
- **IEC 62351-4 Security for Profiles including MMS (ISO-9506)** - Security,
- **IEC 62351-5 Security for IEC 60870-5 and Derivatives** - Security,
- **IEC 62351-6 Security for IEC 61850 GOOSE, GSSE, and SMV Profiles** - Security,

XML Related Technologies

- **OASIS Security Assertion Markup Language (SAML)** - Security,

Network and Enterprise Management Technologies

Network Management Technologies

- **Simple Network Management Protocol (SNMP)** - Network Management,
- **IEC 62351-7 Objects for Network Management** - Quality of Service, Network Management, Data Management

Web-based Network Management

- **Web-based Enterprise Management (WBEM)** - Network Management,

---

Recommended Common Services

Security Services

Common Security Services

- **Authorization for Access Control** - Security,
- **Firewall Traversal** - Security,
- **Identity Establishment Service** - Security,
- **Information Integrity Service** - Security,
- **Quality of Identity Service** - Security,
- **Security Service Availability Discovery Service** - Security,
- **User and Group Management** - Security,

Network and System Management Services

Enterprise Management Services

- **Inventory Management** - Network Management,

- **Communication System/Network Discovery** - Network Management,
- **Routing Management** - Network Management,
- **Traffic Management** - Network Management,
- **Traffic Engineering** - Network Management,
- **System/Network Health-Check Analysis** - Network Management,
- **System/Network Fault Diagnosis** - Network Management,
- **System/Network Fault Correcting** - Network Management,
- **Service Level Agreement (SLA) Determination and Maintenance** - Network Management,
- **System/Network Performance Analysis** - Network Management,
- **System/Network Performance Diagnosis** - Network Management,
- **Performance Tuning/Correction** - Network Management,
- **Accounting and/or Billing** - Network Management,

Data Management Common Services

Data Management Services

- **Object Management Service** - Data Management
- **Address and Naming Management** - Network Management, Data Management
- **Generic Eventing And Subscription** - Network Management,
- **Alarm Detection/Reporting** - Network Management, Data Management
- **Instrumentation and Monitoring Service** - Network Management, Data Management
- **Measurement Data Logging Service** - Network Management,
- **Remote Control** - Network Management,
- **File Transfer** - Data Management

Common Platform Services

Platform Services

- **Component Registry Service** - Data Management
- **Component Lookup Service** - Data Management
- **Component Discovery Service** - Data Management
- **Component Initialization and Termination** - Network Management,
- **Resource Management** - Network Management,
- **Transactions** - Data Management
- **Checkpoint and Recovery** - Network Management, Data Management
- **Workflow Service** - Network Management,

Recommended Best Practices

Data Management Best Practices

Data Management

- **Metadata Files and Databases** - Network Management, Data Management
- **Object Modeling Techniques** - Data Management
- **Quality Flagging** - Network Management, Data Management
- **Time Stamping** - Network Management, Data Management
- **Validation of Source Data and Data Exchanges** - Data Management
- **Data Update Management** - Data Management
- **Management of Data and Object Naming** - Data Management
- **Management of Data Formats in Data Exchanges** - Data Management
- **Management of Transaction Integrity (backup and rollback capability)** - Data Management
- **Management of Data Accuracy** - Data Management
- **Management of Data Acquisition** - Data Management
- **Management of Manual Data Entry** - Data Management
- **Database Maintenance Management** - Data Management
- **Data Backup and Logging** - Quality of Service, Data Management
- **Application Management** - Network Management,

Security Best Practices

Security Frameworks and Policy Documents

- **CICSI 6731.01 Global Command and Control System Security Policy** - Security,
- **FIPS PUB 112 Password Usage** - Security,
- **IETF Security Best Practices Internet Requests for Comments (RFCs)** - Network Management,
- **RFC 1102 Policy routing in Internet protocols** - Network Management,
- **RFC 1322 A Unified Approach to Inter-Domain Routing** - Network Management,
- **RFC 1351** - Network Management,
- **RFC 2008 Implications of Various Address Allocation Policies for Internet Routing** - Network Management,
- **RFC 2196 Site Security Handbook** - Network Management,
- **RFC 2386 A Framework for QoS-based Routing in the Internet** - Network Management,
- **RFC 2505 Anti-Spam Recommendations for SMTP MTAs** - Security,
- **RFC 2518** - Network Management,
- **RFC 2527** - Network Management,

Security Technology Documents

Alternative Technologies

Utility Field Device Related Data Exchange Technologies

- **C37.111-1999 IEEE COMTRADE Standard (Common Format for Transient Data Exchange) for Power Systems** - Data Management
- **IEEE 1159.3 - Power Quality Data Interchange Format (PQDIF)** - Data Management

Utility Control Center Related Data Management Technologies

- **IEC 60870-6 (ICCP)** - Configuration,
- **MultiSpeak** - Data Management

Networking Technologies

- **Internet Protocol Version 6 (IPV6)** - Configuration,
- **Open Shortest Path First (OSPF) Routing Protocol** - Configuration,
- **Border Gateway Protocol (BGP)** - Configuration,
- **Internet Group Management Protocol (IGMP)** - Configuration,
- **Distance Vector Multicast Routing Protocol (DVMRP)** - Configuration,
- **Multicast Open Shortest Path (MOSPF) routing protocol** - Configuration,
- **Protocol Independent Multicast-Sparse Mode (PIM-SM)** - Configuration,
- **Core-Based Tree (CBT) multicast routing** - Configuration,

IP-based Transport Protocols

- **Stream Control Transmission Protocol (SCTP)** - Configuration,
- **Datagram Congestion Control Protocol (DCCP)** - Configuration,
- **Real-Time Transport Protocol (RTP)** - Configuration,

Link Layer and Physical Technologies

- **IEEE 802.1d Spanning Tree Protocol (STP)** - Network Management,
- **IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)** - Network Management,
- **Hubs/Repeaters** - Configuration,
- **Bridges/Switches** - Configuration,
- **Routers** - Configuration,
- **Digital Signal (DSx), Time-division multiplexing, the T-carriers, T1, fractional T1** - Configuration,
- **Frame Relay** - Configuration,

Wireless Technologies

- **3rd Generation Cellular Wireless** - Configuration,
- **Universal Mobile Telecommunication System (UMTS)** - Configuration,
- **Code-Division Multiple Access 2000 (CDMA-2000)** - Configuration,
- **TDMA Cellular Wireless – IS-136** - Configuration,
- **CDMA Cellular Wireless – IS-95** - Configuration,
- **Cellular Digital Packet Data (CDPD)** - Configuration,
- **Short Message Service (SMS)** - Configuration,

- **Trunked Mobile Radio (TMR, TETRA, Project25)** - Configuration,
- **IEEE 802.11 Wireless Local Area Network (WLAN)** - Configuration,
- **IEEE 802.15 Wireless Personal Area Network (PAN)** - Configuration,
- **Bluetooth Special** - Configuration,
- **IEEE 802.16 Broadband Wireless Access Standards** - Configuration,
- **Multiple Address (MAS) Radio** - Configuration,
- **Spread Spectrum Radio System** - Configuration,
- **Satellite Leased Channels and VSAT** - Configuration,
- **Paging Systems** - Configuration,
- **Radio Frequency Identification (RFID)** - Data Management

Virtual Private Networking Technologies

- **Layer 3 VPNs** - Security,
- **Layer 2 VPNs** - Security,
- **PPTP** - Security,

Computer Systems Related Technologies

- **Web Services Description Language (WSDL)** - Data Management

General Internet and De Facto Data Management Technologies

- **Common Warehouse Model (CWM)** - Data Management
- **American Standard Code for Information Interchange (ASCII)** - Data Management
- **Hypertext Markup Language (HTML)** - Data Management
- **RDF** - Data Management

eCommerce Related Data Management Technologies

- **EAN.UCC Identification Numbers** - Data Management
- **EAN.UCC Universal Bar Codes** - Data Management
- **10303 Standard Exchange for Product Data (STEP)** - Data Management

Network Management Technologies

- **Remote Network Monitor (RMON)** - Network Management,
- **OSI Network Management Model** - Network Management,
- **Telecommunications Management Network (TMN) – M series** - Network Management,
- **Transaction Language 1 (TL1)** - Network Management,

Web-based Network Management

- **Policy-based Management Technologies** - Network Management,

Alternative Best Practices

Security Frameworks and Policy Documents

- **ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework** - Security,

ISO/IEC Documents on Security Technologies

- **ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics** - Security,
- **ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols** - Security,
- **ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V** - Security,
- **ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange** - Security,
- **ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages** - Security,
- **ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers** - Security,
- **ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)** - Security,
- **ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands** - Security,
- **ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes** - Security,
- **ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards** - Security,
- **ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods** - Security,
- **ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application** - Security,
- **ISO/IEC 9594-8:1998 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework** - Security,

- **ISO 9735-5:2002 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rul** - Security,
- **ISO/IEC 10164-9:1995 Information technology -- Open Systems Interconnection -- Systems Management: Objects and attributes for access control** - Security,
- **ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework** - Security,
- **ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework** - Security,
- **ISO 10202-1:1991 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 1: Card life cycle** - Security,
- **ISO 10202-7:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management** - Security,
- **ISO 10202-8:1998 Financial transaction cards -- Security architecture of financial transaction systems** - Security,
- **ISO JTC1 SC37 1.37.19784.1 BioAPI - Biometric Application Programming Interface** - Security,
- **ISO JTC1 SC37 1.37.19794 - Biometric Data Interchange Format** - Security,
- **ISO JTC1 SC37 1.37.19794.3 Biometric Data Interchange Format - Part 3: Finger Pattern Spectral Data** - Security,
- **ISO JTC1 SC37 1.37.19794.4 Biometric Data Interchange Format - Part 4: Finger Image Data** - Security,
- **ISO JTC1 SC37 1.37.1974.5 Biometric Data Interchange Format - Part 5: Face Image Data** - Security,

Federal Documents on Security Technologies

- **IECSA_VolumeIV_AppendixD.pdf**- Security,
- **FIPS 197 Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES)** - Security,

IETF Internet Requests for Comments (RFCs) on Security Technologies

- **RFC 1004 Distributed-protocol authentication scheme** - Security,
- **RFC 1352 SNMP Security Protocols** - Network Management,
- **RFC 1507 DASS - Distributed Authentication Security Service** - Security,
- **RFC 1579 Firewall-Friendly FTP** - Security,
- **RFC 1826 IP Authentication Header** - Security,
- **RFC 1827 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1)** - Network Management,
- **RFC 1968 The PPP Encryption Control Protocol (ECP)** - Security,

- **RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms** - Security,
- **RFC 2045 Multi-Purpose Internet Mail Extensions (MIME) and Secure/MIME** - Security,
- **RFC 2086 IMAP4 ACL extension** - Security,
- **RFC 2093 Group Key Management Protocol (GKMP) Specification** - Security,
- **RFC 2228 FTP Security Extensions** - Security,
- **RFC 2230 Key Exchange Delegation Record for the DNS** - Security,
- **RFC 2244 ACAP -- Application Configuration Access Protocol** - Security,
- **RFC 2246 The TLS Protocol Version 1.0** - Security,
- **RFC 2313 PKCS #1: RSA Encryption Version 1.5** - Security,
- **RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5** - Security,
- **RFC 2356 Sun's SKIP Firewall Traversal for Mobile IP** - Security,
- **RFC 2406 IP Encapsulating Security Payload (ESP)** - Security,
- **RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0** - Security,
- **RFC 2440 OpenPGP Message Format** - Security,
- **RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)** - Security,
- **RFC 2409 The Internet Key Exchange (IKE)** - Security,
- **RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile** - Security,
- **RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols** - Security,
- **RFC 2511 Internet X.509 Certificate Request Message Format** - Security,
- **RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,
- **RFC 2547 BGP/MPLS VPNs** - Security, Network Management,
- **RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP** - Security,
- **RFC 2764 A Framework for IP Based Virtual Private Networks** - Security, Network Management,
- **RFC 2753 A Framework for Policy-based Admission Control** - Security,
- **RFC 2817 Upgrades to TLS within HTTP/1.1** - Security,
- **RFC 2818 HTTP over TLS (HTTPS)** - Security,
- **RFC 2865 Remote Authentication Dial In User Service (RADIUS)** - Security,
- **RFC 2869 RADIUS Extensions** - Security,
- **RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering** - Security,
- **RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms** - Security,
- **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** - Security,
- **RFC 2946 Telnet Data Encryption Option** - Security,
- **RFC 2977 Mobile IP Authentication, Authorization, and Accounting Requirements** - Security,

- **RFC 2979 Behavior of and Requirements for Internet Firewalls** - Security,
- **RFC 2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0** - Security,
- **RFC 3053 IPv6 Tunnel Broker** - Network Management,
- **RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)** - Security,
- **RFC 3280 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** - Security,
- **RFC 3369 Cryptographic Message Syntax (CMS)** - Security,
- **RFC 3370 Cryptographic Message Syntax (CMS) Algorithms** - Security,
- **RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)** - Network Management,
- **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** - Security,
- **RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** - Security,

Other Security Technologies

- **IEEE 802.11b Web Encryption Protocol** - Security,
- **IEEE 802.11i Security for Wireless Networks** - Security,
- **RSA Documents on Security Technologies** - Security,
- **RSA PKCS #8 Private-Key Information Syntax Standard** - Security,
- **RSA PKCS #12 Personal Information Exchange Syntax Standard, version 1.0.** - Security,
- **OASIS Documents on Security Technologies** - Security,
- **AGA-12 Cryptographic Protection of SCADA Communications General Recommendations.** - Security,
- **ANSI INCITS 359-2004 Role Based Access Control (RBAC)** - Security,
- **EPRI 1002596 ICCP TASE.2 Security Enhancements** - Security,
- **NIST GSC-IS The NIST Interagency Report 6887 - 2003 edition (Government Smart Card-Interoperability Specification) Version 2.1** - Security,
- **NISTIR 6529 Common** - Security,
- **Smart Card Alliance Smart Card Primer** - Security,
- **Smart Card Alliance Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology** - Security,
- **Smart Card Alliance Government Smart Card Handbook** - Security,
- **WebDAV Access Control Extensions to WebDAV** - Security,
- **WPA WI-FI Protected Access** - Security,
- **WPA2 WI-FI Protected Access Version 2** - Security,
- **TMN PKI - Digital certificates and certificate revocation lists profiles** - Security,

Possible Technologies

Networking Technologies

- **Intermediate System to Intermediate System (ISIS) Routing Protocol** - Configuration,
- **Routing Information Protocol (RIP)** - Configuration,

Application Layer Protocols

- **CSV files** - Data Management