

Inter-Control Center Communications Protocol (ICCP, TASE.2): Threats to Data Security and Potential Solutions

Technical Report

Inter-Control Center Communications Protocol (ICCP, TASE.2): Threats to Data Security and Potential Solutions

1001977

Final Report, October 2001

EPRI Project Manager
D. Becker

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.

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

Hoffman Publications, Inc.

SISCO, Inc.

ORDERING INFORMATION

Requests for copies of this report should be directed to EPRI Customer Fulfillment, 1355 Willow Way, Suite 278, Concord, CA 94520, (800) 313-3774, press 2.

Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc. EPRI. ELECTRIFY THE WORLD is a service mark of the Electric Power Research Institute, Inc.

Copyright © 2001 Electric Power Research Institute, Inc. All rights reserved.

CITATIONS

This report was prepared by

Hoffman Publications, Inc.
16360 Monterey Road
Suite 230
Morgan Hill, CA 95037-5455

Principal Investigator
S. Hoffman

SISCO, Inc.
6605 19 ½ Mile Road
Sterling Heights, MI 48314

Principal Investigator
H. Falk

This report describes research sponsored by EPRI.

The report is a corporate document that should be cited in the literature in the following manner:

Inter-Control Center Communications Protocol (ICCP, TASE.2): Threats to Data Security and Potential Solutions, EPRI, Palo Alto, CA: 2001. 1001977.

REPORT SUMMARY

The ever widening use of the Inter-Control Center Communications Protocol (ICCP) protocol to exchange data between entities in the energy industry, coupled with the confidential, sensitive nature of much of this data, is giving rise to data security concerns related to ICCP use. This report examines how the ICCP protocol addresses data security and summarizes data security threats and recommended preliminary solutions.

Background

EPRI first introduced the ICCP (also known as TASE.2) to help standardize communications between control centers. ICCP applications now also include communication between control centers and power plants and substations and between nodes of NERC's Inter-regional Security Network (ISN). At last count, over 200 installations of ICCP were completed in the U.S. and in many other countries at transmission companies, energy companies, and grid operators. The International Electrotechnical Commission (IEC) and the International Standards Organization (ISO) have adopted ICCP in the form of three international standards. ICCP uses a well-proven, robust, existing standard called the Manufacturing Message Specification (MMS) for the messaging service. With deregulation – and the resultant increased competition – the security of operational data exchanged using ICCP between control centers and other locations becomes increasingly important.

Objective

To provide energy companies, regional transmission organizations (RTOs), and other stakeholders information on the current state of data security related to ICCP use

Approach

The project team gathered information from existing EPRI reports and other documentation, conducted interviews with experts in networking and data security, and synthesized information that was relevant to ICCP data security. They prepared the report for a diverse audience—technical and non-technical middle-level managers at domestic and international energy companies, RTOs, equipment and system vendors in the energy industry, and other stakeholders. Industry experts then reviewed the report for completeness and accuracy.

Results

This report reviews issues associated with secure communications between energy control centers and specifically addresses the role of ICCP. The report provides an introduction to ICCP and its applications, identifies data security threats in ICCP, covers the limited data security features within ICCP, and discusses preliminary data security solutions that experts have proposed.

ICCP provides access control via bilateral tables maintained on an ICCP server. This is the only data security service provided within ICCP; and, to date, no additional data security services within ICCP have been proposed. The documents synthesized to prepare this report did not identify specific additions of data security measures to be implemented within ICCP. The ICCP protocol designers assumed that additional data security measures would be implemented in various layers of the open systems interconnection (OSI) 7-layer stack. Hence, this report discusses data security that ICCP provides via bilateral tables, briefly covers physical security, and provides an overview of preliminary data security solutions relevant to ICCP that experts have proposed for implementation in various layers of the OSI 7-layer stack. These preliminary solutions are organized according to the five types of data security services defined by the OSI model—authentication, access control, data confidentiality, data integrity, and nonrepudiation.

The report also describes a proposed system, currently in review, that defines a new Application Service Element (ASE) called Security Transformations Application Service Element for MMS (STASE-MMS). Residing between MMS and the presentation layer in the OSI protocol stack, the proposed system supports data security services for MMS protocol data units and MMS objects. Proposers point out that this system can, in turn, secure data being communicated using the ICCP protocol.

EPRI Perspective

EPRI has been instrumental in the development and adoption of ICCP worldwide. As use of ICCP expands to a wider range of applications, EPRI continues to address issues of interest to ICCP users. As a result of industry restructuring, trends that include increasing demands on the existing power system, the increasing amount of confidential information exchange, and the growing number of players exchanging this information are giving rise to concerns over data security when ICCP is used. This report is the beginning of a process in which EPRI is examining data security issues relevant to ICCP and recommending security-related enhancements. To continue this process, EPRI plans to publish a second report with specific data security recommendations for ICCP in 2002.

Keywords

Control center
Data security
Information security
Inter-Control Center Communications Protocol (ICCP)
Telecontrol Application Service Element (TASE.2)
Utility Communications Architecture (UCA™)

ABSTRACT

In the mid 1990s, EPRI's Grid Operations and Planning Area brought together key members of the electric industry to design a proposed standard for the interchange of control center data. At that time the industry had no standards for data exchange and sharing of data was very limited due to complexity/customization issues between utilities. EPRI first introduced the Inter-Control Center Communications Protocol (ICCP, also known as the International Standard or TASE.2) to help standardize communications between control centers. ICCP applications now also include communication between control centers and power plants and substations and between nodes of NERC's Inter-regional Security Network (ISN). Now an accepted international standard, ICCP uses a well-proven, robust, existing standard called the Manufacturing Message Specification (MMS) for the messaging service. As a result of industry restructuring, trends that include increasing demands on the existing power system, the increasing amount of confidential information exchange, and the ever widening number of players exchanging this information are giving rise to concerns over data security when ICCP is used. A synthesis of information from a variety of reports and papers, this report provides an introduction to ICCP and its applications, identifies data security threats in ICCP, describes the limited data security measures implemented within ICCP, and discusses potential data security solutions relevant to ICCP that experts have proposed for implementation in various layers of the OSI 7-layer stack. The report also describes a proposed system, currently in review, that defines a new Application Service Element (ASE) called Security Transformations Application Service Element for MMS (STASE-MMS). To continue the process of examining data security issues relevant to ICCP and recommending data-related enhancements, EPRI plans to publish a second report with specific data security recommendations for ICCP in 2002.

ACKNOWLEDGMENTS

EPRI and the report author wish to thank the following individuals for their time and aid in providing information and reviewing this report:

David Becker, EPRI, has been responsible for the development of the control center data exchange Standardization effort within the USA electric industry. In response to the request from the International Standards Group, International Electro technical Commission (IEC), a USA task force comprised of control center data exchange experts was brought together and ultimately developed a draft of a proposed standard called ICCP. This proposal was submitted to the Working Group 7 of the IEC and ultimately approved within the IEC and is known by the formal name of TASE.2 and published as IEC 870-6-503. This USA design was the initial Standard produced as part of the overall EPRI led Utility Communications Architecture (UCA) .

William Blair, EPRI, has been responsible for development of the Utility Communications Architecture (UCA™) since 1991. In addition to leading the effort to establish the UCA™ Users Group and the UCA™ Test Facility, Dr. Blair is presently directly responsible for the Initiative for Substation Automation and EPRI support for the development of IEC International Standards for UCA™. Dr. Blair supported other EPRI managers in various areas of UCA™ development, including Dave Becker (ICCP), Joe Hughes (distribution automation), Frank Goodman (distributed resources), and Joe Weiss (cyber security).

Herb Falk, SISCO, Inc., has been involved in numerous projects involving the application of information systems technology and real-time communications technology to automated manufacturing, electrical distribution and automation, and power quality monitoring. Mr. Falk is a recognized expert on UCA™, ICCP, and MMS, serving on and chairing numerous industry technical committees. Mr. Falk has been appointed the convenor of the IEC TC 57 Working Group 15 (WG15), the scope of which is “data and communication security in the field of IEC/TC 57.”

Terry Saxton, Xtensible Solutions, is the current editor for the ICCP standards documents and is the Chief USA delegate to Working Group 7 of IEC TC 57, which is responsible for the development and publication of the ICCP standards. Mr. Saxton is a recognized expert on ICCP, has delivered numerous courses and presentations on ICCP, and has provided consulting services to energy companies and vendors to assist in its deployment.

David Becker, EPRI

In addition to their contributions to this report, these individuals authored or managed reports on ICCP and related topics, which served as source material for this synthesis report (see bibliography in section 5).

CONTENTS

1 ICCP PRIMER	1-1
Introduction	1-1
Evolution of ICCP	1-1
ICCP Today.....	1-3
ICCP and the Utility Communications Architecture (UCA™)	1-4
Data Exchange Using ICCP	1-5
ICCP Applications	1-5
Sample ICCP Application for Internal Communication.....	1-8
Need at GPU	1-11
The ICCP Solution at GPU	1-11
Results of ICCP Project at GPU	1-13
Related Standards-Based Efforts.....	1-13
2 THREAT/VULNERABILITY IDENTIFICATION IN ICCP.....	2-1
Summary	2-1
Introduction	2-1
Motivation for Attacks.....	2-2
Financial Rewards	2-2
Disgruntled Employee	2-4
Cause Motivation.....	2-4
Demonstration of Capability	2-4
Threat Types	2-4
Bypassing Controls.....	2-4
Integrity Violation	2-5
Authorization Violation.....	2-5
Indiscretion by Personnel	2-5
Illegitimate Use and Information Leakage	2-6
Example of ICCP Data Security Concerns: NERC ISN.....	2-6

3 PRELIMINARY SOLUTIONS	3-1
Data Security in ICCP	3-1
Physical Security	3-2
Authentication	3-2
Access Control	3-3
Data Confidentiality	3-4
Data Integrity	3-4
4 SECURING ICCP USING STASE-MMS.....	4-1
Securing MMS.....	4-1
Supported Security Transformations.....	4-2
Default Data Security Algorithms and Mechanisms	4-3
Data Security Information Exchange.....	4-3
STASE-MMS Model	4-3
5 BIBLIOGRAPHY	5-1
A ACRONYMS	A-1

LIST OF FIGURES

- Figure 1-1 Schematic of Data Exchange. ICCP provides real-time data exchange between energy companies using a client-server model. Either the client or server energy company may initiate a connection. Interactions between a client and server consist of requests for information as well as the issuance of control directives. Field devices in the domain of control center 1 may be included in the domain of control center 2 to create an inter-domain control area. This means that ICCP enables extension of monitoring and control from a local, or intra-SCADA (Supervisory Control and Data Acquisition System) environment to an inter-SCADA environment. Source: "IEC 1999" in bibliography 1-4
- Figure 1-2 GPU's Portland Station ICCP Network. ICCP was integrated in the corporate LAN/WAN station communications and ICCP nodes were established between the corporate EMS and four functional units. This configuration is similar for the two other GPU stations. Source: "EPRI 1999" in bibliography 1-12
- Figure 4-1 Location of STASE-MMS in the Open Systems Interconnection (OSI) Protocol Stack. Within the application layer, Security Transformations Application Service Element for MMS (STASE-MMS) resides below MMS, which operates below ICCP (TASE.2). 4-1
- Figure 4-2 Mandatory Application Service Elements When STASE-MMS Is Used. The ASEs available to an application process require communication over an application association. The application processing the services provided by the Association Control Service Element (ACSE) control the application association. Source: "SISCO 1998" in the bibliography 4-4

LIST OF TABLES

Table 1-1 ICCP Conformance Blocks	1-6
Table 1-2 Applications of ICCP in the United States and Europe.....	1-7
Table 1-3 ISN Data Exchange Requirements. ICCP is the primary real-time protocol for the ISN.	1-8
Table 1-4 Data Exchange Requirements Between Control Centers and Power Pools or ISOs/RTOs.....	1-10
Table 2-1 Control Center Data Security Comparison: Percent of Respondents Expressing Concern over Data Security	2-3

1

ICCP PRIMER

Introduction

Since its initial use in the mid 1990s, ICCP (TASE.2) has become the international standard form of communication between energy control centers, and between control centers and power plants and substations. It is also the primary protocol used on NERC's Inter-regional security network (ISN), is used for control center to ISO/RTO communications, and is being considered for even wider adoption.

ICCP is the most widely adopted communications protocol available to the electric power industry today, with over 200 completed installations in the United States, and in many other countries, at transmission companies, energy companies, and grid operators. A wide range of hardware and software vendors support ICCP, allowing energy companies to implement the protocol inexpensively.

Since ICCP is instrumental in helping energy control centers maintain a high level of power system security (i.e., reliability), discussing the data security aspects of ICCP can lead to some confusion. To avoid any misunderstanding, this report refers to either *power system security* or *data security*.

Evolution of ICCP

The electric power industry uses more operating data than perhaps any other industry. Seamless communication of this information to appropriate locations smoothes the process of generating, transmitting, and distributing electricity. To achieve this objective, over the years energy companies developed their own custom-designed communications protocols to facilitate exchange of these data from one location to another. Unfortunately, these protocols were often developed on an as-needed basis, leading to a proliferation of proprietary, incompatible protocols. Around 1980, most energy companies that possessed inter-control center communications capabilities used these proprietary, custom-developed protocols for point-to-point transmission.

In the years leading up to 1980 (before the days of independent system operators, ISOs, or regional transmission organizations, RTOs), North America witnessed an increase in cooperative enterprises such as power pools and regional centers. Industry participants needed the seamless exchange of data but found themselves hampered by the technical and economic limitations of the available protocols.

This led two groups of energy companies, first one in the western U.S. and then later one in the eastern U.S., to begin design of a common protocol they could all use. Their objective was to rid themselves of the costly difficulties of using proprietary protocols.

In the western U.S., members of the Western Systems Coordinating Council (WSCC) initiated efforts in the early 1980s to develop an inter-energy company data communications standard. This group succeeded in developing the initial version of what became known as the WSCC protocol. Later, in the mid 1980s, a group of energy companies in the eastern United States formed the Inter-Utility Data Exchange Consortium (IDEC) and developed the inter-utility data exchange protocol. Elcom 83 and Elcom 90 were used in Europe.

IEEE explains that “as the need for a unified standard became clear, the International Electrotechnical Commission (IEC) solicited member bodies for contributions to be considered for international standardization. The lack of a consensus standard in the U.S., as well as the perceived limitations of all of the existing candidate protocols, led to the formation of a utility/vendor task force sponsored by EPRI, WSCC, IDEC, and a number of utilities. This task force led development of the Intercontrol Center Communications Protocol (ICCP). The name was later changed to the Telecontrol Application Service Element 2 (TASE.2) to conform to IEC Technical Committee 57 Working Group 7 taxonomy.” These efforts culminated in the late 1990s when ICCP received official status as an international standard (see “IEEE 1999” in bibliography for more information).

While this effort to develop ICCP was proceeding, dramatic changes were taking place in the U.S. energy industry. The 1996 Federal Energy Regulatory Commission (FERC) passage of Orders 888 and 889 mandated “open access” to the U.S. transmission system. This and other legislative and regulatory changes presented major implications for energy company communications of data. The amount and types of data exchanged between energy companies, between energy companies and new entities, and within various parts of each energy company expanded dramatically. Secure wide area operation of the power system necessitated effective communication of data between energy control centers. And as ISOs began operation, communication between energy companies and these new entities became necessary. This need will only increase, as the FERC continues to move aggressively forward to mandate formation of a finite number of RTOs in the U.S.

Increasing demands on the power system have also fueled the need to effectively communicate data. As wholesale transactions of power increase in magnitude and frequency, securely operating a power system strained by these transactions becomes increasingly challenging. In light of these developments, efficient communication between involved parties to ensure secure power system operation becomes a necessity, rather than simply a beneficial capability.

The drive to maintain power system security amidst these changes has resulted in establishment of new types of systems and networks. For example, the Inter-regional Security Network (ISN) established by the North American Electric Reliability Council (NERC) provides coordinated power system security processes both regionally and in individual control areas. But such a system needed a way for the security coordinators and other participants to communicate needed data using standard protocols.

U.S. energy industry restructuring has also led to the deregulation of the power generation function in many parts of the country. The consequent buying and selling of generation assets has led to new entrants in the power business, new business models in the power generation industry, and other fundamental structural changes. This, in turn, has led to added complexity in communicating between energy control centers or ISOs/RTOs and these power plants.

But maintaining power system security is not the only motivation for a uniform communications protocol. In order to succeed in the deregulated power generation market, energy companies look to curtail operating costs by improving operating efficiency and reducing maintenance expenditures. Hence, communication of information must be accomplished cost effectively.

ICCP is meeting each of these needs for a standardized communication protocol, as well as other emerging applications.

ICCP Today

ICCP is a modern comprehensive client/server protocol (see Figure 1-1). Data exchange information consists of real-time and historical power system monitoring and control data, including measured values, scheduling data, energy accounting data, and operator messages. ICCP also defines a mechanism for exchanging time-critical data between locations.

The International Electrotechnical Commission (IEC) and the International Standards Organization (ISO) adopted ICCP in the form of the following international standards:

- TASE.2 Services and Protocol (IEC 60870-6-503)
- TASE.2 Object Models (IEC 60870-6-802)
- TASE.2 Application Profile (IEC 60870-6-702).

ICCP uses a well-proven, robust, existing standard called the Manufacturing Message Specification (MMS) for the messaging service. MMS (ISO/IEC-9506) was designed to facilitate the exchange of real-time application data among manufacturing and process control systems and is broad enough in scope to address the needs of many industry sectors.

MMS is an object-oriented program, allowing organization of a complex system into a collection of easily understood, discrete objects that incorporate both information and behavior. This means that MMS is relatively easy to implement and maintain. ICCP uses MMS objects to define messages and data structures, and all ICCP operations run from these objects. Supported data types include control messages, status, analogs, quality codes, schedules, text and simple files. In addition to data exchange, optional functions include remote control, operator station output, events, and remote program execution. Using MMS as a foundation enables use of widely available telecommunications technologies, such as frame relays and ISDN lines.

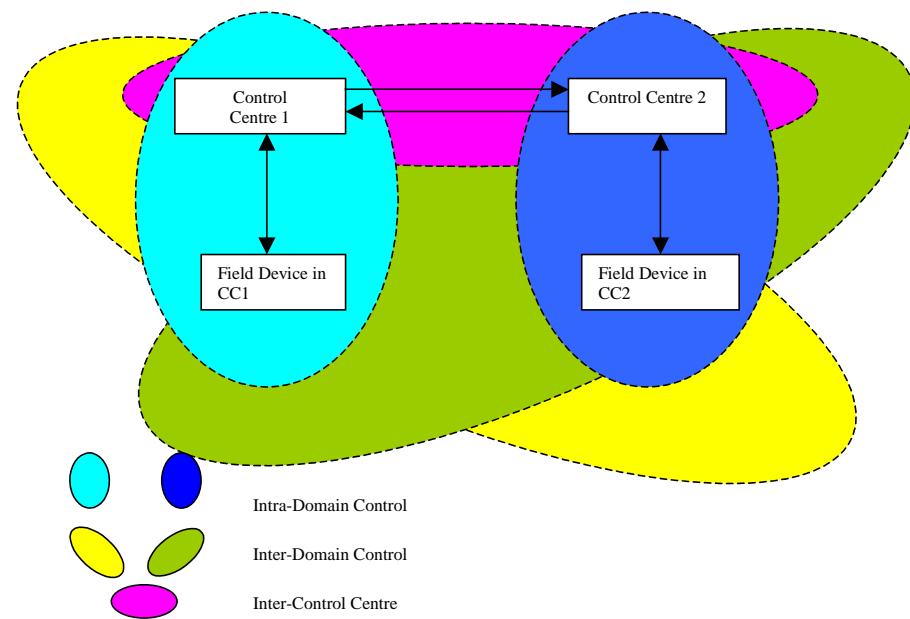


Figure 1-1

Schematic of Data Exchange. ICCP provides real-time data exchange between energy companies using a client-server model. Either the client or server energy company may initiate a connection. Interactions between a client and server consist of requests for information as well as the issuance of control directives. Field devices in the domain of control center 1 may be included in the domain of control center 2 to create an inter-domain control area. This means that ICCP enables extension of monitoring and control from a local, or intra-SCADA (Supervisory Control and Data Acquisition System) environment to an inter-SCADA environment. Source: "IEC 1999" in bibliography

ICCP and the Utility Communications Architecture (UCATM)

ICCP is part of the Utility Communications Architecture (UCATM). IEEE defines UCA as a “standards-based approach to utility communications that provides for wide-scale integration at reduced costs and solves many of the most pressing communication problems for today’s utilities. The UCA is designed to apply across all of the functional areas within the electric, gas, and water utilities. These functional areas include customer interface, distribution, transmission, power plant, and control centers” (see “IEEE 1999” in bibliography for more information).

As IEEE explains, the role that ICCP plays is best understood by examining the two main types of applications that involve exchange of real-time data acquisition and control information in the energy industry:

1. Access to real-time databases (e.g., supervisory control and data acquisition, or SCADA, systems, and energy management systems, or EMS)
2. Access to real-time devices (e.g., remote terminal units, switchgear, and meters)

UCA supports access to real-time databases through ICCP (see “IEEE 1999” in bibliography for more information).

The three IEEE standards for TASE.2 (IEC 60870-6-503, IEC 60870-6-802, and IEC 60870-6-702) are published independently of the rest of UCA, but are included by reference in UCA Version 2.0.

Data Exchange Using ICCP

Data types that can be exchanged between two or more ICCP nodes include the following (see Table 1-1 for a complete list):

- Real-time process analog and discrete control and data acquisition signals used by the existing remote terminal units (RTUs) and new substation automation computers
- Historical data such as average values of accumulations over time
- Predefined reports
- Unit forecast schedule data
- Unit commitment data
- Simultaneous updating of generation report requirements through utilization of a common distributed database.

ICCP Applications

ICCP capabilities range from linking wide-area interconnected power systems to facilitating internal communications. Table 1-2 provides a list of types of ICCP communication applications, along with other protocols used in each application. The types of data links (e.g., dedicated point-to-point and frame relay WAN with routers) are discussed in the context of data security in Chapter 2.

Linking individual control centers with regional coordinators, ICCP enables real-time exchange of system data, such as MW, MVAR, kV, and breaker status, allowing instant assessment of the interconnected networks. For example, the Southwest Power Pool (SPP) collects data via two ICCP systems. As transmission security coordinator, SPP collects operational data from 17 control areas via an ICCP-compliant communications system. Data, collected within 30 seconds, are used to perform state estimation and power flow modeling.

SPP also collects operational data from neighboring control areas with the ICCP-compliant communications system in place on the NERC ISN. Capabilities include anticipating contingencies and taking both preventive measures prior to a disturbance and corrective measures in the event of a disturbance.

Table 1-1
ICCP Conformance Blocks

ICCP Conformance Block Name		Type of Services
Block 1	Periodic Power System Data	Periodic transfer of power system data, including field device status, analog values, and accumulator values with quality and time stamps
Block 2	Extended Data Set Monitoring	Non-periodic transfer of data, including detection of system changes or integrity check performance
Block 3	Block Transfer Data	Efficient transfer mechanism where bandwidth is at a premium
Block 4	Information Messages	General message transfer mechanism, including capabilities to transfer simple text or binary files
Block 5	Device Control	Mechanism for transferring a request to operate a device from one node to another
Block 6	Program Control	Mechanism for ICCP client to conduct program control at a server site
Block 7	Event Reporting	Extended reporting of system events at remote sites
Block 8	Additional User Objects	Mechanism for transferring scheduling and accounting information, device outage information, and power plant information
Block 9	Time Series Data	Mechanism enabling transmission of time series data

Source: "EPRI 1998" in bibliography.

The latter example illustrates the pivotal role ICCP plays as the only protocol used to exchange real-time data between ISN nodes. The ISN is comprised of 18 security coordinator systems interconnected via ICCP operating over a frame relay network. Each security coordinator is in turn connected to one or more control areas to obtain the electric system security data needed for the security coordinators to perform operational power system security assessments and coordinate reliable operations. This latter connection has no specific protocol requirements placed on it. Each security coordinator is free to choose the protocols most appropriate for their control area.

Now functional with links to all ten U.S. NERC regions, the ISN is designed to provide coordinated power system security processes both regionally and within individual control areas. Central to the success of the ISN is the use of ICCP as the communications highway.

Table 1-2
Applications of ICCP in the United States and Europe

ICCP Application	Dedicated Point-to-Point	Frame Relay WAN with Routers	Internet
Control Center to Control Center (different entities)	ICCP, WSCC	ICCP, WSCC	
Control Center to Control Center (same entity)	Proprietary, ICCP	Proprietary, ICCP	
Control Center to Transmission Substation	ICCP, DNP, Proprietary, RTU, CASM		
Control Center to Power Plant	Proprietary, RTU, ICCP		
Control Center to Power Pool or ISO/RTO	ICCP, WSCC, Proprietary, FTP, Telnet, TCP/IP, SQL	ICCP, Proprietary, FTP, Telnet, TCP/IP, SQL	
ISN data exchange (node to node)		ICCP	
ISN off-line file transfer of configuration data		ICCP, FTP	FTP

Source: modified from Table 4-1 in “EPRI 2000a” in bibliography.

Data exchange can take place between the following entities:

- Security coordinator to other security coordinators
- Control area to security coordinator
- Control area to other control areas via a common security coordinator or over the ISN if attached to different security coordinators.

The electric system security data to be exchanged over these links is described in Table 1-3. The data with specific elements identified on the right side of the table is updated and sent every ten minutes. The remainder of the data is updated whenever it changes and is available.

ISOs/RTOs present another important application of ICCP. In this case, energy companies are able to directly communicate with the ISO/RTO control center(s) using a standardized protocol. Table 1-4 identifies typical exchange requirements between a control center and a power pool or

ISO/RTO. The use of ICCP for most transactions, now common for data links to a power pool or ISO/RTO from control centers, is assumed.

Table 1-3

ISN Data Exchange Requirements. ICCP is the primary real-time protocol for the ISN.

Type of Data	Examples
Transmission Data	<ul style="list-style-type: none">• Status• MW or ampere loadings• MVA capability• Transformer tap and phase angle settings• Key voltages
Generator data	<ul style="list-style-type: none">• Status• MW and MVAR capability• MW and MVAR net output• Status of automatic voltage control facilities
Operating Reserve	<ul style="list-style-type: none">• MW reserve available within ten minutes
Control Area Demand	<ul style="list-style-type: none">• Instantaneous
Interchange	<ul style="list-style-type: none">• Instantaneous actual interchange with each control area• Current interchange schedules with each control area by individual
Interchange Transactions	<ul style="list-style-type: none">• Interchange schedules for the next 24 hours
Control Area Error and Frequency	<ul style="list-style-type: none">• Instantaneous area control error• Clock hour area control error• System frequency at one or more locations in the control area

Source: "EPRI 2000a" in bibliography.

Sample ICCP Application for Internal Communication

Applications of ICCP for internal communications include communication between control centers that the same energy company operates. Neighboring control centers can communicate with each other easily, transmitting the entire range of real-time and historical power system monitoring and control data.

Other internal communication needs that ICCP facilitates include communication between a control center and transmission substations for purposes of substation control. For power plant control from control centers, ICCP enables direct digital communication between power plant control and central dispatch systems. Load-following commands are transmitted to selected

generators via the Supervisory Control and Data Acquisition System (**SCADA**) network. In this application, ICCP also provides for additional communications comprising outage scheduling, reporting of availability and real-time status reporting of emissions data, and forecasting.

By deploying ICCP for communication between control centers and power plants, power producers benefit from improved accuracy, speed, and flexible response for load demands and transmission grid stability. The enabling technology enables power producers to be more agile and responsive when business success requires quick and accurate management decisions. A project at GPU illustrates the value of ICCP in this type of application.

Table 1-4
Data Exchange Requirements Between Control Centers and Power Pools or ISOs/RTOs

Application	Data/Comments
Basic SCADA applications for data acquisition, such as limit processing, to process data received via data links same as telemetered from RTU	ICCP Block 1,2 energy management system (EMS): analogs (engineering units) status, accumulators; status data
Network status processor, drive map board	ICCP Block 1,2 to EMS: status of lines, SS buses, generation, condensers, loads, capacitors, circuit breakers, switches, tap changers – down to 69 kV
Energy dispatch	ICCP Block 8 to Participants: log time, unit ID, block # (up to 7 blocks), MW, price, required action, operational flag, comments
Regulation	ICCP Block 1,2 to Participants: MW reading to security coordinator (SC), ACE (float) to participant
Reserve	ICCP Block 8 to Participants
Real-time power system security – state estimator, penalty factor calculations	ICCP Block 1,2 to SC: ICCP Block 8 to participants
System alerts	ICCP Block 4 to Participants: text alarms and messages; emergency procedure information; and power system restoration summary
System controller console messages	ICCP Block 4 bi-directional
Load forecasting	ICCP Block 8 to EMS: load forecasts of participants (aggregate loads); ICCP Block 1,2 or external link to EMS; weather data
Notification of electronic tags	ICCP Block 5 to SC
Regulation dispatch setpoints, device control	ICCP Block 5,7 to Participants
Generation event tracking information	ICCP Block 8 to EMS (transaction): generation outage report with reason and impact on capacity
Transmission outage scheduling information	ICCP Block 8 to EMS (transaction): device name and requested start/stop time of outage
Interchange scheduling data	ICCP Block 8 to EMS (transaction): data for establishing two-party interchange contracts, including start/stop time, name of parties, path name, MW values
Generation scheduling data	ICCP Block 8 to EMS (transaction): generating unit or schedule name, and data values for associated parameters
Generation dispatch data	ICCP Block 8 to EMS: participants choice of previously-approved generation schedule, including limits
Power system restoration status	ICCP Block 8 to Participants
Accounting data report	ICCP Block 8 bi-directional: hourly accounting data from participants is compiled and balanced, and a summary report returned
Line/transformer limits	ICCP Block 8 to EMS: normal, load dump, short term, and long term limit values
AGC regulation capacity report	ICCP Block 8 to Participants: amount of regulation by type assigned to each generating unit
Contingency status report	ICCP Block 8 to Participants: list of primary lines impacted by a contingency and the affect on flow
Lines out of service report	ICCP Block 8 to Participants: name of line and voltage level for each critical line out of service
Transmission overload report	ICCP Block 8 to Participants: actual, trend, and contingency overloads
Load Summary	ICCP Block 8 to Participants: summary of current loads

Source: ‘EPRI 2000a’ in bibliography.

Need at GPU

As documented in “EPRI 1999” in the bibliography, the GPU Demonstration Project deployed ICCP for connecting power plant control systems to the organization’s energy management system. The organization lacked a standard communications link between the generating units DCS, the central dispatching systems energy management control system, the corporate client server environment, and the legacy corporate mainframe. Each of these systems contained data generated by one or more of the other systems. Unit control and financial data were transmitted throughout the organization, often over public data paths. Access to this data by a competitor would jeopardize the company’s competitive edge, and data security was a critical issue.

The GPU energy management system (EMS) is located in a corporate facility separate from the electric generating stations. This project linked the EMS to three different plants with the following DCSs:

- Conemaugh Station with a Honeywell DCS
- Portland Station with a Westinghouse DCS
- Shawville Station with a Bailey DCS

The primary objective of the project was integrating the corporate power plant process data to the client server environment. A secondary objective was to demonstrate the ability to exchange data between different DCS systems over the WAN. Because of the geographic differences between the plan locations, as well as the heterogeneous DCS systems, a detailed risk analysis was required to validate that the LAN/WAN was secure.

The ICCP Solution at GPU

The system implemented was based on the hierarchical control functions performed in each of the modules. A spatial model was developed based on the objective tree of the project. The short-term objective focused on delivering an operational communications systems based on the long-term needs of the organization. This prototype system delivered capability for data exchange functionality between the various DCS and the EMS. This functional operation was selected to validate the life-cycle methodology and provide immediate benefit to the organization.

The initial phase of the project established the ICCP digital link between the EMS and DCS. The project team developed and established all necessary interfaces for exchanging the required data over the ICCP links, whether analog, discrete, or object format. This was followed by implementation of the selected applications to demonstrate viability of the enabling technology. Figure 1-2 illustrates implementation of the ICCP network at one of the GPU stations.

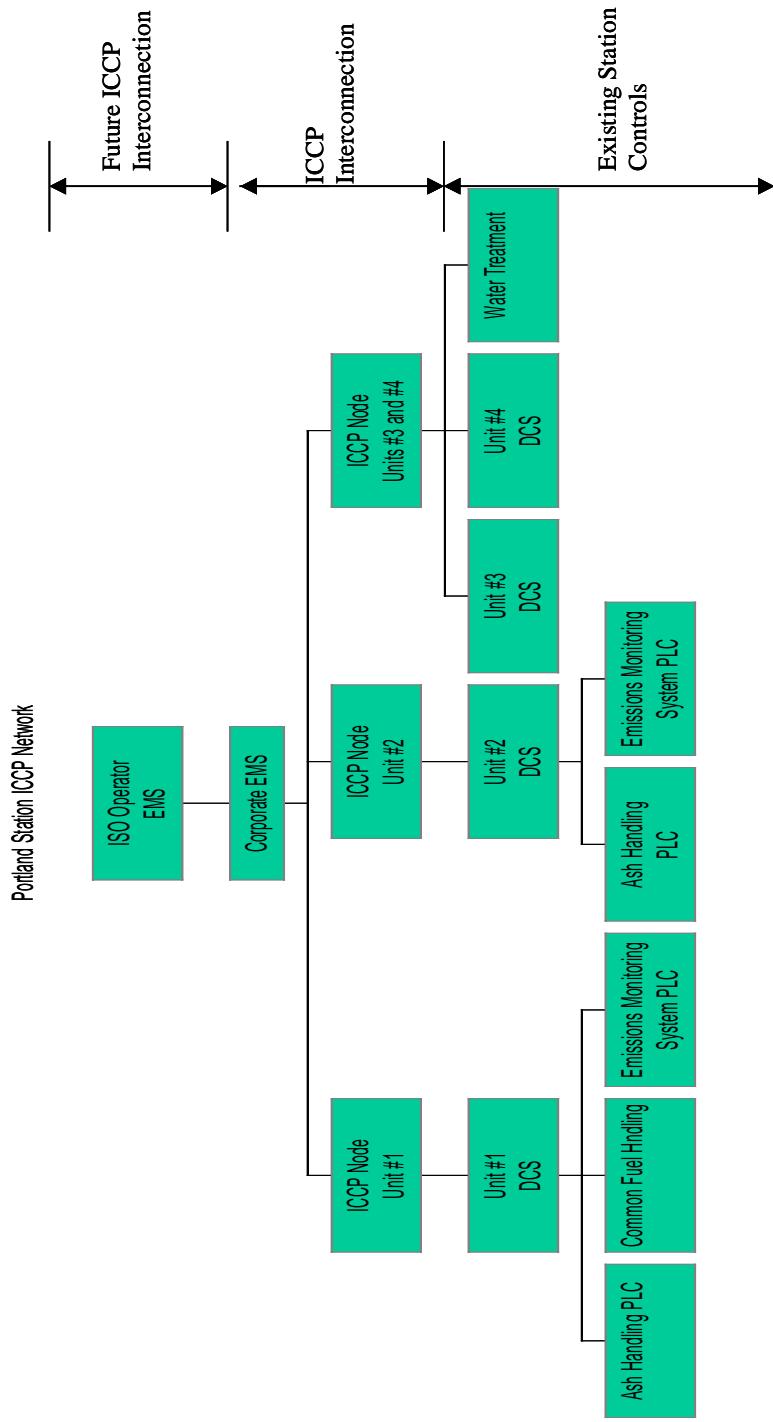


Figure 1-2
GPU's Portland Station ICCP Network. ICCP was integrated in the corporate LAN/WAN station communications and ICCP nodes were established between the corporate EMS and four functional units. This configuration is similar for the two other GPU stations. Source: "EPRI 1999" in bibliography

The team anticipated the following results from the study:

- Reduced dependence on verbal communication between the dispatching center and unit control rooms, resulting in an expected cost-saving of five man-hours per month during peak system coordination.
- Elimination of RTUs at the stations, reducing the station book value by approximately \$65,000 and associated O&M costs by 40 man-hours per year.
- Reduction in Lost Generation Report Accounting development time by two man-hours per month.
- Relief of 45 man-hours per month for the Group Shift supervisor due to automation of the Daily Status Report.

Results of ICCP Project at GPU

Both of the objectives for this project – integrating corporate power plant process data to the client server environment and exchanging data between two different DCS systems over the WAN – were met. The project demonstrated through the use of selected applications the ability to transmit/receive data and objects for information exchange and unit dispatch control between dissimilar systems. In addition, GPU found that integration through a standard protocol such as ICCP enabled greater efficiency and improved production while reducing costs.

The project team found the ICCP system easy to install. When configuring an ICCP connection, precise spelling (including case) is critical. Most of the problems encountered during installation were due to minor configuration errors. Databases on both the Honeywell PHD and Siemen's ICCPNT were easy to configure and maintain. The Honeywell receiver data interfaces (RDIs) were easily configured into the system and provided a good method of exacting data from the various DCS. The LAN connection could be either Ethernet or Token Ring. With NT-based PCs, Honeywell's PHD and RDIs, and Siemen's ICCPNT, the team found that they could transmit data to almost any system with minimal effort.

Related Standards-Based Efforts

ICCP is not the only state-of-the-art, standards-based control center tool. While ICCP serves as the standard for communication of data, two sets of standards-based approaches EPRI also helped initiate--the Control Center Application Program Interface (CCAPI) and Common Information Model (CIM)--provide a standard interface and standard model format for exchange of data between control centers.

The CCAPI is essentially a standardized interface that enables users to integrate applications from various sources by specifying the data that applications will share and how they will share it. The heart of the CCAPI, the CIM defines the essential structure of a power system model in order to provide a common language for information sharing among applications. This common language reduces the number of needed software translators between applications. Furthermore, as vendors develop new applications, developing internal and external data structures in

The team anticipated the following results from the study:

- Reduced dependence on verbal communication between the dispatching center and unit control rooms, resulting in an expected cost-saving of five man-hours per month during peak system coordination.
- Elimination of RTUs at the stations, reducing the station book value by approximately \$65,000 and associated O&M costs by 40 man-hours per year.
- Reduction in Lost Generation Report Accounting development time by two man-hours per month.
- Relief of 45 man-hours per month for the Group Shift supervisor due to automation of the Daily Status Report.

Results of ICCP Project at GPU

Both of the objectives for this project –integrating corporate power plant process data to the client server environment and exchanging data between two different DCS systems over the WAN –were met. The project demonstrated through the use of selected applications the ability to transmit/receive data and objects for information exchange and unit dispatch control between dissimilar systems. In addition, GPU found that integration through a standard protocol such as ICCP enabled greater efficiency and improved production while reducing costs.

The project team found the ICCP system easy to install. When configuring an ICCP connection, precise spelling (including case) is critical. Most of the problems encountered during installation were due to minor configuration errors. Databases on both the Honeywell PHD and Siemen's ICCPNT were easy to configure and maintain. The Honeywell receiver data interfaces (RDIs) were easily configured into the system and provided a good method of exacting data from the various DCS. The LAN connection could be either Ethernet or Token Ring. With NT-based PCs, Honeywell's PHD and RDIs, and Siemen's ICCPNT, the team found that they could transmit data to almost any system with minimal effort.

Related Standards-Based Efforts

ICCP is not the only state-of-the-art, standards-based control center tool. While ICCP serves as the standard for communication of data, two sets of standards-based approaches EPRI also helped initiate--the Control Center Application Program Interface (CCAPI) and Common Information Model (CIM)--provide a standard interface and standard model format for exchange of data between control centers.

The CCAPI is essentially a standardized interface that enables users to integrate applications from various sources by specifying the data that applications will share and how they will share it. The heart of the CCAPI, the CIM defines the essential structure of a power system model in order to provide a common language for information sharing among applications. This common language reduces the number of needed software translators between applications. Furthermore, as vendors develop new applications, developing internal and external data structures in conformance with the CIM eliminates the need for software translators altogether (see ‘EPRI 2000b”in bibliography for more information).

2

THREAT/VULNERABILITY IDENTIFICATION IN ICCP

Summary

The major threats to control center data security are bypassing controls, integrity violation, authorization violation, indiscretion by personnel, illegitimate use, and information leakage. Motivations for control center attacks include disgruntled current or previous employees (who initiate 80 percent of all data security attacks), financial rewards, “causes,” and the ability to demonstrate capability. NERC has identified malicious external hackers, disgruntled employees, unintentional employee errors, and “trusted” external users as the four general threats to the Inter-regional Security Network (ISN).

Introduction

Whenever a system is designed to exchange data among various entities, including the use of ICCP, the focus on data security issues is important. In the case of the GPU example of ICCP application at the end of chapter 1, project investigators conducted a risk analysis for the project. This analysis identified threats that relate to ICCP from the following categories:

- Intentional human intervention – the deliberate disruption of control of the data link. While the source of this type of intrusion is usually within the organization, knowledgeable outside hackers also fall into this category.
- Accidental human intervention – the accidental or procedural failure by which an individual is able to access the data link.
- Physical threats – a category that might cause faulty data or physical loss of equipment and services.
- Natural threats such as storms and fires.

Of the four threats the team identified, the first two relate to data security, and the third threat relates to physical security. Although little publicly available information exists on attacks on energy company communication systems, this does not rule out the possibility that such attacks are taking place. For example, many energy companies may not be aware that such attacks are occurring or may opt not to disclose these events—both of which are endemic in other industries.

As more data is transmitted outside the physical control center, the acquisition of such information by hackers, disgruntled employees, or terrorists increases in possibility. The likelihood of such threats leading to problems also increases as the financial motivation rises

(due to the ability to profit from power market information) and the ease of conducting attacks rises (due to technological advances and easy access online to hacking tools).

According to a recent EPRI survey (EPRI 2000a) of energy companies and vendors regarding current communication security practices, the main threats to control center data security are in the following areas (in order, most likely threats first, with percent of respondents listing the threat in parentheses):

- Bypassing controls (42 percent)
- Integrity violation -- interception and/or alteration (40 percent)
- Authorization violation (38 percent)
- Indiscretion by personnel (35 percent)
- Illegitimate use and information leakage (32 percent)

None of the perceived threats currently cause widespread concern among end-users, although concern about data security threats increases as the size of the energy company increases (according to peak load). Table 2-1 compares the percent of all respondents ("aggregate response") expressing concern about data security threats with the percent of respondents from large energy companies expressing this concern (data based on 160 respondents). For technologies currently in use that are relevant to ICCP, Table 2-1 also illustrates the type of data security risks that control centers face, according to the survey. As communication outside of the control center via the Internet and WAN connections increases, so do potential data security exposures.

The survey also found that hackers and disgruntled employees are the highest perceived intruder threats to the control center, while competitors and terrorists are of concern among fewer respondents. After summarizing the motivations for attacks on control centers, this chapter examines each of the individual data security threats and vulnerabilities that are relevant to ICCP.

Motivation for Attacks

Motivations for data security attacks on portions of energy companies' and other players' infrastructures that are relevant to ICCP range from financial gain to mayhem. The following motivations are discussed in order of importance.

Financial Rewards

In the deregulated energy industry, advance information on outages or lower than predicted available power would represent a financial advantage to the traders of wholesale power. Such advance information could allow traders to reap millions of dollars of revenue per transaction.

Table 2-1
Control Center Data Security Comparison:
Percent of Respondents Expressing Concern over Data Security

	Aggregate Response (percent)	Large Energy Companies (percent)	Conclusion
Equipment attached to modems			The aggregate responses reflect usage of older technology.
NT Servers	31	40	
UNIX Servers	27	35	
ASCII terminals	23	15	
Terminal servers	21	25	
Potential exposure due to non-secure connected devices	50	44	Although the technology used is different, the amount of exposure is similar between the aggregate responses and the larger utilities.
WAN connections in use	33	73	
WAN support for TCP/IP	51	57	Larger utilities will be more exposed to Internet security threats.
Firewall protecting WAN (of those utilities responding with WAN connectivity)	48	40	Aggregate response represents best case scenario.
Person assigned to manage firewall	80	35	
Exposure due to firewall issues	62	65	

Source: modified from Table 2-1 in “EPRI 2000a” in bibliography

However, the financial rewards of eavesdropping are directly related to the timeliness of the information. “Fresher” information yields higher potential financial rewards. Therefore, the part of the appropriate data security objective to combat this threat is to protect the information during the time period over which the information has value. For example, the fact that surplus generation is available for the next hour should be protected for a relatively short period of time – about five minutes. Disclosure into the appropriate channels would occur rapidly in order for the surplus power to be sold, and data security is required only until the information is disclosed

properly. This approach is valuable because limited protection of information is much easier to address than perpetual protection.

As with capital equipment, the value of information typically decreases with time. While an expired login password has no value, a one-year generation schedule may represent significant value. Therefore, control centers managers should determine the time period during which each data type has value.

Disgruntled Employee

Current or previous employees initiate 80 percent of all data security attacks. Abuse by current employees with appropriate access to information is difficult to prevent. However, effective corporate security policies include provisions for restricting access by previous employees. Because assigning a general username/password alone for employee remote login requires that the username/password be changed whenever an employee departs, administrators are increasingly assigning specific username/passwords or combining two authentication methods (e.g., a password and a token).

Cause Motivation

Religion, politics, and other closely held beliefs might motivate attacks on control centers. Depending upon the level of motivation, the “cause” could manifest itself in disruption, rendering of certain assets useless, or extensive damage and cost.

Demonstration of Capability

Individuals may cause disruption and damage as a way to demonstrate their capability and power.

Threat Types

Bypassing Controls

Recent FERC orders and industry restructuring have unwittingly created financial incentives for accessing operational cost data maintained in control center EMS systems. Hackers, disgruntled employees (or ex-employees) or competitors may bypass authentication and computer access control schemes for the purpose of obtaining confidential data for financial gain and/or modifying data to sabotage power system operations. In the case of ICCP, this involves bypassing the bilateral table form of access control built into ICCP (see Section 3). Hackers may also be able to gain access to data that use ICCP by accessing MMS directly.

Integrity Violation

An unauthorized user could send false information to the EMS by tapping into an ICCP network or SCADA network. The false data would appear as valid data sent from an RTU. This could cause a control center EMS operator to take incorrect actions (e.g., in response to a false out-of-limit measurement reading, or a false trip reading from a circuit breaker). Unless the operator took an inappropriate action, no harm would occur to the power system.

Similarly, an unauthorized user could tap into an ICCP or SCADA network and send false information to a substation or power plant. In the case of a substation, this could cause breakers or switches to open or close, causing local outages, or even wide area blackouts in critical transmission substations. In the case of a power plant, consequences could include improperly changing a set point on a generator.

For an integrity violation to occur, the data would need to be modified at one of the following locations:

- The EMS/SCADA database and/or ICCP clients/servers in a control center
- SCADA master or substation computer in the substation
- The control system computer in the power plant.
- The data circuit between the control center and substation, power plant, or other control center.

Authorization Violation

Unauthorized users could obtain access to data and/or software. This threat could result from a trusted, external source who has gained certain access rights, but who has violated the access rights granted. Control centers that rely on physical security and authentication, and ICCP alone, which relies only on built-in bilateral table access control, are vulnerable.

Indiscretion by Personnel

The following types of inadvertent mistakes by employees can impact system operations and network reliability:

- Data entry error
- Inadvertent disclosure of confidential data (e.g., via improper disposal methods)
- Incorrect system command entry
- Changes to software source code

There is a high vulnerability to indiscretion at most control centers. Data entry errors and inadvertent disclosure by enabling garbage diving represent the most prevalent types of personnel indiscretion.

Illegitimate Use and Information Leakage

Illegitimate use and information leakage, which compromises the confidentiality of sensitive information, is a key threat for ISOs/RTOs. Cost, scheduling, and outage data transmitted between control centers are potential targets for illegitimate use.

Example of ICCP Data Security Concerns: NERC ISN

The NERC ISN uses ICCP exclusively for real-time data exchange. ICCP is also used (along with ftp) to transmit configuration data via off-line file transfer.

From a communication security perspective, the following are known security requirements for the NERC ISN:

- Integrity and accuracy of operational data
- Confidentiality of data, especially ensuring that purchasing/selling entities in the wholesale merchant community are not able to access the operational data.

NERC has identified the following four general threat sources to the ISN:

- Malicious, external hacker
- Disgruntled employee
- Unintentional employee error
- “Trusted” external user

Potential damage resulting from these threats depends upon the extent of the intrusion or error and ranges from a brief loss of system functionality to database or software corruption that results in extended loss of availability and lengthy recovery. Database content alteration could propagate invalid information to critical decision support systems and potentially disrupt power grid operations.

Based on these general data security requirements, range of threat sources, and serious potential consequences of intrusion or error, examining data security provisions in ICCP is warranted to protect the ISN alone. Consideration of the additional uses of ICCP in a range of energy company communication applications listed in Table 1-2 reinforces this conclusion.

3

PRELIMINARY SOLUTIONS

ICCP provides access control via bilateral tables maintained on an ICCP server. This is the only data security service provided within ICCP. To date, no additional data security services within ICCP have been proposed. Further, documents synthesized to prepare this report did not identify specific additions of data security measures to be implemented within ICCP. The ICCP protocol designers assumed that additional data security measures—such as authentication to ensure users are who they say they are and encryption to ensure data integrity—would be implemented in various layers of the OSI 7-layer stack.

Based on information presented in “EPRI 2000a” in the bibliography, this chapter discusses data security that ICCP provides via bilateral tables, briefly covers physical security, and provides an overview of preliminary data security solutions that can be implemented in various layers of the OSI 7-layer stack. These preliminary solutions are organized according to the five types of data security services defined by the OSI model—authentication, access control, data confidentiality, data integrity, and nonrepudiation. The solutions covered in this chapter are preliminary; EPRI plans to publish a second report with specific data security recommendations for ICCP in 2002.

Data Security in ICCP

ICCP specifies access control through the use of bilateral tables defined for each client/server association. Clearly specified in IEC 60870-6-503 (ICCP Services and Protocol), bilateral tables provide execute, read/write, read-only, or no access for each item that can be requested by a client. The server checks each client request to verify that the client has access rights to the data or capability requested. An ICCP client can view only data pre-approved and listed in these tables. Either a client or a server can initially establish an association, and an established association can be used by either a client or server application, independent of how the association was established. The Protocol Implementation Conformance Statement (PICS) performance specifies how associations are used in ICCP actual configurations.

Implementation, including the management and maintenance of these tables, is a “local implementation issue.” As a result, each vendor that markets a product based on ICCP can choose how to implement the bilateral tables, including the type of operator interface provided. This means that an actual physical table is not required, as long as the functionality is implemented according to the ICCP specification.

In some cases, ICCP users may decide not to use the data security mechanisms provided through bilateral tables (e.g., ICCP use between two regional control centers within the same energy company). One way to handle this is to provide the same access to all control center objects in

the Virtual Control Center to any client. However, the protocol operations and actions defined in the ICCP specifications must be implemented to ensure interoperability.

Physical Security

Physical security is important to control access to devices that can, in turn, enable access to data being exchanged using ICCP. The majority of the respondents to the EPRI survey on control center security indicated that their control centers were physically secure. However, recent invasions and malicious destruction of control center equipment by ex-employees has demonstrated that procedures used to enforce this security are often missing or ignored.

In addition, a large percentage of the respondents indicated that the garbage of the control center is not secure and that it is removed by non-bonded services. This allows for the threat of information leakage through what is commonly called “garbage diving.”

Although measures that block physical access to control centers and control center data are an important component of a data security program, a detailed discussion is beyond the scope of this report.

Authentication

One of the five types of data security services that the OSI model defines, authentication services verify the identity of a user or entity and are usually performed when a connection is established. Access requests to the ICCP server may originate from an individual within the control center or from an entity at a remote location.

The following services can be used to authenticate *individuals* seeking to access a network that uses ICCP:

- **Passwords.** Passwords can be required for each host and for individual applications. In a distributed computing environment, a directory service can provide a single entry point for all distributed services, avoiding the need for a separate password for each service.
- **Key cards.** Key cards are especially useful for challenge-and-response authentication techniques. Commonly used on EMS operator consoles to gain access, key cards are a more secure form of individual authentication than usernames/passwords.
- **Biometrics.** The next level of individual authentication, biometrics incorporate information about physical characteristics such as signatures, fingerprints, voiceprints, eye prints.

In some cases, individual authentication procedures involve combinations of these techniques, incorporating information that you know (e.g., a password) with something you have (e.g., a key card or physical characteristic).

The following services can be used to verify the identity of an *entity* seeking access to a network using ICCP:

- **Private key technology or public key technology** (i.e., public key infrastructure, PKI). After ICCP users create a connection and establish an association, these technologies enable entities to authenticate themselves using a digital certificate issued from a trusted source.
- **UCA 2.0 ACSE.** The Utility Communications Architecture (UCA™) Version 2.0 profile document specifies the use of the OSI layer 7 Association Control Service Element (ACSE) Authentication-value parameter.

Access Control

After authenticating the identity of individuals or entities, the next step in the OSI security model is access control, which controls what information the users is authorized to access and what actions the users is permitted to enact (e.g., read, write and/or execute). Alternative mechanisms to provide access control for individuals include the following:

- **Access control lists.** For example, UNIX file systems can restrict access privileges to the user ID of the owner, a workgroup, or all users, but fall short of the full functionality of access control lists, which define access privileges for each individual user for each system resource. Most UNIX vendors offer optional software to provide access control lists.
- **Passwords.** Passwords are a form of access control, when used by individual applications such as EMS consoles.

In addition to access control lists, access control techniques for remote entities include the following:

- **Bilateral tables.** Bilateral tables in ICCP provide limited access control, and must be coupled with an authentication service when a connection is first established between client and server.
- **Router.** The filtering capability of a router, which can restrict access by address (destination or source IP address and port for TCP/IP networks), provides another type of access control. Packet filtering provides a way to build a firewall around a specific network or system. This technique typically is used internally (e.g., to restrict access to the real-time EMS/SCADA system from devices not on the real-time EMS LAN). A router can also be used to restrict external access from the Internet, although a gateway offers better protection.
- **Gateway.** Some types of application-level gateways or “proxies” can provide more robust protection for vital system resources against intentional or inadvertent intrusion. When used as the link to the Internet, the gateway is configured like a router, except that it appears as an end system to the Internet. Such a gateway limits the types of TCP connections permitted from outside the gateway to the control center networks, while permitting more possibilities for control center personnel to access external systems. A gateway is more secure than a router, but less convenient for users and has the potential to become a bottleneck due to lower performance.

- **Firewall.** Increasingly sophisticated firewalls typically combine most of the data security features described above and incorporate additional features. A recent EPRI report recommended the following key capabilities of firewalls in a control center environment:
 - Packet filtering in order to restrict access based on both source and destination IP addresses
 - Application-layer proxy capability
 - Ability to guard against IP spoofing (i.e., would-be intruder outside the firewall configures its machine with IP addresses on the internal EMS LAN)
 - Protection against denial-of-service attacks (e.g., by rejecting packets identified as part of such an attack)
 - Performance of network address translation, enabling the control center to hide IP addresses used on the internal EMS LAN from external view
 - Comprehensive logging capability to log break-in attempts
 - Notification via pager and/or email when a break-in attempt is detected
 - Remote management
 - Granular management to prevent the attack response from denying communication services to legitimate users (e.g., both source and destination address-based filtering, port-based filtering, and protocol-based filtering).

Data Confidentiality

Data confidentiality is concerned with protecting data from unauthorized disclosure. Available alternatives include the following:

- Physical protection, such as installing transmission media through conduit or observed areas to prevent tapping.
- Security routing, which specifies selected routes for routers to use when routing packets. This permits the use of only certain links, such as privately owned links, when sending sensitive data between sites. This feature requires OSI network layer software to accept such routing information. ICCP uses this feature.
- Encryption with the DES standard.

Data Integrity

Data integrity services ensure that no modification, insertion, or deletion of data can occur in either the entire message or in selected fields. Typically this is done at higher layers in the protocol stack, such as layers 4 or 7. Some protection is provided through standard error detecting algorithms, such as cyclic redundancy codes (CRC) in layer 2.

4

SECURING ICCP USING STASE-MMS

Securing MMS

This chapter summarizes a proposed system described in “SISCO 1998” in the bibliography, currently in review, that defines a new Application Service Element (ASE) called Security Transformations Application Service Element for MMS (STASE-MMS). Residing between MMS and the presentation layer in the OSI protocol stack, the proposed system supports data security services for MMS protocol data units (PDUs, which are packets that contain structured message content) and MMS objects. The system can, in turn, secure data being communicated using the ICCP protocol (see Figure 4-1).

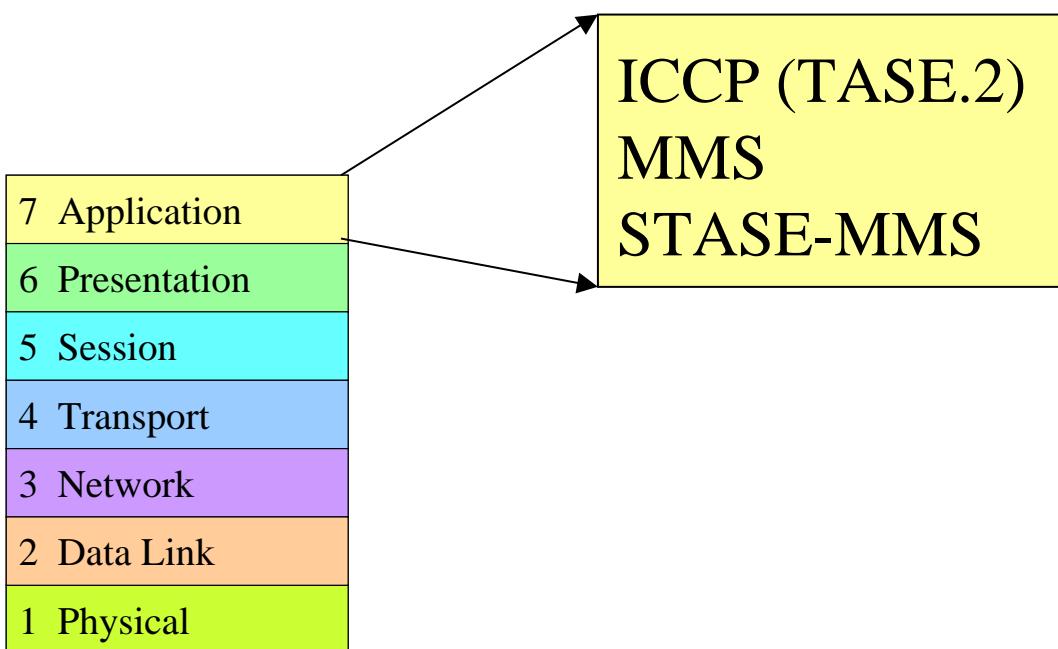


Figure 4-1

Location of STASE-MMS in the Open Systems Interconnection (OSI) Protocol Stack.
Within the application layer, Security Transformations Application Service Element for MMS (STASE-MMS) resides below MMS, which operates below ICCP (TASE.2).

The proposed system provides an approach for performing security transformations (STs). Security transformations are used to provide security services such as peer entity authentication, data origin authentication, confidentiality, integrity, and non-repudiation. STs include encryption, hashing, digital seals, and digital signatures. STASE-MMS makes use of the Association Control Service Element (ACSE) (layer 7) and adds additional transformation

functions within the Presentation layer (layer 6). Otherwise, no other security enhancements are required for layers 1 through 5 of the communications stack. STASE-MMS is an implementation of several options specified by the Generic Upper Layers Security (GULS) standard.

ICCP uses MMS as its messaging service, and STASE-MMS was developed with ICCP in mind.

Supported Security Transformations

STASE-MMS is an application service element that provides the transformations necessary for secure transfer of MMS PDUs. In addition, STASE-MMS provides a means for exchanging information regarding the data security being provided. A request from MMS on the transmitting side invokes STASE-MMS, and STASE-MMS provides an indication to MMS on the receiving side. Both the request and the indication contain the MMS PDU being protected, as well as (optionally) information regarding the type of data security being provided.

STASE-MMS protects MMS PDUs by applying selected security transformations to whole MMS PDUs encoded with the Distinguished Encoding Rules (DERs). STASE-MMS supports the following STs:

- **Confidential:** The DER-encoded MMS PDU is encrypted for privacy protection with a symmetric key encryption algorithm.
- **Public enciphered:** The DER-encoded MMS PDDU is encrypted for privacy protection with a public key encryption algorithm.
- **Hashed:** STASE-MMS computes a hash-based Message Authentication Code (MAC) of the DER-encoded MMS PDU and a secret password and appends the result to the MMS PDU for integrity protection.
- **Sealed:** STASE-MMS computes the digital seal of the DER-encoded MMS PDU and appends the result to the MMS PDU for integrity protection.
- **Signed:** STASE-MMS computes the digital signature of the DER-encoded MMS PDU and appends the result to the MMS PDU for non-repudiation protection.
- **Confidential signed:** STASE-MMS computes the digital signature of the DER-encoded MMS PDU and appends the result to the encrypted (see “confidential” above) MMS PDU for non-repudiation and privacy protection.
- **Confidential hashed:** STASE-MMS computes the MAC of the DER-encoded MMS PDU and appends the result to the encrypted (see “confidential” above) MMS PDU for integrity and privacy protection.
- **Confidential sealed:** STASE-MMS computes the digital seal of the DER-encoded MMS PDU and appends the result to the encrypted (see “confidential” above) MMS PDU for integrity and privacy protection.

STASE-MMS can also pass through MMS PDUs in the clear, without encoding or STs.

Default Data Security Algorithms and Mechanisms

Unless otherwise agreed between the communication entities, the following selected default conventions, data security algorithms, and data security mechanisms are proposed:

- Default encryption algorithm for symmetric key encryption: the Digital Encryption Standard (DES) in the Cipher Block Chaining (CBC) mode.
- If triple DES is needed: Encryption Decryption Encryption in the CBC outer feedback mode with three different DES keys.
- The default public key encryption algorithm: RSA
- The default hashing algorithm: MD5.
- The default MAC (for keyed hashing): HMAC.
- The default seal: the MD5 hash of the DER encoded MMS PDU encrypted with DES.
- The default digital signature: the MD5 hash of the DER encoded MMS PDU encrypted with RSA and the user's private key.

Data Security Information Exchange

The following messages, exchanged between STASE-MMS entities, or between MMS and STASE-MMS, specify which of the STs listed above is being used to protect the MMS PDU:

- MMS invokes STASE-MMS on the originating side
- The originating STASE-MMS sends a STASE-MMS PDU to a peer STASE-MMS entity on the receiving side
- STASE-MMS on the receiving side provides an indication to MMS.

Knowledge of which STs are performed is mandatory, but not sufficient for proper communications. Indeed, both sides need to know which algorithms are being used, as well as the values of all parameters (e.g., encryption keys, initialization vectors) that are in use. The proposed STASE-MMS provides several default values and mechanisms that require only the bare minimum of security-related information exchange. It also provides facilities for negotiating at association setup time which algorithms will be supported and for changing and specifying such information dynamically for every MMS PDU.

STASE-MMS Model

In the OSI environment, communication between application processes is represented in terms of communication between a pair of application entities (AEs) using the presentation service (see Figure 4-2). Communication between application entities may require secure transfer of application protocol data units (APDUs).

APDUs sent by one AE (the sender) are received by the other AE (the receiver). Secure transfer ensures that APDUs transferred by the sender can be correctly verified for integrity, and/or checked for non-repudiation, and/or understood only by the intended receiver. Secure transfer involves security transformation (e.g., encryption) of APDUs from the sending application entity before transferring them and performing the reverse security transformations (e.g., decryption). STASE-MMS only deals with the secure transfer of the MMS application protocol data units.

Secure transfer is carried out within the context of the application association. An application association defines the relationship between a pair of AEs, and is formed by the exchange of application protocol control information through the use of presentation layer services. The AE that initiates the association is called the association initiating entity, or the association initiator, while the AE that responds to the initiation of an application association by another AE is called the application responding AE, or the association responder.

The functionality of an AE is factored into one application process and a set of application service elements (ASEs). Each ASE may itself be factored into a set of more primitive ASEs. The interaction between AEs is described in terms of their use of ASEs.

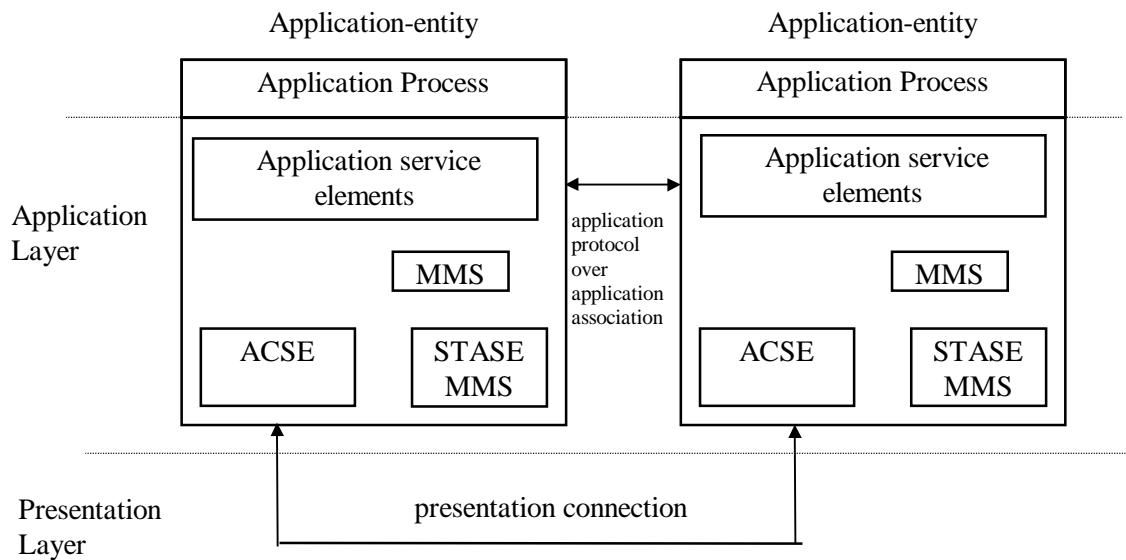


Figure 4-2
Mandatory Application Service Elements When STASE-MMS Is Used. The ASEs available to an application process require communication over an application association. The application processing the services provided by the Association Control Service Element (ACSE) control the application association. Source: "SISCO 1998" in the bibliography

5

BIBLIOGRAPHY

EPRI 2000a. ‘Communication Security Assessment for the United States Electric Utility Infrastructure,’ EPRI Technical Report 1001174, EPRI project manager: William Blair, report prepared by SISCO with assistance from Xtensible Solutions, Inc., (Palo Alto, CA: EPRI, December 2000).

EPRI 2000b. ‘The Benefits of Integrating Information Systems Across the Energy Enterprise: The Power of the Control Center Application Program Interface (CCAPI) and Common Information Model (CIM),’ EPRI Technical Report 1001324, EPRI project manager: Dave Becker, report prepared by Hoffman Publications, Inc., (Palo Alto, CA: EPRI, December 2000).

EPRI 1999. ‘Guidelines for ‘Inter-Control Center Communications Protocol (ICCP) Demonstration: Plant Controls to Dispatch Computer,’ EPRI Technical Report TR-113652, EPRI project manager: R. Shankar, report prepared by EPRI Instrumentation and Control Center, (Palo Alto, CA: EPRI, September 1999).

EPRI 1998. ‘Systems Integration at Kansas City Power and Light Using API and ICCP,’ EPRI Technical Report TR-111443, EPRI project manager: Dave Becker, report prepared by Hoffman Publications, Inc., (Palo Alto, CA: EPRI, October 1998).

EPRI 1996. ‘Inter-Control Center Communications Protocol (ICCP) User’s Guide,’ EPRI Technical Report TR-107176, EPRI project manager: Dave Becker, report prepared by KEMA-ECC, (Palo Alto, CA: EPRI, December 1996).

EPRI 1995a. ‘Intercontrol Center Communications Protocol (ICCP) Demonstration,’ EPRI Technical Report TR-105800, EPRI project manager: Dave Becker, report prepared by ECC, Inc., (Palo Alto, CA: EPRI, November 1995).

EPRI 1995b. ‘Inter-Control Center Communications Protocol (ICCP): Interoperability Test Version 5.1,’ EPRI Technical Report TR-105552, EPRI project manager: Dave Becker, report prepared by ECC, Inc., (Palo Alto, CA: EPRI, September 1995).

IEC 1999. ‘Data and Communication Security,’ Initial Report from TC 57 ad-hoc WG06, International Electrotechnical Commission (IEC), (Geneva, Switzerland: IEC, September 1999).

Bibliography

IEEE 1999. ‘IEEE-SA Technical Report on Utility Communications Architecture (UCA™) Version 2.0,’ IEEE-SA TR 1550-1999, volume 1, part 1: Introduction to UCA™ Version 2.0, (New York: Institute of Electrical and Electronics Engineers (IEEE), 15 November 1999).

SISCO 1998. ‘STASE-MMS,’ draft report, provided by Herb Falk, (Sterling Heights, MI: SISCO, Inc., March 10, 1998).

A

ACRONYMS

ACSE	association control service element
ACE	area control error
AE	application entity
APDU	application protocol data unit
ASE	application service element
CASM	common application service model
CBC	cipher block chaining
CCAPI	control center application program interface
CIM	common information model
CRC	cyclic redundancy codes
DCS	distributed control system
DER	distinguished encoding rules
DES	digital encryption standard
DNP	distributed network protocol
EMS	energy management system
EPRI	Electric Power Research Institute (www.epricom)
FERC	Federal Energy Regulatory Commission
FTP	file transfer protocol
GULS	generic upper layers security
ICCP	Inter-Control Center Communication Protocol
IDEC	Inter-Utility Data Exchange Consortium
IEC	International Electrotechnical Commission (www.iec.ch)
IEEE	Institute of Electrical and Electronics Engineers (www.ieee.org)
IP	Internet protocol

Acronyms

ISN	inter-regional security network
ISO	International Standards Organization (www.iso.ch)
ISO	independent system operator
LAN	local area network
MAC	message authentication code
MMS	manufacturing messaging specification
NERC	North American Electric Reliability Council (www.nerc.com)
OSI	open systems interconnection
PDU	protocol data unit
PICS	Protocol Implementation Conformance Statement
PLC	programmable logic controller
RDI	receiver data interface
RTO	regional transmission organization
RTU	remote terminal unit
SC	security coordinator
SCADA	supervisory control and data acquisition
SPP	Southwest Power Pool
SQL	Structured Query Language
ST	security transformation
STASE-MMS	security transformations application service element for MMS
TASE	Telecontrol Application Service Element
TCP	transmission control protocol
UCA™	Utility Communications Architecture
WAN	wide area network
WSCC	Western Systems Coordinating Council (www.wscc.com)

The Utility Communications Architecture (UCA™) is a trademark of the Electric Power Research Institute (EPRI), Palo Alto, CA.

Targets:

Grid Operations and Management

About EPRI

EPRI creates science and technology solutions for the global energy and energy services industry. U.S. electric utilities established the Electric Power Research Institute in 1973 as a nonprofit research consortium for the benefit of utility members, their customers, and society. Now known simply as EPRI, the company provides a wide range of innovative products and services to more than 1000 energy-related organizations in 40 countries. EPRI's multidisciplinary team of scientists and engineers draws on a worldwide network of technical and business expertise to help solve today's toughest energy and environmental problems.

EPRI. Electrify the World

© 2001 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc. EPRI. ELECTRIFY THE WORLD is a service mark of the Electric Power Research Institute, Inc.

 Printed on recycled paper in the United States of America

1001977