

 Eskom	Standard	Technology
---	----------	------------

Title: **INTER-CONTROL CENTRE
COMMUNICATIONS PROTOCOL
STANDARD**

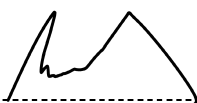
Unique Identifier: **240-82331576**

Alternative Reference Number: <n/a>

Area of Applicability: **Engineering**

Next Review Date: **STABILISED**

COE Acceptance



Richard Mccurrach
Senior Manager – PTM&C Engineering

Date: 3 August 2020

DBOUS Acceptance



Amelia Mtshali
Senior Manager - DBOUS

Date: **03/08/2020**

This document is **STABILISED**. The technical content in this document is not expected to change because the document covers: *(Tick applicable motivation)*

1	A specific plant, project or solution	
2	A mature and stable technical area/technology	x
3	Established and accepted practices.	

Document has no technical changes.

 Eskom	Standard	Technology
--	-----------------	-------------------

Title: **INTER-CONTROL CENTRE
COMMUNICATIONS PROTOCOL
STANDARD**

Unique Identifier: **240-82331576**

Alternative Reference Number: **N/A**

Area of Applicability: **Engineering**

Documentation Type: **Standard**

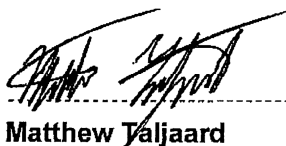
Revision: **2**

Total Pages: **31**

Next Review Date: **September 2020**

Disclosure Classification: **Controlled
Disclosure**

Compiled by



Matthew Taljaard
Engineer
Telecommunications T&S

Date: **20/07/2015**

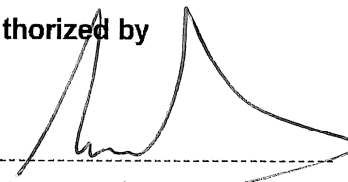
Approved by



Rosalette Botha
System Operator

Date: **20 July 2015**

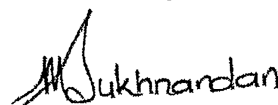
Authorized by



Richard McCurrach
PTM&C Senior Manager

Date: **07/09/2015**

Supported by SCOT/SC



Marlini Sukhnandan
Telecontrol & SCADA SC
Chairperson

Date: **26/08/2015**

Content

	Page
1. Introduction.....	4
2. Supporting clauses.....	4
2.1 Scope.....	4
2.1.1 Purpose.....	4
2.1.2 Applicability.....	4
2.2 Normative/informative references.....	4
2.2.1 Normative.....	4
2.2.2 Informative.....	4
2.3 Definitions.....	5
2.3.1 General.....	5
2.3.2 Disclosure classification.....	5
2.4 Abbreviations.....	5
2.5 Roles and Responsibilities.....	6
2.6 Process for monitoring.....	7
2.7 Related/supporting documents.....	7
3. ICCP.....	7
3.1 Legal Application and Guidelines.....	7
3.1.1 Guidelines.....	7
3.1.2 Bilateral Agreement.....	7
3.2 Architecture.....	8
3.2.1 TEMSE.....	8
3.2.2 Network Configuration.....	9
3.2.3 RCC Peer Communication.....	10
3.2.4 ICCP Server.....	10
3.2.5 Security.....	10
3.2.6 Management Tools.....	14
3.3 Link Application.....	14
3.3.1 ICCP Associations.....	14
3.3.2 AP Title.....	15
3.3.3 Protocol Selectors.....	16
3.3.4 TCP Port Number.....	16
3.3.5 Domain Names.....	17
3.3.6 Domain Name Conventions.....	18
3.4 ICCP Protocol.....	19
3.4.1 ICCP Version.....	19
3.4.2 Bilateral Tables.....	19
3.4.3 Bilateral Table Identifier.....	20
3.4.4 Bilateral Table Version Management.....	20
3.4.5 Data Exchange.....	21
3.4.6 TEMSE PDU Sizes.....	21
3.4.7 Conformance Blocks.....	21
3.4.8 Conformance Block 1.....	22
3.4.9 Conformance Block 2.....	22
3.4.10 Conformance Block 4.....	22
3.4.11 Conformance Block 5.....	22

ESKOM COPYRIGHT PROTECTED

3.5	Data Semantics Conversion.....	23
3.5.1	Conversion of Status Representation	23
3.5.2	Conversion of Flow-Direction Sign	23
3.5.3	Scaling	24
3.5.4	Units of Measure for Measured Values	24
3.5.5	Data Quality	25
3.6	Data Elements.....	25
3.6.1	TEMSE Date Items	25
3.6.2	IEC ASDU Address Range	27
3.6.3	Data Item Type	28
3.6.4	Data Item Source	28
3.6.5	TEMSE Data Item Permission / Network Type.....	28
3.6.6	Data Sets	29
3.6.7	Information Message Request.....	30
3.7	Access Control	30
3.8	Local Implementation	30
4.	Authorization.....	30
5.	Revisions	31
6.	Development Team	31
7.	Acknowledgements	31

Figures

Figure 1: Master Station and RTU Communication Ideal Architecture	9
Figure 2: Data Exchange between adjacent RCCs	10
Figure 3: Overview of Solution 1	11
Figure 4: Network and Security Architecture using the Transport Network	12
Figure 5: Overview of Solution 2	13
Figure 6: Network and Security Architecture using an IP Network	13
Figure 7: Domain Names and the Implementation Thereof	18

Tables

Table 1: Local AP Titles and AE Qualifiers.....	16
Table 2: TEMSE Conformance Blocks	21
Table 3: Sign convention for the different equipment types	23
Table 4: Unit of Measure	24
Table 5: Data Item Bay Naming Convention	26
Table 6: Data Item General Naming Convention	27
Table 7: Eskom ASDU Information Object Address Range	27

1. Introduction

The Inter Control Centre Communication Protocol Standard sets standards, conventions, and fundamental parameters required to exchange data in Eskom between Transmission's Energy Management System (TEMSE) and the various Distribution Management Systems (DMS) using the Inter-Control Centre Communication Protocol (ICCP). Also included is a description of the physical architecture between TEMSE and the DMS.

The document specifies important configuration and functional requirements for ICCP implementations to ensure interoperability. Such information includes addressing specifications, naming conventions and the required ICCP Conformance Blocks. However, the naming convention offered here purely addresses the unique identification for each common point from the Remote Terminal Unit (RTU) back to the respective master. Standards for units of measure, value semantics, sign conventions and quality code semantics are also provided.

2. Supporting clauses

2.1 Scope

The document is presented in two parts. The first part defines the standards, conventions and parameters in logical format. The use cases in the document provide a reference for the actual configuration of the data exchange using ICCP.

2.1.1 Purpose

The document provides guidelines for the configuration of ICCP between TEMSE and the various DMS.

2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited Divisions. This document specifically shall apply to the Energy Management System at the National Control Centre (NCC) and all the DMS in the various Regional Control Centres (RCCs).

2.2 Normative/informative references

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

- [1] ISO 9001 Quality Management Systems
- [2] IEC 870-6-503 TASE.2 Services and Protocol
- [3] IEC 870-6-802 TASE.2 Object Models
- [4] IEC 870-6-702 TASE.2 Profiles
- [5] 240-55410927 Cybersecurity Standard for Operational Technology

2.2.2 Informative

- [6] The standard documentation for the *e-terraplatform* from Alstom Grid is available for the configuration of the Open Access Gateway (OAG) on TEMSE
- [7] EDS ERCOT Nodal ICCP Communication Handbook. Version 2.0 Date: 12 May 2007.

2.3 Definitions

2.3.1 General

Definition	Description
DMZ	Short for demilitarized zone, a computer or small sub-network that sits between a trusted internal network, such as a corporate private local area network (LAN), and an untrusted external network such as public internet. Typically, the DMZ contains devices accessible to internet traffic, such as Web servers.
Dual-use Association	If Control Centre A's and Control Centre B's ICCP nodes act as client and server over one association. Information can be sent in either direction per association. The association type is determined by prior agreement between the two users.
e-terraplatform	The e-terraplatform is a comprehensive set of computer applications from Alstom Grid that form the foundation of generation, transmission, distribution, and training systems for the electric power industry.
MMS	Manufacturing Message Specification. ICCP is based on MMS.
OAG	The Open Access Gateway (OAG) is the system used within e-terraplatform to provide inter-control centre communication.
SCC	Standby Control Centre. The SCC is also known as STABNAC.
Single-use Association	If Control Centre A's and Control Centre B's ICCP nodes act as either client or server over one association. Information can be sent in only one direction per association. The client must initiate the association.
TEMSE	Refers to the Transmission Energy Management System Evolution project, and is now used as the name of the Energy Management System at NCC.
Transport Network	Refers to utilizing the Synchronous Digital Hierarchy and or Optical Transport Network
VCC	Visual Control Centre. Logical view of the elements an ICCP server provides to client sites.
VMD	Virtual Manufacturing Device. MMS's view of a VCC.

2.3.2 Disclosure classification

Controlled disclosure: controlled disclosure to external parties (either enforced by law, or discretionary).

2.4 Abbreviations

Abbreviation	Description
AGC	Automatic Generator Control
AIEF	Association Information Exchange Form
AP	Application Process
AR	Application Reference
ASDU	Application Service Data Unit
BME	Bandwidth Management Equipment
DMS	Distribution Management Systems

ESKOM COPYRIGHT PROTECTED

Abbreviation	Description
DMZ	Demilitarized Zone
Dx	Distribution
EMS	Energy Management System
ET	Eskom Telecommunications
ICCP	Inter-Control Centre Communication Protocol
IEC	International Electrotechnical Commission
ISD	Intra Site Data
ISN	Inter-regional Security Network
ISO	International Organization for Standardization
ISO-TSAP	International Organization for Standardization - Transport Service Access Point
LAN	Local Area Network
MMS	Manufacturing Message Specification
NAT	Network Address Translation
NCC	National Control Centre
OAG	Open Access Gateway
OSI	Open Systems Interconnection
PSEL	Presentation Selector
RBE	Report-By-Exception
RCC	Regional Control Centre
RTU	Remote Terminal Unit
SAPP	Southern African Power Pool
SCC	Standby Control Centre
SSEL	Session Selector
STABNAC	Standby National Control Centre
TCP/IP	Transmission Control Protocol / Internet Protocol suite
TEMSE	Transmission Energy Management System Evolution
TSAP	Transport Service Access Point
TSEL	Transport Selector
Tx	Transmission
VCC	Visual Control Centre
VMD	Virtual Manufacturing Device
WAN	Wide Area Network

2.5 Roles and Responsibilities

To be agreed.

ESKOM COPYRIGHT PROTECTED

When downloaded from the WEB, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the WEB.

2.6 Process for monitoring

The configuration according to the guidelines in the document will be verified as part of the commissioning for all data points.

2.7 Related/supporting documents

- 1) 342-292: Commissioning of substation from the Energy Management System
- 2) SOPPC0071: Point to point testing of plant data from National Control

3. ICCP

3.1 Legal Application and Guidelines

3.1.1 Guidelines

Prior knowledge of an EMS and/or DMS and data communication concepts are recommended before reading the document. The following describes the required modelling steps to enable real-time data exchange via ICCP between the NCC and the RCCs.

- 1) Configure IP Addresses, Reference Names and Links for each ICCP enabled control centre
- 2) For each RCC to be connected with the local NCC, configure a Bilateral Table (Agreement on resource sharing and access) and Associations (multiple redundant associations are possible)
- 3) Within the Bilateral Table for the ICCP Server, configure a subset of the local Data Items and devices to be made available to the remote client with access permissions
- 4) Within the Bilateral Table for the ICCP client, configure the Data Items and Devices that are to be accessible for the local SCADA
- 5) Group local Data Items into different Data Sets
- 6) Assign Transfer Sets for carrying the Data Sets and set condition-monitoring parameters, such as interval-based or event-based triggers, which specify under what conditions each Data Set will be triggered to be packaged and sent to the remote
- 7) Specify filtering conditions like report-by-exception which specifies whether the entire Data Set needs to be sent out or only the changed values in the Data Set need to be sent out

3.1.2 Bilateral Agreement

A Bilateral Agreement is a legal agreement between two control centres detailing the real-time data exchange. The Bilateral Table is the representation of the Bilateral Agreement modelled in the TEMSE Open Access Gateway (OAG) for ICCP data exchange and the respective Distribution Management System (DMS) ICCP servers. The RTU configuration files will be the base for the Bilateral Agreement between control centres in the Transmission and Distribution network.

3.2 Architecture

3.2.1 TEMSE

3.2.1.1 TEMSE SCADA RTU Communication Overview

The primary operating facility for TEMSE is at the NCC. The system has a dual configuration over two equipment rooms. However, the termination of the single telecommunication circuits from the RTUs is split evenly between the two equipment rooms. The secondary operating facility for TEMSE is at the SCC. The SCC is regarded as a hot standby except a few exceptions as all the RTUs have a second telecommunication circuit to the SCC. The SCC provides backup telemetry to NCC for all the RTUs available at the SCC. The net result is that even during a single floor failure at the NCC the backup telemetry via the SCC will provide practically full visibility at the NCC. TEMSE uses IEC 60870-5-101 for communication to the RTUs.

3.2.1.2 TEMSE ICCP Overview

Full redundancy must be used and configuration must avoid dependency on surrounding equipment. Failover functionality of ICCP servers shall occur with each database update and have the option of a fail back requirement.

TEMSE ICCP at NCC shall have the following redundancy:

- 1) ICCP Servers
- 2) Firewalls
- 3) External switches
- 4) ET firewalls
- 5) ET routers

TEMSE ICCP at SCC shall consist of a single hardware installation, software and database configuration shall be identical to NCC.

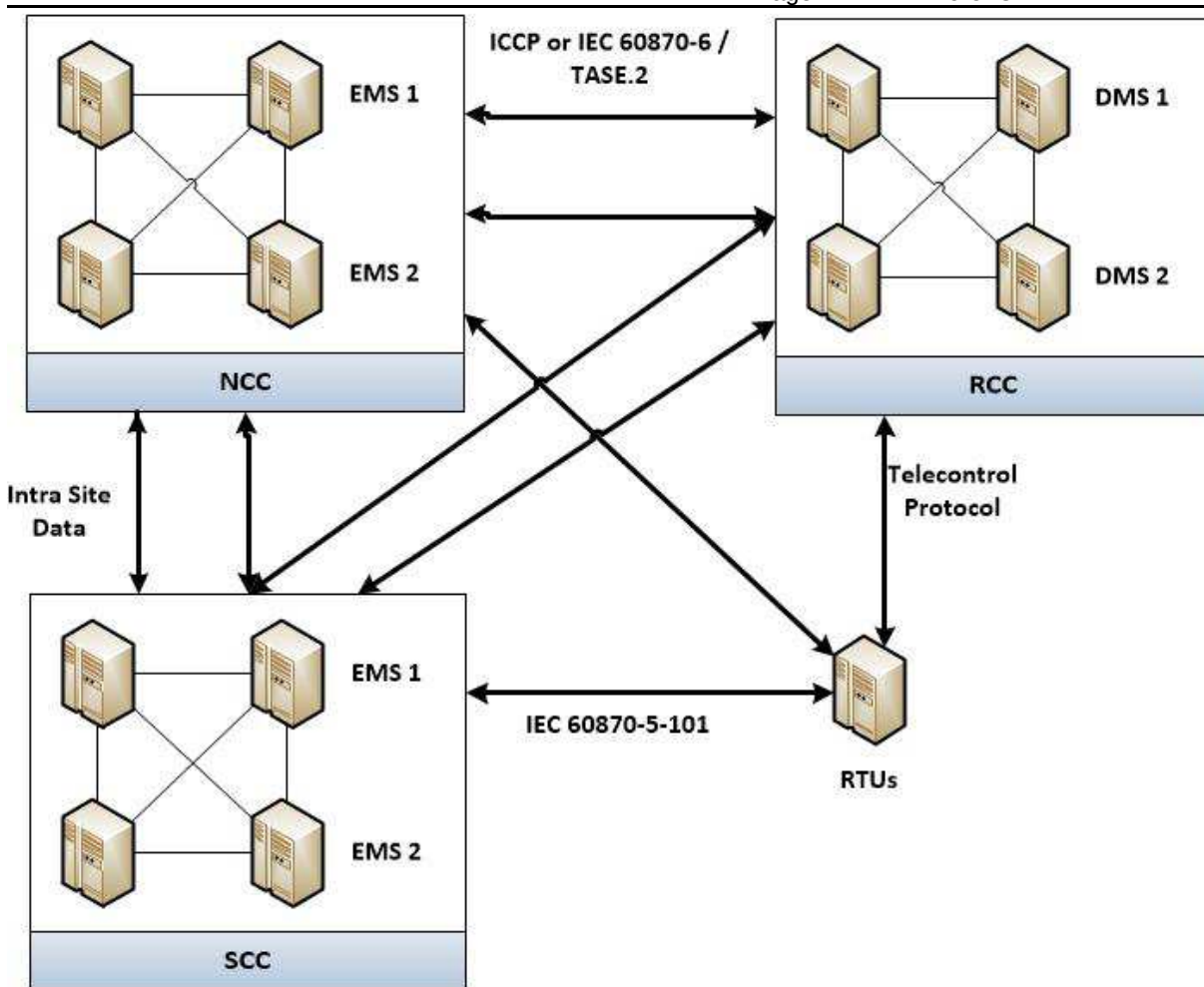


Figure 1: Master Station and RTU Communication Ideal Architecture

3.2.2 Network Configuration

The WAN architecture, used for the inter-control centre real-time data exchange, allows for redundant ICCP OAG servers at NCC, a single ICCP OAG server at SCC and redundant ICCP servers at each of the RCCs in Distribution.

ICCP WAN communications shall make use of virtual point-to-point links over a router based WAN, which is owned and managed by Eskom Telecommunications. The bandwidth of the links can be sized according to user requirements.

Communications between sites will comprise of 2 virtual links between the NCC and RCCs and a single virtual link between SCC and RCCs. ICCP resides in the Layer 7 of the OSI Network Model and is therefore independent of the underlying transport network, so any combination of sub-networks may comprise the WAN, including the LANs within a site. The routers auto-negotiate for network bandwidth (10 or 100 Mbps) and Duplex (full/half). The ICCP network is configured over TCP/IP.

The RCCs shall have a shared WAN where the RCCs WAN router will be shared with other applications and users, but the ICCP link will be virtually separated. The security within the local area network shall reside with the individual control centres at each entry point. The Transmission System Operator and Distribution is responsible for the ICCP OAG server and firewalls. ET is responsible for their firewalls and WAN routers.

ESKOM COPYRIGHT PROTECTED

In the network infrastructure, the line of demarcation is defined to be the output network interface of the Transmission and Distribution owned firewall, and the incoming network connection of the ET owned routers or firewalls.

ICCP should be prioritized if shared on a VLAN with other services. ICCP priority should be higher between regional and national than regional and regional.

Where NAT is required, static NAT shall be used.

Participants shall ensure that full redundancy is maintained at all times.

3.2.3 RCC Peer Communication

The network architecture establishes point-to-point communication between each RCC and both NCC and SCC ICCP servers. The NCC routers are configured to accept only traffic that originates with a RCC and is destined to NCC.

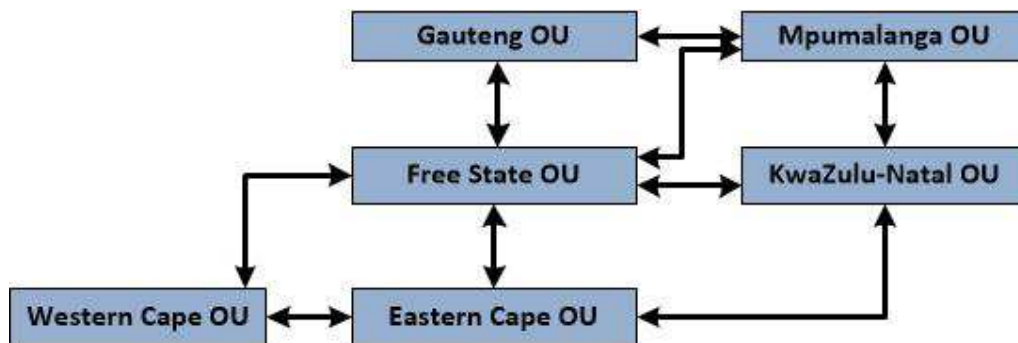


Figure 2: Data Exchange between adjacent RCCs

3.2.4 ICCP Server

Fixed IP addresses are published for the ICCP server on the AIEF. The ICCP servers must respond to these addresses when processing Association Initiation requests.

Five IP addresses shall be allocated to each of the control centres. The IP addresses are for the primary and secondary servers at the primary operating facility as well as the primary and secondary servers, where those exist, at the secondary (backup) operating facility. A development/test ICCP server IP address is assigned to each control centre whether or not such an ICCP server exist as can be indicated on the AIEF.

IP addresses are assigned to the ICCP servers recognising that the control centre may implement NAT in its firewalls/routers. Using NAT, the control centre can assign internal IP addresses to the ICCP servers that are compatible with the control centre's LAN addressing plan.

3.2.5 Security

ICCP Sec protocol will not be used. No Certification Authority is used. An external Certification Authority will require internet access for all control centres. Security for the real-time data exchange between the national and regional control centres is achieved through the use of dedicated virtual point-to-point telecommunication circuits. Each control centre is responsible to provide network security between the shared communication circuits and servers.

The accepted network architectures to comply with cyber security requirements for operational technology are:

3.2.5.1 Solution 1: Use of the Transport Network

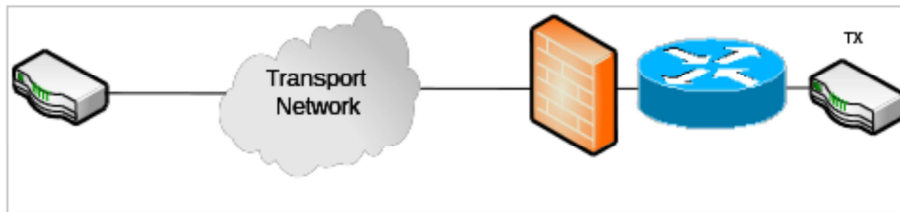


Figure 3: Overview of Solution 1

The network architecture is using the transport network; therefore the “Cybersecurity Standard for Operational Technology” 240-55410927 compliance will not be in the scope. The use of the ADM architecture does not use a routable protocol and the IP Eskom Telecommunications network will not be utilized.

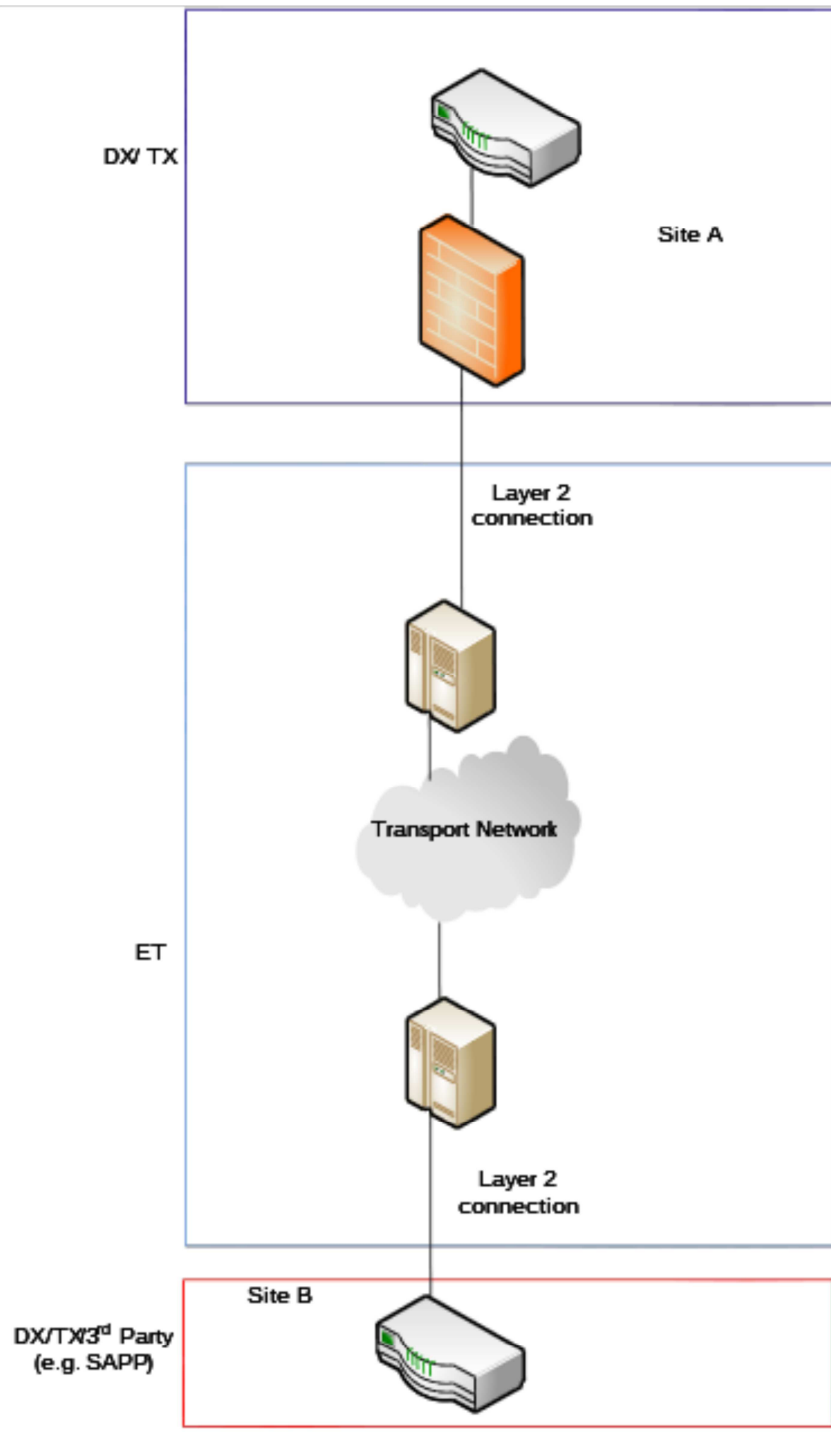
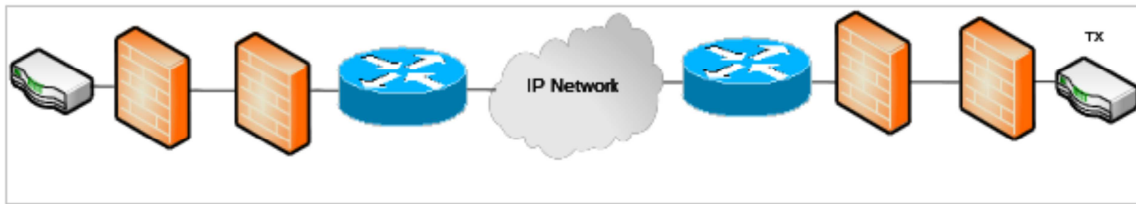
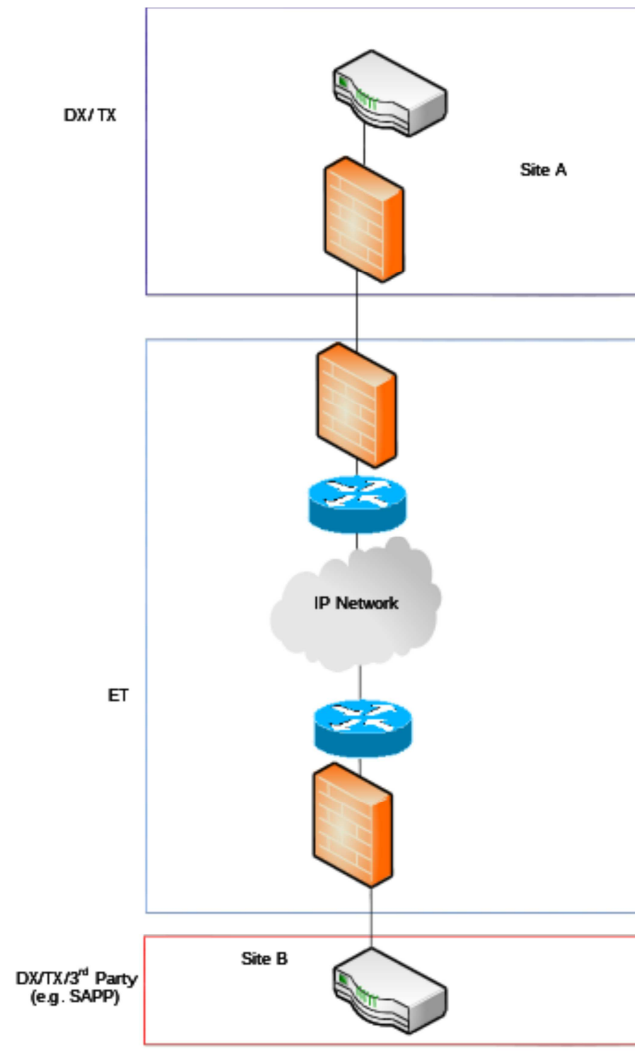


Figure 4: Network and Security Architecture using the Transport Network

ESKOM COPYRIGHT PROTECTED

3.2.5.2 Solution 2: Use of Layer 3 architecture – IP Network**Figure 5: Overview of Solution 2**

Due to the routable protocol and the use of an IP Network (layer 3), the network and security architecture must comply with the “Cybersecurity Standard for Operational Technology” 240-55410927 and “IP Network Security Framework” 240-70732264. The architecture is separated into two divisions Transmission, ET and a 3rd party. Due to the interconnecting of these three sectors, firewall security must be implemented on the access point (seen in figure 4) and the exit point (seen in figure 4) of the ET IP Network.

**Figure 6: Network and Security Architecture using an IP Network****ESKOM COPYRIGHT PROTECTED**

3.2.6 Management Tools

ICCP management tools will be needed to configure and maintain the ICCP database. The minimum functions required by the tool or tools are as follow:

- 1) ICCP modelling
- 2) Database updates
- 3) ICCP updates
- 4) Backup configurations
- 5) Mapping of database points
- 6) Database alignment between ICCP masters
- 7) Fault finding

3.3 Link Application

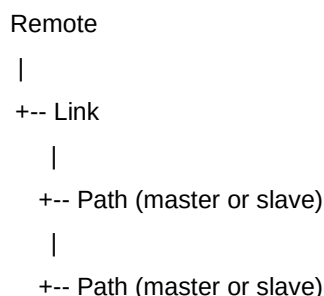
ICCP will be used in both the monitoring and control direction from NCC to the RCCs. The RCC SCADA will receive only monitoring information from TEMSE. Real-time data exchange between RCCs will be for monitoring. Communication between the control centres is through a DMZ and/or firewall.

3.3.1 ICCP Associations

An ICCP Association is the same as a TCP network connection. ICCP Associations can be formed as single or dual (one link record for TEMSE) Associations. These Associations is described according to the client/server role taken on by the control centre in the real-time data exchange. The RCC system is defined as the client when it receives data from the NCC as a result of a request for data. The DMS at the RCC acts as a server when it sends data to the EMS at the NCC as requested. The ICCP servers at all the control centres manage the client and server roles as separate and independent data exchange processes. The initial configuration for the Eskom real-time data exchange will have the DMSs at the RCCs configured as servers and the EMS at the NCC as clients to all the ICCP servers.

A Single-use Association is one where one side of the Association always performs the client role and the other side performs the server role. Single-use Associations require two Associations, one link for the client and one link for the server, if data have to be exchanged both ways, each link having one or two paths depending on the remote system being redundant or not. Single-use Associations in TEMSE with one way data exchange require only one link with one or two paths. With a Dual-use Association, one Association supports both ends acting as both client and server. For either configuration in TEMSE, the number of paths under a link is not limited to two. As many paths as necessary can be configured to support backup control centres for example, but only one path will be active at a time. Valid configurations are:

- 1) Dual Direction Association (all paths have the TEMSE Single Direction Association reset):



- 2) Single Direction Association (all paths have the TEMSE Single Direction Association set, the maximum of links is 2, it is possible to have only one link when data is exchanged only one way):

```

Remote
|
+-- Link
| |
| +-- Path (master)
| |
| +-- Path (master)
|
+-- Link
|
+-- Path (slave)
|
+-- Path (slave)

```

TEMSE supports both kinds of Associations in order to be compatible with any system. However, to manage access and simplify system management, NCC requires RCC ICCP servers to establish Dual-use Associations if their ICCP nodes support it, even if they also support Single-use Associations. To conform to the ICCP standard when Single-use Associations are established, the client will always initiate the Association. For Dual-use Association the establishing side will be determined by agreement but preference will be given to NCC establishing the association.

3.3.2 AP Title

The AP Titles must be unique throughout the entire ICCP network. When using both OSI and TCP/IP transports, you must use a different value for the TSEL parameter, one for each transport e.g. TCP/IP and another for OSI.

The AP Title is an MMS Object Identifier, representing the Application Process Title for your particular application process. An Object Identifier is a sequence of integer values representing an application in the OSI Model. The first value in the AP Title should be in the valid range from 0 to 2. The second value should be 1, 2, or 3 (the valid range is 0 to 39). The third value is open for international assignment. If your addressing is local, then this value should be 9999. The rest of the values are arbitrary. For example, values could be assigned to represent type and location of the application.

The full MMS Object Identifier ("address") is divided into 5 parts: AP_Title, AE_Qualifier, Psel, Ssel and Tsel. In the Network Manager from Ventyx/ABB all 5 are configurable and the only limitation is that the identification of any two systems must be different in at least one of the 5 parts. Other manufacturers may have limitations like only using 2 or 3 of the 5 parts or line where the AE_Qualifier must be the last part of the AP_Title. To accommodate this, the AP_Title in Network Manager can be the same for server 1 and 2 if AE_Qualifier (or Psel, Ssel or Tsel) are different.

Another thing to notice is that the local MMS identification is defined per association and that it is possible to define up to 8 different local identifications. This means that a local identification can be used inside Eskom and if needed, a different identification is used towards other companies. Since the ICCP network does not form part of an ISN, the use of an AP title is optional for TEMSE. The AP Title used within this local network will use the international dialling code for the Republic of South Africa and the local area code for the primary site.

Table 1: Local AP Titles and AE Qualifiers

SITE	ICCP Server 1		ICCP Server 2		ICCP Server DR	
	AP Title	AE Qualifier	AP Title	AE Qualifier	AP	AE
NCC	1 3 9999 27 1	1	1 3 9999 27 1	2	1 3 9999 27 1	3
FS OU	1 3 9999 27 51	1	1 3 9999 27 51	2	N/A	N/A
WC OU	1 3 9999 27 21	1	1 3 9999 27 21	2	N/A	
EC OU	1 3 9999 27 41	1	1 3 9999 27 41	2	N/A	
KN OU	1 3 9999 27 31	1	1 3 9999 27 31	2	N/A	
MP OU	1 3 9999 27 13	1	1 3 9999 27 13	2	N/A	
LP OU	1 3 9999 27 15	1	1 3 9999 27 15	2	N/A	
GN UO	1 3 9999 27 11	1	1 3 9999 27 11	2	N/A	
Dx ECC	1 3 9999 27 10	1	1 3 9999 27 10	2	N/A	
SAPP	1 3 9999 263 4	1	1 3 9999 263 4	2	N/A	
ZESA	1 3 9999 1	1	1 3 9999 2	2	N/A	
ZESCO	1 3 9999 3	3	1 3 9999 4	4	N/A	

Therefore, unpacking an AP Title “1 3 9999 27 21” and AE Qualifier “1” for server 1 and “2” for server 2 result in the first “1” indicates that it is an ISO address, “3” indicates “Identified Organization” and “9999” that “The interchange partners shall agree on the identification of the identification scheme”.

3.3.3 Protocol Selectors

Making association is matching a pair of local/remote AR names from the calling node to a pair of remote/local AR names on the called node. Actually, it is not the AR names themselves that are matched but the information associated with them in the OSI stack configuration (AP title, AE Qualifier, Psel, Tsel, Ssel). Protocol selectors are numerical identifiers for the PSEL, SSEL and TSEL. These fields are optional in TEMSE and only one local AR name can be configured without a Psel, Ssel, and Tsel. The selectors are specified of the form XX XX, as in 00 01. The maximum length is 16 octets (32 ACSII encoded hex digits).

Most systems specify 00 01 for the protocol selectors. The TEMSE example is:

- Psel = 00 00 00 01
- Ssel = 00 01
- Tsel = 00 01

3.3.4 TCP Port Number

By default, ICCP uses the well-known port TCP/102, which is the port number for the ISO-TSAP for Transport Class 0.

3.3.5 Domain Names

The ICCP standard does not impose any specific design requirements on domain implementation. Domain implementation in the ICCP server normally allows for a designated storage area for each client to segregate the values for one client from those for other clients. Each of these storage areas is distinguished by the domain name.

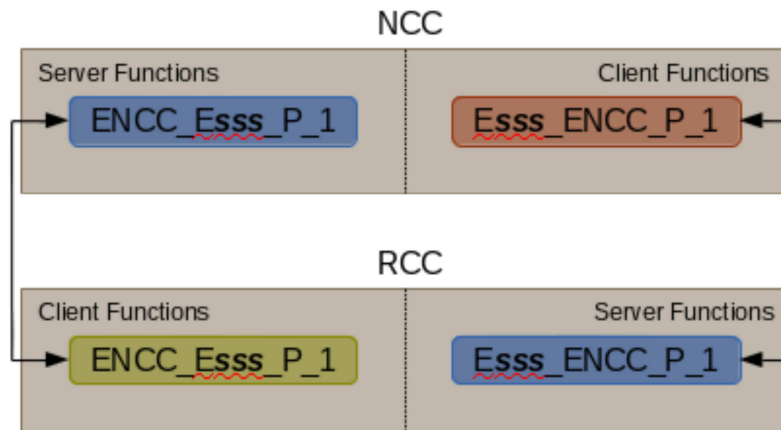
A client does not necessarily require a separate storage area to contain the values accessed from individual servers so that named Data Items accessed from one server won't override the same object name accessed from another server. A "remote" domain and a "local" domain are sometime created with having the same name.

For example, it may be required to create a local domain with the name **Esss_ENCC_P_1** in NCC's ICCP node and to create a remote domain with the same name in RCC's ICCP node, the server node. The local domain simply means that the user is configuring a storage area in its server that will contain the values to be retrieved by the client node (NCC), which will refer to the name **Esss_ENCC_P_1**. In addition, there may be a requirement to create a remote domain, named **ENCC_Esss_P_1**, in the RCC node. In this case the RCC node, acting as client, will retrieve Data Items from the domain **ENCC_Esss_P_1** in the NCC node which is acting as a server. These values will then be stored in a named region being set aside for that purpose.

The abbreviations for the control centres will be Eskom National Control Centre (ENCC), Eskom College Test Centre / ECC (ESTC), Northern Region / Mpumalanga Operating Unit (ESMC), Southern Region / Eastern Cape Operating Unit (ESEC), Western Region / Western Cape Operating Unit (ESWC), Eastern Region / Kwazulu Natal Operating Unit (ESKC), Central Region / Gauteng Operating Unit (ESGC), North West Region / Free State Operating Unit (ESFC), Limpopo Operating Unit (ESLC).

The non-standard terms "local" and "remote" used by the suppliers and assign arbitrary meanings to the terms are more confusing than helpful. The ICCP standard does assign well-defined meanings to the terms "client" and "server" and describes ICCP operations in those terms. Specifically, a "server" makes values available to interconnected computers, and a "client", requests the available values. Servers define (and create) domains and clients refer to them when requesting data. The illustration given below describes the intent of the standard and the effect of its interpretation by the product vendors.

In Network Manager from Ventyx/ABB in the ICCP server there is a pair of Domain Name and Bilateral Table ID defined for each client. This means that for one connection there is one local Domain Name and one Bilateral Table ID that is used when acting as a server for this connection. There is also one Domain Name and one Bilateral Table ID defined in the remote system that is used when this system is acting as a client for the connection. In Network Manager these values can be defined independent of each other, but other manufacturers may have limitations that the Bilateral Table ID's must be the same.



Blue areas represent real domains in an ICCP node. They exist as part of the ICCP server environment. These domains contain the values that can be accessed by the ICCP clients. The domains are physically allocated and exist in the ICCP server memory.

The green area represents NCC's client functions. In order for NCC to access data in the RCC's ICCP server, the data requests must reference the appropriate RCC ICCP server domain names. As defined in the ICCP standard, domain names specified by the client are access reference parameters. They are not formally defined as domains in the NCC client.

The red areas represent the RCC's ICCP client functions. In order for the RCC to access data in the NCC ICCP server, data requests must reference the appropriate NCC ICCP server domain names.

In some systems, domains that exist in an ICCP server, are also mirrored in the ICCP client as if they were "client domains". Because of this vendor-dependent implementations, they are sometimes called "remote" domains (or "local" domains). Regardless of the vendor's implementation strategy, the primary purpose for configuring the NCC server domain names in the RCC's ICCP client is to provide a reference to the correct Data Item in the NCC ICCP server.

Figure 7: Domain Names and the Implementation Thereof

The above discussion of domains is given to assist in the completion of the AIEF document. The point being that a domain is always a server specification. Domains are never assigned to client nodes.

3.3.6 Domain Name Conventions

The domain is a subset of the control centre's view of a VCC, the VMD. The VCC is a logical view of the elements a server ICCP provides to client sites. Domains are server specific. That is, a domain is configured in a server to contain the specific values a particular client can access. The client must then know the name of the domain in the server to which it has access in order to access those values. Every ICCP server shall implement domains. In particular, every RCC shall configure a domain since all RCCs act as a server for the NCC.

In TEMSE the remote domain name can be entered in mixed case and with up to 32 characters as per the ICCP specification. The remote site will refer to this name when requesting data. The MMS domain name is a MMS identifier and thus must begin with a letter, and contain the characters [a...z], [A...Z], [0...9], \$ and _ (underscore) only.

The domain name has the form:

`Esss_Eccc_f_n`

Where:

- 1) **Esss** is the control centre identifier for the server requesting the connection
- 2) **Eccc** is the control centre identifier for the server confirming the connection
- 3) **f** is used to identify the operating facility
- 4) **n** is used to identify the ICCP server node number

The operating facilities are identified as primary operating facility (P), secondary operating facility (S) and the development facility (D). Thus, the primary/backup server node at the primary operating facility will both use a server domain name ending with, "P_1", and the primary/backup server node at the secondary operating facility will both have a server domain name containing, "S_1". If, however, the backup ICCP server node at the primary operating facility should be accessed in parallel then the domain names should be made unique. This will result in two Domain names being defined for the primary operating facility ending with "P_1" and "P_2" respectively.

Shown here is an example of a domain name for the client/server Association where the server is the Central Region/ Gauteng Operating Unit (ESGC) and the client is the National_Control_Centre (NCC):

`ESGC_ENCC_P_1`

Central Region / Gauteng Operating Unit stores the values accessible to the National Control Centre (NCC) in each domain as appropriate. NCC then includes the relevant domain name in its access requests. Conversely, the NCC, when acting as a server would contain a domain for the RCC configured as:

`ENCC_ESGC_P_1`

3.4 ICCP Protocol

This part of the reference defines the TEMSE implementation of the ICCP protocol. To ensure that control centres successfully connect and exchange information, many components of ICCP and its underlying protocol stack must be configured in all ICCP servers in a coordinated way.

3.4.1 ICCP Version

The ICCP versions supported are ICCP version 2000-08 and ICCP version 1996-08. If not supplied, the TEMSE validation will default the version to 1996-08. If the version selected here and the actual version the RCC is using mismatch, the connection will be aborted.

Other software installed for TEMSE includes SISCO MMS-EASE Version 8.01.

3.4.2 Bilateral Tables

Bilateral Tables reflect a security mechanism ICCP defines to control access to data objects. A Bilateral Table is a computer-generated reflection of a Bilateral Agreement. A Bilateral Agreement is a legal document stating the data elements a data owner is willing to provide to the client and the means to access them. Bilateral Agreements through Bilateral Tables provide for contractual agreements between data exchange partners.

The full methodology suggested by the ICCP standard for Bilateral Agreements will not be implemented. Such a formal, contractual process is unrealistic in a single utility between the national and regional control centres. Rather, the definition of the Data Items shall include access control attributes and the domains the items are assigned to. Access control attributes combined with domain assignments implement the concept of the Bilateral Table.

3.4.3 Bilateral Table Identifier

The Bilateral Table Identifier (ID) is the version identifier of the Bilateral Table Agreement with the client. The version is exchanged between communicating sites and must be the same for an Association to be formed. This is a character string with a maximum length of 32.

Regardless of the specific internal implementation a Bilateral Table Identifier is designed to ensure that the data element access list between the NCC and various RCCs are consistent. In the ICCP standard, this identifier is called the Bilateral Table Version.

The naming convention for the Bilateral Table Name includes a text identifier and version number. The number portion of the Bilateral Table Name is typically incremented each time the Bilateral Agreement changes. Since the Bilateral Table Version number will rarely change (no formal Bilateral Agreement) and a Bilateral Table Name mismatch will result in a failure to establish an Association, it is required that no procedure should be defined that would artificially cause an Association to fail. Therefore, the following Bilateral Table Version management procedure is designed to be consistent with this policy.

3.4.4 Bilateral Table Version Management

Bilateral Table ID has the form:

ENCC_Eccc_vvv
or
ENCC_Eccc_dddddddd

Where:

- 1) **ccc** is the control centre identifier for the RCC
- 2) **vvv** is the Bilateral Table version identifier
- 3) **dddddddd** is the optional alternative using the database update date as yyyyymmdd in the event that Data Item changes requires frequent notifications.

A valid example for a Bilateral Table ID for an Association between TEMSE and the Western Region / Western Cape Operating Unit is the following:

ENCC_ESWC_001

To minimise the impact database updates has on the frequent and rapid changes to the Bilateral Tables, the Bilateral Table ID will change only after mutual agreement between the control centres that the Bilateral Table should be re-synchronised. Therefore, the adding or deletion of objects will not require a change in the Bilateral Table ID. The first Bilateral Table ID shall always start with 001.

The result of the above policy is that Associations can be established even if the Bilateral Table between the client and server disagree. In this situation, when the client requests an object which it can no longer access, an object access error will be reported. The configuration mismatch between the control centres for a Data Item can then be resolved by referring back to the current RTU configuration file either through an automated process or by human intervention.

It is also possible that new items will be made available in the server of which the client is not aware. To avoid this problem, the client can periodically retrieve the names of all the objects in the server to which the client has access. The client can then compare this list with the objects defined in its database. If any missing objects are discovered, and deemed by the client to be important, the client can add the objects to the database.

There shall be a weekly confirmation to the changes in the bilateral table and all participating partners shall be notified and agreed upon of any changes by the distribution of the latest bilateral table.

3.4.5 Data Exchange

The Data Items exchanged in Conformance Block 1 and Conformance Block 2 between control centres using ICCP typically correspond to points, analogues or controls in an EMS or SCADA system. Data Sets group Data Items according to the reporting preferences of the parent remote. The Data Set ID is the identifier for the data set and must be unique within a remote. It is a character string, length 32, with no embedded blanks.

In normal operation (after Associations are established and initial handshaking is done), only Data Sets are exchanged. Sending a Data Set via ICCP is an operation not requiring response from the receiving side (in MMS, this is an 'unconfirmed request'). Only SCADA Data Sets may contain more than one Data Item.

In TEMSE Data Items that will be inserted in a Data Set are modelled as child records for the Data Set, one record per Data Item. The number of records (i.e. Data Items) per Data Set is limited by the maximum MMS PDU size.

3.4.6 TEMSE PDU Sizes

Defined scopes for the TEMSE OAG are VMD (global), Domain (restricted to a single remote site), and Association (restricted to a single association with a remote site). During handshaking the list of Data Items in the Data Sets is exchanged between the control centres. The list contains the Data Item names and for each Data Item in Domain scope, the name of the Domain. Depending on the size of the names, the absolute limit can be divided almost by a factor of 2. For example, with names of 20 characters and Domain names of 8 characters, the limit falls to about 800 Data Items per Data Set, for a PDU size of 32 000 bytes – the maximum supported by TEMSE. It is better, when possible to have:

- 1) Short data item names
- 2) Maximum of data item in VMD scope (in this case only the data item name is exchanged, not the domain name)

It is recommended not to have Data Sets with more than 800 Data Items. The TEMSE validation program gives an estimate of the PDU size for each data set.

3.4.7 Conformance Blocks

All ICCP implementations shall provide the ICCP functionality specified as "Conformance Blocks" listed below. These objects are used to convey the data which are defined in various parts of IEC 60870-6-503.

Table 2: TEMSE Conformance Blocks

Conformance Block 1	Periodic System Data: Status points, analogue points, quality flags, time stamp, change of value counter, protection events. Association objects to control ICCP sessions.
Conformance Block 2	Extended Data Set Condition Monitoring: Provides report-by-exception capability for the data types that block 1 is able to transfer periodically.
Conformance Block 4	Information Messages: Simple text and binary files.
Conformance Block 5	Device Control: Device control requests: on/off, trip/close, raise/lower etc. and digital set-points. Includes mechanisms for interlocked controls and select before-operate.

ESKOM COPYRIGHT PROTECTED

3.4.8 Conformance Block 1

Conformance Block 1 includes the following objects:

- 1) Association
- 2) Data Value
- 3) Data Set
- 4) Transfer Set

Conformance Block 1 provides for the periodic transfer of power system data. Data Values are the some alphanumeric quantity database representation of field device status (i.e. breakers, links, substation gates, etc.); analogue values (i.e. MW, MVAR, voltage, tap settings, phase shifter angles, etc.), and accumulator values. Each data item may also have associated with it a quality code that provides information about the reliability of the data item itself. The data object transferred in Conformance Block 1 is the Indication Point Object.

3.4.9 Conformance Block 2

Conformance Block 2 compared to Conformance Block 1 is used to optimise the data exchange. Conformance Block 1 reports every value to the client every time the report is generated; it is not very bandwidth efficient. Conformance Block 2 is also referred to as report-by-exception (RBE).

Report by exception allows the client to specify that power system objects will be reported only when a change is detected or when an integrity check is performed. ICCP does this by having the server monitor a number of conditions and when one or more of those conditions occurs, the data that has changed is sent to the client. The client sets the conditions to be monitored in the transfer set at the server.

The conditions that can be monitored are:

- 1) IntervalTimeOut: The normal reporting period is due is the same condition that is monitored in Conformance Block 1
- 2) ObjectChange: The value, state or quality code of a value has changed
- 3) OperatorRequest: The operator at the server site has requested that the value be sent to the client
- 4) IntegrityTimeOut: A periodic report of all values is sent to the client to ensure that the two databases are still synchronized and that no changes have been lost since the last integrity check
- 5) OtherExternalEvents: These are unspecified conditions which are monitored

3.4.10 Conformance Block 4

Conformance Block 4 adds the Information Message Transfer Set server object with the associated Information Buffer data object. It provides a general message transfer mechanism that allows for the transfer of simple text or binary files by agreement of the two parties.

3.4.11 Conformance Block 5

The request to operate a device through ICCP Conformance Block 5 provides a mechanism for transferring a request from one ICCP implementation to another. ICCP does not directly control the device; rather it communicates a client's request to operate a device to the remote ICCP server, which will do in on behalf of the requestor.

NCC uses a select-before-execute for most device controls. An exception is the AGC command, where the RTU will not require the select-before-execute function, but will operate on an execute command only basis to allow for parallel processing. However, NCC will not request AGC commands to be issued through a RCC.

No controls shall be modelled for any control centre.

3.5 Data Semantics Conversion

Data semantics conversion is provided to support:

- 1) Defined representations of status, and conversions to alternate representations.
- 2) Conversions between different meanings of the sign bit on analogue values. The sign of an analogue is used to represent the direction of flow, but there is no standard convention as to whether positive represents "from" or "to" between control centres.
- 3) Conversions between different units of value (scaling).

A data semantics conversion can take place when the data is received ("on input"), or when the data is transmitted ("on output"). The scope of the data conversion can be done either remote-wide, when the majority of the Data Items require conversion, or Data Item-specific modelling for a single Data Item. Sequential conversions of the same type of conversions are allowed, and are performed only to the extent of their common scope. This means the Data Item-specific modelling will block the execution of a conversion of the same type for a remote-wide conversion.

3.5.1 Conversion of Status Representation

Conversions of status representation are modelled remote-wide or on a per-Data Item-per-remote basis, so that only when the exchanging sites differ in representation a conversion can be applied.

When a status conversion is modelled in TEMSE it is applied to both the current state and the expected state when using data items of type supplemental introduced in ICCP 2000-08 as well as the Supplemental Objects data types defined in IEC 60870-6-802 Annex B.

The modelling for the status conversions are:

The modelling of the status conversion on input in TEMSE is always done from the remote representation to the ICCP standard representation as described in Section 8.1, "Use of Indication Point Model" in ICCP IEC 870-6-802, TASE.2 Object Models, and Version 1996-08.

The modelling of the status conversion on output is done the inverse which is between the ICCP standard representation and the own representation of the remote. This is because it is more likely that the status values in the ICCP server do not follow the ICCP standard (necessitating the conversion in the first place), hence for modelling status conversion on output in TEMSE, it is required to specify whether the values in the database follow or not follow the ICCP standard.

3.5.2 Conversion of Flow-Direction Sign

TEMSE has no native convention for direction of flow, and some values have no directional meaning. NCC has adopted a standard whereby flow out of the busbar is positive and the flow into the busbar is negative. However the sign for the capacitor is relative to the local bus node.

The measurements associated with each of the equipment types in the power system are defined in Table 3.

Table 3: Sign convention for the different equipment types

Equipment Type	Measurement	Sign Conversion
Busbar	kV, Hz	Always Positive
Capacitor	MVar	Relative to local bus node
	kV	Always Positive
Circuit Breaker	MW, MVar	Flow into the busbar is negative
DC Injection	MW, MVar	Flow into the busbar is negative

Equipment Type	Measurement	Sign Conversion
Generator	MW, MVar	Flow into the busbar is negative
	kV, Hz	Always Positive
Line	MW, MVar	Flow into the busbar is negative
Load	MW, MVar	Flow into the busbar is negative
	Amp	Always Positive
Reactor	MW, MVar	Flow into the busbar is negative
	kV	Always Positive
Transformer	MW, MVar	Flow into the busbar is negative
	Amp	Always Positive
	Tap Position	Always Positive
	°C	Always Positive

3.5.3 Scaling

TEMSE has no native convention for units of value.

1) The formula for scaling upon input is:

$$OAGValue = (RemoteValue - bias) / ratio$$

The formula for scaling upon output is:

$$RemoteValue = (OAGValue * ratio) + bias$$

Where:

OAGValue is the data item value as stored in the TEMSE transient value database.

RemoteValue is the data item value as received from or shipped to the remote site.

Ratio is the number or fraction of remote units equal to one TEMSE unit. For example, if the value received from the remote is in units 100 times smaller than the units stored on the TEMSE, the ratio is 100. If the value received from the remote is in units 100 times larger than the units stored on the TEMSE, the ratio is .01.

Bias is a positive, negative, or null constant.

3.5.4 Units of Measure for Measured Values

Values representing measured values are to be provided in the units defined in Table 5.

Table 4: Unit of Measure

Value Semantics	Unit of Measure
Power	Megawatts (MW)
Energy	Megawatt-hours (MWh)
Reactance	MegaVar (MVar)
Frequency	Cycles per Second (Hz)
Voltage	Kilovolts (kV)
Current	Amps (A)
Temperature	Degrees Celsius (°C)

ESKOM COPYRIGHT PROTECTED

3.5.5 Data Quality

All analogue values shall have the server data quality forwarded with the value. Indication / state changes shall be time stamped by the server and include the Data Item quality.

3.6 Data Elements

This section discusses the data exchange conventions applicable to Data Items and Data Sets for data that is shared between the NCC and a RCC.

Most Data Items in TEMSE are created by the data engineer during modelling. One type is created by the TEMSE validation program: Component Status Data Items.

3.6.1 TEMSE Data Items

There are three types of data attributes to be modelled for each data items:

- 1) Data Items – Type: To configure the type, attributes, size, and special purpose flags of the data items
- 2) Data Items – Source: To configure the source, and the scope (for ICCP) of the data items. This display also allows inserting a short description, optional names, devices information, and data semantics conversions on a data item basis
- 3) Data Item Permissions / Network Type: To configure the Read, Write, Execute permissions, and network type (in which format the data item will be sent/received) of each data item for each remote

For performance, the shorter an ICCP data item name, the better ICCP names are exchanged over the network when data is sent by exception, which is the most common way of transferring data. Characters allowed in an ICCP data item name is restricted to the upper/lower letters, the ten digits and 2 special characters (dollar sign and underscore) without embedded blanks. If the device is Select Before Operate, name length must not exceed 24 characters because TEMSE has to build a names such as: <ICCP device name>_success (concatenation of up to 8 characters). For Direct Operate devices the maximum length is 32.

Data Item names follow a convention indicating the data point as defined for the electrical bay with the optional inclusion of the point address in the RTU configuration file:

sssss_<electrical bay measurement>_<point address>

Where:

- 1) **sssss** is the 5 letter substation identifier
- 2) **<electrical bay measurement>** is the definition of the electrical bay element which include the device name, voltage level and measurement
- 3) **<point address>** the optional source address at the RTU as per the configuration file

IEC point address: **cccc_nn**

- 1) **cccc** is the common address for the RTU,
- 2) **nnnn** is the IEC address as per the configuration file

DNP point address: **cccc_nn_xxxxx**

- 1) **cccc** is the common address for the RTU
- 2) **nn** is the group address as per the configuration file
- 3) **xxxx** is the bit nr as per the configuration file

The definition of the ICCP names for the **<electrical bay measurement>** is shown in Table 5.

Table 5: Data Item Bay Naming Convention

Bay Type	Proposed ICCP Data Item Naming Convention
Lines	SSSSS_TTTTTTN_LVL_IDENT_<point_address> Where : - SSSSS is the origin station up to 5 letters id - TTTTTT is the target station up to 5 letters id - N is the line number - LVL is the voltage level - IDENT is the 2 to 4 letters of the point/analogue identifier (CB, <isolator>, MW, MVAR, MVA, PF, KV, HZ, AMP, MWH, DEG)
Transformers	SSSSS_TRFRNN_LVL_IDENT_<point_address> Where : - SSSSS is the origin station up to 5 letters id - TRFR is the transformer up to 5 letters id - NN is the transformer number - LVL is the voltage level (at node of measurement) - IDENT is the 2 to 4 letters of the point/analogue identifier (CB, <isolator>, MW, MVAR, MVA, PF, KV, HZ, AMP, MWH, DEG)
Generator, SVC, Shunt, Cap and Reactor	SSSSS_EEEX_LVL_IDENT_<point_address> Where : - SSSSS is the origin station up to 5 letters id - LVL is the voltage level - EEE is type of equipment (GEN, CAP, RX, CX, SVC) - X is the equipment unit number - IDENT is the 2 to 4 letters of the point/analogue identifier (CB, <isolator>, MW, MVAR, MVA, PF, KV, HZ, AMP, MWH, DEG)
Bus Selection and Couplers	SSSSS_BBNN_EEEEX_LVL_IDENT_<point_address> Where : - SSSSS is the origin station up to 5 letters id - LVL is the voltage level - BBNN is the busbar identifier - EEEE is type of equipment (SECT, CPLR) - X is the equipment unit number - IDENT is the 2 to 4 letters of the point/analogue identifier (CB, <isolator>, MW, MVAR, MVA, PF, KV, HZ, AMP, MWH, DEG)
Control Area / Utility Information	Data_Ident_UUUU Where : UUUU is the name of the utility

The definition for the <isolator> shall be:

- 1) **IS0** is used if there is a single busbar
- 2) **IS1** is the busbar1 isolator
- 3) **IS2** is the busbar2 isolator
- 4) **ISW** is the west bus section isolator
- 5) **ISE** is the east bus section isolator
- 6) **ISN** is the north bus section isolator

ESKOM COPYRIGHT PROTECTED

- 7) **ISS** is the south section isolator
- 8) **ISL** is the line isolator
- 9) **ISB** is the bypass isolator
- 10) **IST** is the transfer busbar isolator

Table 6: Data Item General Naming Convention

Data Type	Proposed ICCP Data Item Naming Convention
Meteorological Data	SSSSS_TTT_PPPPN_IDENT_<point_address> Where : SSSSS is the origin station 5 letters id TTT is the MET for meteorological data PPPP is the measurement locations namely MAST N = 1 or 2 is the line number when there are two lines LVL is the voltage level IDENT is the 2 to 4 letter <meteorological data> identifier where acceptable <meteorological data> are: WS is Wind Speed WD is Wind direction ATMP is Air temperature APRS is Air pressure ADEN is Air density SOLR is Solar irradiation HUM is Humidity)
Generator Modes	SSSSS_EEEX_LVL_IDENT_<point_address> Where : SSSSS is the origin station 5 letters id LVL is the voltage level EEE is type of equipment (GEN) X is the equipment unit number IDENT is the 2 to 4 letter <mode> identifier (where acceptable <modes> are: CTMO is Curtailment Mode PFMO is Power factor mode VCMO is Voltage control mode QCMO is Q control mode SPMW is Curtailment set-point)

No provision has been made for alarm indications.

3.6.2 IEC ASDU Address Range

Eskom ASDU information objects address values:

Table 7: Eskom ASDU Information Object Address Range

IEC ASDU	Information Object Address Range
Single point information	1 to 10 000
Single point information	10 001 to 15 000
Single point information	15 001 to 20 000

ESKOM COPYRIGHT PROTECTED

IEC ASDU	Information Object Address Range
Measured Value	20 001 to 25 000
Integrated Totals	25 001 to 30 000
Single Command	30 001 to 35 000
Double Command	35 001 to 40 000
Bitstring of 32 bit command (Lamp Drive Outputs)	40 001 to 43 000
Bitstring of 32 bit command (AGC Outputs)	43 001 to 45 000
Set-point command (Meter Drive Outputs)	45 000 to X
Set-point command (Set-point Outputs)	(X + 1) to 65 355

An address of less than five characters will be zero padded in front for the Data Item names.

3.6.3 Data Item Type

TEMSE categories data items as:

- 1) SCADA, fixed length: Integers, Reals, and Statuses used for Conformance Blocks 1 and 2.
- 2) Non-SCADA, variable length: Message Objects (Conformance Block 4) and Control Messages (used to forward Conformance Block 5 operations - command and setpoint – between remotes).

Data item type defines the format of the data (Real, Integer, Status, etc.) and associated qualifiers (Quality, Time Stamp, Change of Value Counter)

To avoid the loss of precision because of a Real versus Integer mismatch preference should be given to interchange Real values

3.6.4 Data Item Source

The Data Items Source specifies where a Data Item comes from. For TEMSE valid remotes for the National Control Centre (ENCC) will be Eskom College Test Centre / ECC (ESTC), Northern Region / Mpumalanga Operating Unit (ESMC), Southern Region / Eastern Cape Operating Unit (ESEC), Western Region / Western Cape Operating Unit (ESWC), Eastern Region / Kwazulu Natal Operating Unit (ESKC), Central Region / Gauteng Operating Unit (ESGC), North West Region / Free State Operating Unit (ESFC) and Limpopo Operating Unit (ESLC).

3.6.5 TEMSE Data Item Permission / Network Type

Data item permissions are TEMSE's translation of the access rights defined in the ICCP's Bilateral Table. There are three types of permissions: Read, Write, and Execute.

- 1) A remote site having Read permission to a data item can access it either by a direct read data value request or by putting it in a data set. In TEMSE any remote site may have Read permission although the initial implementation is to provide TEMSE with an alternative access to the RTUs
- 2) A remote site having Write permission to a data item can access it either by a direct write data value request or by putting it in a data set. In TEMSE, only the remote source of the data item may have Write permission
- 3) A remote site having Execute permission is allowed to operate the device associated with the data item. Any remote sites may have Execute permission, except the remote source of the data item (i.e. a remote site cannot have Execute and Write permissions at the same time)

The specification of the Network Type, ICCP data type, is important to avoid mismatches between the control-centres. Each data type has a particular field structure; specifying the wrong type will likely lead to conversion errors since the correct field as specified by the ICCP server will not be located in the expected position in the Data Value structure of the ICCP client. Failure to specify a valid ICCP data type will force the interface into an object-by-object query of the ICCP server, which can be time consuming at initialisation. TEMSE has the option of populating the Network Type during database validation with the type associated with the database point which will be used.

There are two types of component data items:

- 1) Topology component data items
- 2) Data Set component data items

3.6.6 Data Sets

The restrictions on the Data Set name is that it must begin with a letter and only alphanumeric characters (0-9, a-z, AZ) and \$ and _ (underscore) characters are allowed. Data Set names (32 Characters) follow a convention indicating the source and destination:

Data Sets have the form:

`Efff_dd_Ettt_sssss_rrr_yyy`

Where:

- 1) **Efff** is the control centre identifier for the server initiating the connection
- 2) **dd** is the direction of the data exchange, i.e. either from (FR) or to (TO)
- 3) **Etttt** is the control centre identifier for the server confirming the connection
- 4) **sssss** is the data set identifier number (i.e. the 5 letter substation identifier used on TEMSE or sequential number 00001 for points and 0002 for analogs)
- 5) **rrr** is a trigger to indicate if the data set reporting is periodic, reported as an exception or on request
- 6) **yyy** indicates if all data items in the data set are transmitted (ALL) or report-by -exception (RBE), when only data items which have their value or attributes changed are transmitted

TEMSE support the following triggers (**rrr**):

- 1) PER = Periodic: Data set is input/output on a periodic basis
- 2) EXC = Exception: Data set is input/output when an exception occurs (data value and/or attribute of a data item in the data set has changed). Only the last value is reported even if it has changed multiple times during the buffering time
- 3) REQ = On Request: Data set is input/output upon request
- 4) RCT = On Receipt: For output data set only. Data set is output upon receipt of its twin data set
- 5) UDT = Unsolicited Data Transfer: This is the same as trigger by exception (EXC), except that all changes occurring during the buffering time are reported. The style (**yyy**) must be RBE

If the NCC System Operator were to create Data Sets for data transfers between itself and the Central Regional / Gauteng Operating Unit the names could be as follows:

- ENCC_FR_ESGC_00001_EXC_RBE
- ENCC_FR_ESGC_00002_PER_ALL

A similar set of data sets created in the Central Regional server could have the following names:

- ESGC_TO_ENCC_00001_EXC_RBE
- ESGC_TO_ENCC_00002_PER_ALL

The reporting of all digital and analogue point changes shall be done as report-by-exception. In addition a data set for a general interrogation of the substation is recommended every 50 minutes and a data set for an update of all digital and analogue points on demand.

3.6.7 Information Message Request

The initial implementation for ICCP between NCC and the RCCs will be for SCADA functionality. However, the definition of Information Reference numbers, which are 32 bit integers, to identify the request between the control centres will have to be defined. Proposals could include that this number be broken down into 9 bytes or fields. Each byte (or combination of 2 or more bytes) can be assigned a meaning. One byte can be reserved for indicating whether the information message is a request for a specific information message object or whether it is the actual object.

3.7 Access Control

To provide access control, the ICCP servers' checks each client request to ensure that that particular client has access rights to the data or control requested. The scope limits the visibility and accessibility to the remote sites that have the data object specified in their Bilateral Table. Access control is thus provided through the use of these Bilateral Tables defined for each client/server association. Bilateral Tables provide execute, read/write, read only, or no access for each item that can be requested by a client.

Defined scopes for the TEMSE OAG are VMD (global), Domain (restricted to a single remote site), and Association (restricted to a single association with a remote site). The functionality required is clearly presented in IEC 870-6-503.

3.8 Local Implementation

The following provides a check list between data exchange partners for when a control centre implements ICCP, and joins the existing network or begins to communicate with another ICCP implementation:

- 1) Pre-defined Data Set object names are published to appropriate data exchange partners
- 2) The maximum number of associations that will be allowed is known
- 3) The maximum exchange frequency of data is agreed upon in order to avoid overloading a SCADA/EMS with data request
- 4) Data types specified as critical data
- 5) The use and specification of retry counters
- 6) The assignment of values to the Information Reference Number used by most data objects

4. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Les Fenn	Eastern Cape operating Unit SCADA Manager
Marumo Kgare	Western Cape Operating Unit SCADA Manager
Michael Rawson	Free State Operating Unit SCADA Manager
Phemelo Olifant	North West Operating Unit SCADA Manager
Robert Shandu	Mpumalanga Operating Unit SCADA Manager
Sanjiv Bandu	KwaZulu Natal Operating Unit SCADA Manager
Xolani Mkala	Gauteng Operating Unit SCADA Manager
Geoffrey Ive	Chief Engineer Professional Energy Planning

ESKOM COPYRIGHT PROTECTED

Name and surname	Designation
Ian Naicker	Chief Engineer
Marlini Sukhnandan	Chief Engineer
Rosalette Botha	Corporate Specialist System Operating
Prudence Madiba	Generation Senior Manager
Richard McCurrach	PTM&C Senior Manager
Ayanda Ndlebe	Senior Advisor for Energy Management
Tebogo Modiba	Senior Advisor for Information Systems.
Kenneth Brown	Senior Engineer Processional Engineering Support
Thendo Ramulondi	Senior Engineer Processional Engineering Support
Dave Suttan	Senior Technician Electrical
Philla Kgole	Senior Technician Engineering
Gato Buthelezi	Senior Technician Operations
Peter Henson	Senior Technician Operations
Thobekile Mkhwanazi	Senior Technician Systems Support
Alphonse Malete	Senior Technologist
Pieter Vink	Technologist Engineer

5. Revisions

Date	Rev	Compiler	Remarks
Sept 2015	2	MM Taljaard	Compiled ICCP Standard Updated signatures with bypass
March 2015	1	MM Taljaard	First issue

6. Development Team

The following people were involved in the development of this document:

- Alphonse Malete
- Geoffrey Ive
- Matthew Taljaard
- Rosalette Botha
- Thobekile Mkhwanazi

7. Acknowledgements

- Robert Shandu