TECHNICAL REPORT

IEC 60870-6-505

2002

AMENDMENT 1
2005-09

Amendment 1

Telecontrol equipment and systems –

Part 6-505: Telecontrol protocols compatible with ISO standards and ITU-T recommendations – TASE.2 User guide

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE S

For price, see current catalogue

FOREWORD

This amendment has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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

Enquiry draft	Report on voting
57/663/DTR	57/695/RVC
57/730/DTR	57/737/RVC

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

The committee has decided that the contents of this amendment and the base publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

Page 59

Insert, after subclause 20.3, the following new Annexes A, B and C.

Annex A
(informative)

Power system model exchange with TASE.2 linkage

A.1 General

This annex defines the relations between the power system model and the TASE.2 model as applied to power system model exchange.

A.2 Summary

Exchange of power system models with linkage to TASE.2 measurements is exchanged using the IEC 61970 (CIM) classes Measurement, MeasurementValue, and MeasurementValue Source.

The MeasurementValueSource class defines the control center supplying the TASE.2 data. The Name attribute is set to „CC Link“ and the pathName holds the name of the supplying control center. The MeasurementValue class specifies the TASE.2 Object ID. The aliasName attribute holds the TASE.2 Object ID, and the Name attribute holds the SCADA point name. Each MeasurementValue being supplied via TASE.2 shall also have an association to a MeasurementValueSource. Each MeasurementValue is associated with one Measurement.

A.3 Actor(s)

Name	Role description
EMS A Data Engineer	Maintains EMS A power system model. Adds TASE.2 linkage data to power system model.
EMS B Data Engineer	Maintains EMS B power system model. Makes mapping between TASE.2 Object ID in received model and measurements received via TASE.2 link.

A.4 Probable participating systems

System	Services or information provided
EMS A	Converts an internal representation of a power system model to CIM XML format and sends to EMS B. Also sends real-time TASE.2 SCADA points via an TASE.2 link to EMS B.
EMS B	Receives power system model from EMS A as a CIM XML formatted file and converts to internal model representation of EMS B. Also receives real-time measurement data from EMS A via a TASE.2 link.

A.5 Pre-conditions

a) A unique local SCADA Reference ID has been locally assigned to each measurement value by EMS A data engineer to be included in the power system model transferred from EMS A to EMS B

b) A TASE.2 link is already established and a TASE.2 Object ID has been assigned to at least some of the measurement values available for transfer to the intended receiver.

c) A CIM-compatible representation of the power system model at both EMS A and B exists.

d) A bilateral table is already established for SCADA points available at Control Center A to be received by Control Center B.

A.6 Assumptions / design considerations

A typical use of this linkage will be when regional transmission companies collect data from their local member companies. Including the TASE.2 Object ID will allow software to automatically define the TASE.2 to power system model linkage, and when used in combination with the ability of TASE.2 Clients to scan TASE.2 Servers for Object IDs, these can be mapped together to reduce the manual data definition required.

This would be performed as a background function incorporated as part of the data modeling work.

This would be an infrequent action, occurring any time major changes in the power system model and TASE.2 objects affect data exchange requirements. This is expected to be a major task at the initial set up of a system, and then as major changes occur which may be monthly or weekly.

The size of this data exchange would be a minor expansion of the existing CIM XML data exchange, and would not be considered as significant.

A.7 Normal sequence

See Table A.1.

Table A.1 – Normal sequence

Use case step	Description
Step 1	EMS A data engineer adds TASE.2 Object ID to each measurement value in the power system model that is available for transfer to EMS B. The TASE.2 Object ID shall be exactly the same as the TASE.2 Object ID that is used with the real-time data transfers via TASE.2 link. In CIM MeasurementValue class: a) store SCADA ID in MeasurementValue.name attribute; b) store TASE.2 Object ID in MeasurementValue.aliasName attribute. In CIM MeasurementValueSource class: a) store “CC LINK” in MeasurementValueSource.name to indicate data is supplied by a TASE.2 link; b) store “EMS A” in MeasurementValueSource.pathName to give specific instance of control center providing the TASE.2 data.
Step 2	EMS A converts power system model to CIM XML format and transfers file to EMS B.
Step 3	EMS B receives EMS A power system model in CIM XML format and converts to internal model format.
Step 4	EMS B Data Engineer merges the power system model from EMS A into the EMS B power system model. This requires configuring EMS B software to correlate each measurement value in the EMS A power system model and the real-time SCADA points received via the TASE.2 link. Recommendation: Using the CIM SCADA package, the MeasurementValue and MeasurementValueSource instances received from EMS A should be stored at EMS B as remote measurements. This should be done by modeling the EMS A control center as a RemoteUnit and all the MeasurementValues as RemotePoints. This requires the following mapping: a) MeasurementValueSource.name to RemoteUnit.name b) MeasurementValueSource.pathName to RemoteUnit.pathName c) MeasurementValue.name to RemotePoint.name d) MeasurementValue.aliasName to RemotePoint.aliasName

A.8 Exceptions / alternate sequences

a) A TASE.2 SCADA point is available via TASE.2 link and there is no corresponding measurement value in the CIM power system model. This will require manual intervention to update the power system model TASE.2 linkage data for that point and perhaps a resend of the model (or an incremental update if available).

b) The converse: there is a measurement value in the CIM model with an TASE.2 source and TASE.2 Object ID, but there is no real-time data received from the EMS A over the TASE.2 link for that point. The TASE.2 object is not in the bilateral table on EMS A for EMS B. This is not necessarily a problem. It is up to the EMS B, as a TASE.2 client, to request all TASE.2 SCADA points available to it from EMS A. It may require a revision to the bilateral table as well.

A.9 Post-conditions

A mapping is established at EMS B between each TASE.2 Object ID received and a measurement value in its power system model. This is needed, for example, to run power flow and state estimator applications and for displaying real-time measurement data on one-line displays.

Note that it is possible to have a complete round-trip transfer of the model from EMS A through EMS B and then back to EMS A with the RemoteUnit and RemotePoint model information added at EMS B so that EMS A can verify completeness/correctness of the transfer.

A.10 References

CPSM Minimum Data Requirements in Terms of the EPRI CIM Version 1.8 April 18, 2002 Prepared by Joe Evans and Kurt Hunter

A.11 Use case diagram

In Figure A.1, dotted lines indicate existing use cases, solid lines indicate this use case.

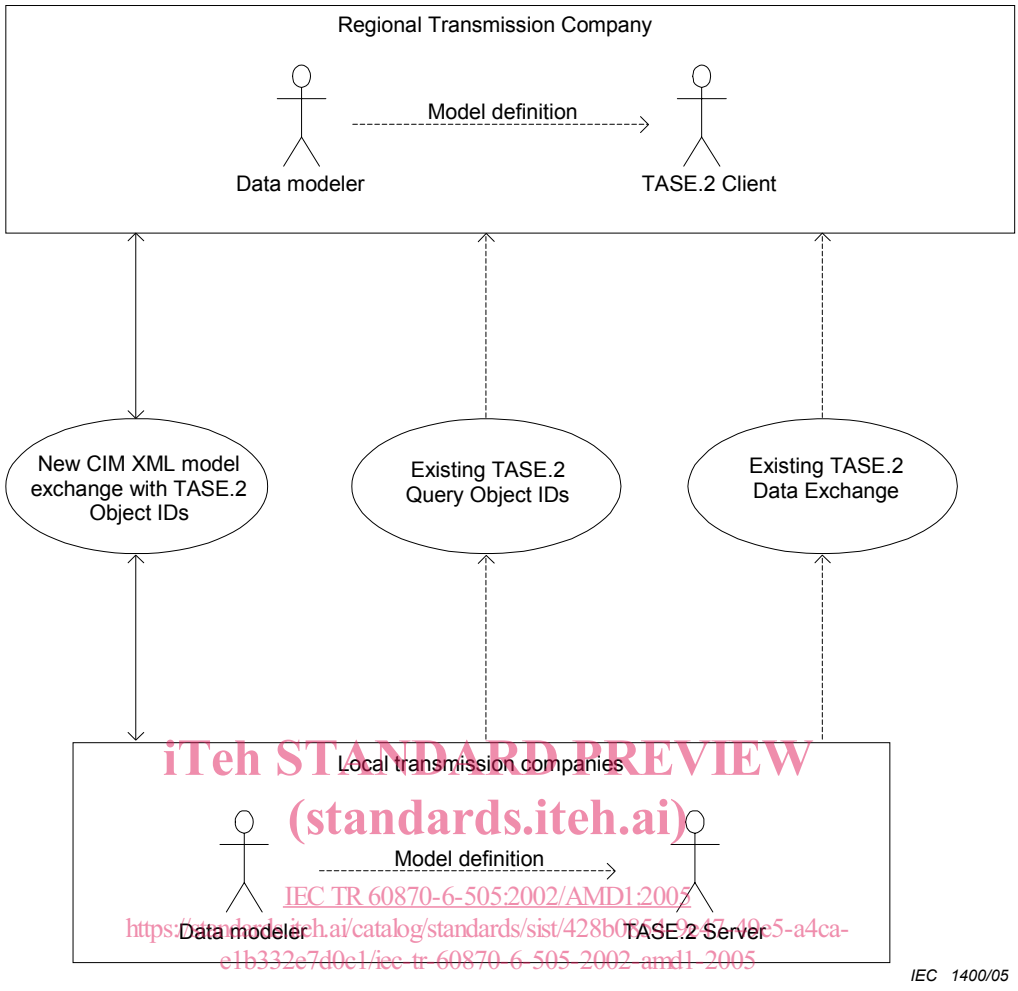

Figure A.1 – Use case diagram

Annex B
(informative)

TASE.2 security recommendations

B.1 Scope

B.1.1 General

This annex provides a set of security guidelines on the use of the following TASE.2 international standards[1]:

IEC 60870-6-503, TASE.2 Services and Protocol

IEC 60870-6-702, TASE.2 Application Profiles

IEC 60870-6-802, TASE.2 Object Models

These standards specify a method of exchanging time-critical control centre data through wide- and local-area networks using a full ISO compliant protocol stack. They contain provisions for supporting both centralized and distributed architectures. These standards include the exchange of real-time indications, control operations, time series data, scheduling and accounting information, unstructured ASCII or binary files, remote program control, and event notification.

This annex was issued to cover only the appropriate areas of security that impact the implementation and use of the TASE.2 standards. This annex is not normative and offers the end users only recommendations.

B.1.2 Intended audience

This annex is intended for a broad audience of readers from an end user trying to decide if TASE.2 is appropriate for his data transfer needs to a vendor planning to implement TASE.2, with the goal of offering a TASE.2 product. In particular, this annex should be helpful to the following:

- An end user, such as an electric utility, with the need to transfer real-time data to another utility or utilities or to another internal control centre, who is trying to evaluate which protocol is most appropriate.
- An end user who already has decided to use TASE.2 and now needs guidance in how to procure TASE.2.
- An end user that has procured TASE.2 and now is concerned about exactly how to map their actual data into TASE.2 data objects.
- An end user that is looking for conventions and answers to practical questions regarding configuring TASE.2 software and networks.
- A vendor with a project to implement the TASE.2 specification either as a project special or to offer a standard product.

---

[1] The documents referenced are TASE.2 Edition 2 versions. The following information also applies to the TASE.2 Edition 1 version of the documents, which may still be in use.

B.1.3 Organisation of annex

This annex introduces the background and security issues formulated by the IEC Technical Committee 57 Working Group 15. The remainder of the annex addresses recommended solutions to issues that are within the domain of the protocol and describes other areas that the user should evaluate which are not covered in IEC 60870-6-503, IEC 60870-6-702 and IEC 60870-6-802.

The documents referenced are TASE.2 Edition 2 versions. The following information also applies to the TASE.2 Edition 1 version of the documents, which may still be in use.

B.2 Terms and definitions

For the purposes of this annex, the following terms and definitions apply.

B.2.1
authorisation violation
entity authorised to use a system for one purpose that uses it for another unauthorised purpose

B.2.2
availability
information exchange is possible

B.2.3
bypassing controls
system flaws or security weaknesses are intentionally attacked

B.2.4
data validity
the data being provided, by the back-end systems or databases, is valid and represents the current state

B.2.5
denial of service
authorised communication flow/exchange is impeded

B.2.6
eavesdropping
information is revealed to an unauthorised person via monitoring of communication traffic

B.2.7
illegitimate use
an individual authorised for one action performs an action, control, or information retrieval, but an action is completed for which the individual is not authorised

B.2.8
indiscretion
an authorised person discloses restricted information to a non-authorised entity

B.2.9
information leakage
an unauthorised entity acquires restricted information

NOTE Typically this term is for non-eavesdropping acquisition of the information (e.g., through other means of disclosure).

B.2.10
integrity violation
information is created or modified by an unauthorised entity

B.2.11
intercept/alter
a communication packet is intercepted, modified, and then forwarded as if the modified packet were the original

NOTE This is a typical man-in-the-middle scenario.

B.2.12
masquerade
an unauthorised entity attempts to assume the identity of an authorised entity

B.2.13
replay
a communication packet is recorded and then retransmitted at an inopportune time

B.2.14
repudiation
an exchange of information occurs and one of the two parties in the exchange later denies that the exchange took place

B.2.15
spoof
this attack is a combination of one of the following threats: eavesdropping; information leakage; integrity violation; or intercept/alter and masquerade

B.3 Abbreviations

For the purpose of this technical report annex, the following abbreviations apply.

ACSE	Association Control Service Element
API	Application Program Interface
EPRI	Electric Power Research Institute
FDIS	Final Draft International Standard
ICCP	Inter-Control Centre Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
MMS	Manufacturing Messaging Specification
QOS	Quality of Service
TASE	Telecontrol Application Service Element, IEC's designation of an international standard protocol for utility data exchanges
TASE.2	TASE version based on the ICCP protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UCA	Utility Communications Architecture
UDP	User Datagram Protocol
VCC	Virtual Control Centre
VMD	Virtual Manufacturing Device

B.4 TASE.2 security issues

Table B.1 lists the top 10+ security issues associated with TASE.2, these issues were supplied by IEC Technical Committee 57 Working Group 15. This list may not be a complete set of issues and are listed by priority. IEC Technical Committee 57 Working Group 07 has included in the first column the evaluation of the issue as to whether or not it is considered a TASE.2 protocol issue or an issue that is circumstantial to the protocol.

Table B.1 – TASE.2 security issues

TASE.2 Issue	Priority	Concern when using	
		Non-secure profile	Entire set secure profile recommendations
Yes	1	Bypassing controls	Bypassing controls
Yes	2a	Integrity violation	Indiscretion
No	2b	Authorisation violation	Illegitimate use
No	3	Indiscretion	Information leakage
Yes	4	Intercept/alter	Availability
No	5	Illegitimate use	Data validity
No	6	Information leakage	Performance
Yes	7	Spoof	Local security administration and procedures
Yes	8	Masquerade	Remote security procedures
Yes	9	Availability (e.g. denial of service)	Certificate and authentication management
Yes	10	Eavesdropping (e.g. data confidentiality)	Certificate authority privacy and security procedures

B.5 Evaluation of TASE.2 security issues

B.5.1 General

Evaluations of the issues are based upon a node to node protocol impact. Security issues involving the interaction between control centre applications and TASE.2 (clients or servers), so called “end to end” issues are beyond the scope of this document. For further clarification see Figure 6 of IEC 60870-6-503:2002.

B.5.2 Bypassing control

Transport layer authentication, node to node, is a TASE.2 security protocol issue, TLS addresses this issue and is recommended. Intrusion detection is not a TASE.2 security protocol issue.

Strong application authentication may be a TASE.2 security protocol issue. A clear definition of the security issues is still under consideration.

B.5.3 Integrity violation

Integrity Violation is a TASE.2 protocol security issue. TLS with an appropriate hashing algorithm that is encrypted with the message addresses this issue and is recommended.

B.5.4 Authorisation violation

Not a TASE.2 specific issue. An entity authorised to use the system for one purpose and uses it for an unauthorised purpose is not a protocol issue.

B.5.5 Indiscretion

Not a TASE.2 specific issue. Authorised person disclosures are not a protocol issue.

B.5.6 Intercept or alter

TASE.2 security issue. TLS with an appropriate hashing algorithm that is encrypted with the message addresses this issue and is recommended.

B.5.7 Illegitimate use

Not a TASE.2 specific issue. Policies, procedures, and audits are not protocol issues.

B.5.8 Information leakage

Not a TASE.2 specific issue. Policies, procedures, and audits are not protocol issues. IEC Technical Committee 57 Working Group 07 does not believe performance is an issue with information leakage.

B.5.9 Spoof

TASE.2 security issue. TLS with an appropriate hashing algorithm that is encrypted with the message addresses this issue and is recommended.

B.5.10 Masquerade

TASE.2 protocol security issue. TLS with an appropriate hashing algorithm that is encrypted with the message addresses this issue and is recommended.

B.5.11 Availability

TASE.2 protocol security issue. Currently implemented using TASE.2 parameters limiting client performance impacts on server. Other denial of service issues outside of TASE.2 (which may require intrusion detection systems) are out of scope of IEC 60870-6-505.

B.5.12 Eavesdropping

TASE.2 protocol security issue. TLS with an appropriate hashing algorithm that is encrypted with the message addresses this issue and is recommended.