

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**

© IEC 2005 Droits de reproduction réservés — Copyright - all rights reserved

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- withdrawn,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 MeasurementValueSource.

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	<p>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.</p> <p>In CIM MeasurementValue class:</p> <ul style="list-style-type: none"> a) store SCADA ID in MeasurementValue.name attribute; b) store TASE.2 Object ID in MeasurementValue.aliasName attribute. <p>In CIM MeasurementValueSource class:</p> <ul style="list-style-type: none"> 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	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> 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.

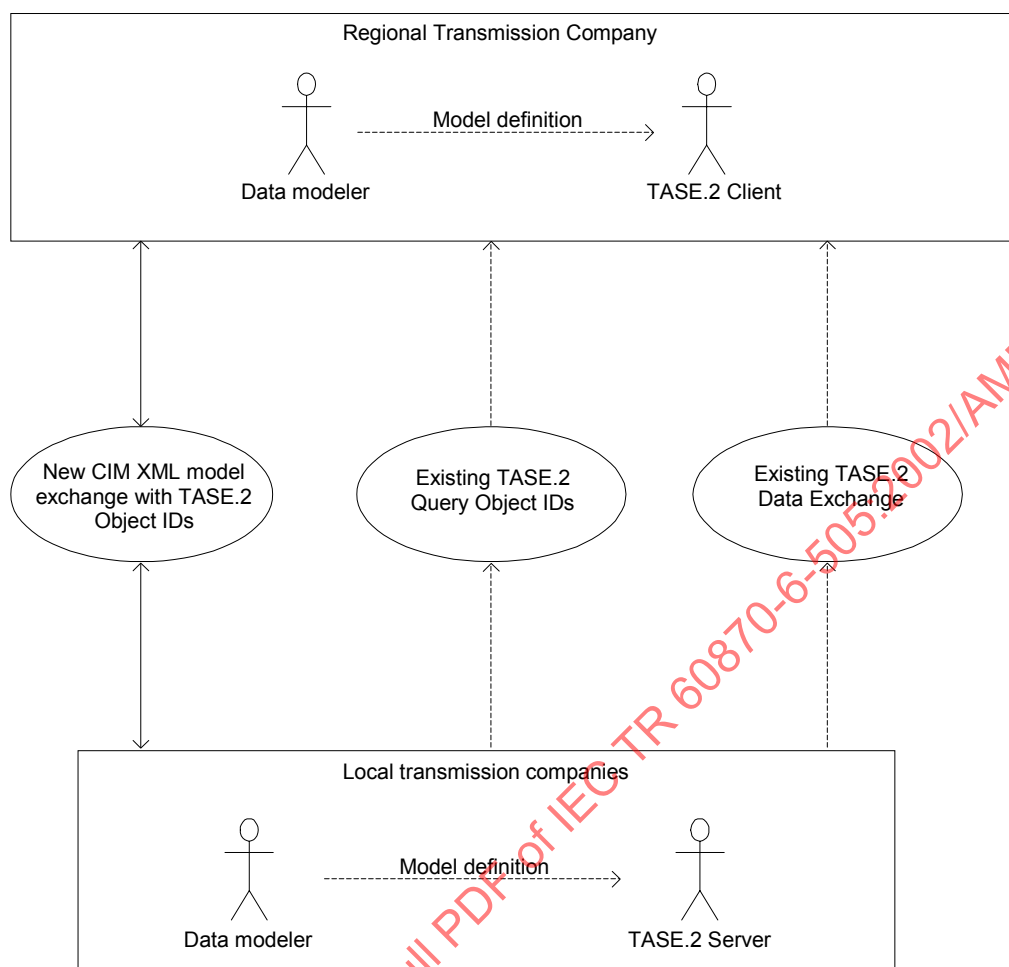
Note that it is possible to have a complete round-trip transfer of the model from EMS A through EMS B and then back to EMS A with the RemoteUnit and RemotePoint model information added at EMS B so that EMS A can verify completeness/correctness of the transfer.

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.



IEC 1400/05

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 standards¹:

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.

B.6 Recommended solutions

TASE.2 Issue	Priority	Concern when using	Recommended solution
Yes	1	Bypassing controls	Implementation of TLS with proper security policies is recommended
Yes	2a	Integrity violation	Implementation of TLS with proper security policies is recommended
No	2b	Authorisation violation	No recommendation
No	3	Indiscretion	No recommendation
Yes	4	Intercept/alter	Implementation of TLS with proper security policies is recommended
No	5	Illegitimate use	No recommendation
No	6	Information leakage	No recommendation
Yes	7	Spoof	Implementation of TLS with proper security policies is recommended
Yes	8	Masquerade	Implementation of TLS with proper security policies is recommended
Yes	9	Availability (e.g. denial of service)	No recommendation
Yes	10	Eavesdropping (e.g. data confidentiality)	Implementation of TLS with proper security policies is recommended

B.7 Security management

The TASE.2 specifications do not specify a security policy or a specific digital certificate managing and maintaining processes. This is left as another “local implementation issue.”

The following areas need to be addressed by the user’s requirements:

- Know, on an association-by-association basis, which links are operating in a secure or non-secure mode.
- Allow simultaneous inter-operability with existing non-secure associations and new secure associations on an association-by-association basis.
- Allow or prevent, by prior mutual agreement, an association to be unilaterally taken out of (or returned to) secure mode for debug purposes on an association-by-association basis.
- Allow new associations to be commissioned in secure or non-secure mode without requiring a complete restart of the TASE.2 application.
- Allow certificate negotiation rates to be set on an association-by-association basis.
- Multiple digital certificates shall be supported.

B.8 Bilateral table issues

Bilateral table issues are covered in IEC 60870-6-503, IEC 60870-6-802 and IEC 60870-6-505. The bilateral table concept is used for data access control.

B.9 User interface issues

The TASE.2 specifications do not specify a user interface for managing and maintaining TASE.2. This is left as another “local implementation issue.” Each vendor is free to choose an appropriate interface. As such, user interface security issues are not addressed.

The following areas may need a user interface:

- Displaying of associations as either being secured on unsecured.
- Operator notification of transition of secure link to unsecured state.
- Operator notification on the expiration of the digital certificate.
- Operator notification on the future expiration of the digital certificate.

B.10 Network profiles

Figure B.1 depicts the standard TASE.2 network profile while Figure B.2 depicts the secure TASE.2 network profile.

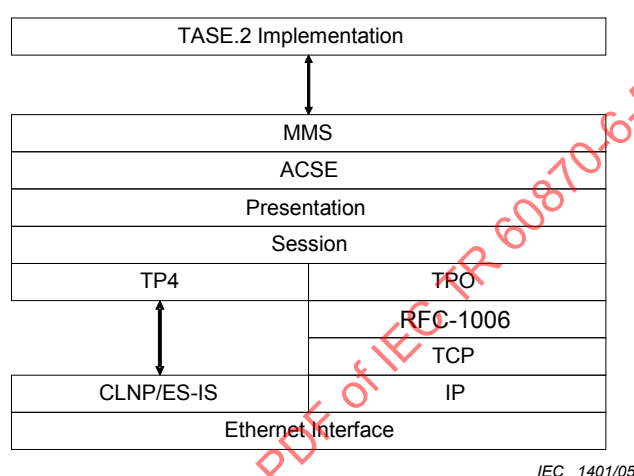


Figure B.1 – TASE.2 standard profile

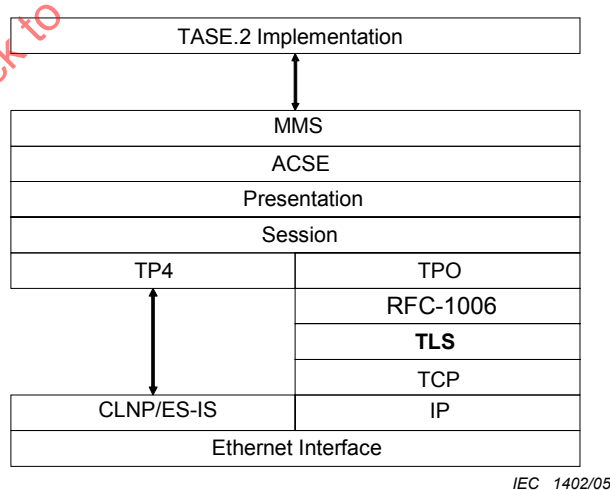


Figure B.2 – TASE.2 secure profile

B.11 Bibliography

ICCP (TASE.2) Security Enhancements Volume 1, EPRI, Palo Alto, CA 2002. 1001642.

SSL and TLS Essentials – Securing the Web, Wiley Computer Publishing, John Wiley & Sons, Inc., NY, NY. Stephen A. Thomas

Request For Comment 2246, The TLS Protocol Version 1.0 January 1999, Internet Engineering Task Force

IECNORM.COM : Click to view the full PDF of IEC TR 60870-6-505:2002/AMD1:2005

Annex C (informative)

TASE.2 User's guide implementation recommendations

C.1 General

This Annex covers the following four implementation issues.

- 1) generator raise/lower pulse support;
- 2) use of change of value counter;
- 3) quality code encoding rules;
- 4) TASE.2 association and dataset alarming.

C.2 Generator raise/lower pulse support

The existing TASE.2 data objects do not provide a general generator raise/lower pulse capability. This function is highly hardware-dependent and is not common in new generator governing units delivered today. The following implementation is modeled from a typical RTU protocol implementation and assumes that the TASE.2 server would configure a dataset to transfer the following values as a periodic group. The purpose is to create the capability to pass the dataset as a periodic automatic generation control function.

To implement a generic generator raise/lower capability, the following four values shall be able to be passed between control centres.

- 1) A *control code* discrete value indicating the control function to perform. The applicability of this code will depend on the type of hardware used in the end device.
- 2) A *count* discrete value indicating the number of times that the control operation should be performed in succession.
- 3) The *on-time* discrete value specifies the amount of time the digital “on” output is to be turned on. This value may not apply to all control types.
- 4) The *off-time* discrete value specifies the amount of time the digital “off” output is to be turned on. This value may not apply to all control types.

The following recommendation does not require modification to existing TASE.2 implementations or implementation of extensions. The purpose of using this approach is to not negatively impact existing systems.

To implement the recommended general pulse raise/lower service, a TASE.2 server periodic dataset should be configured with four named variables to represent the control code, count, on-time, and off-time described above. All data objects in this dataset should be data type **Data_Discrete integer (width {32})**. The clients may then establish a periodic data set containing the required four elements. The actual utilization of these four values will be a local implementation issue: the purpose of this recommendation is to standardize on the data and values to be passed to allow interoperability of this function.

C.3 Use of change of value counter

Interoperability issues may occur if the change of value counter is not implemented consistently across implementations. The COVCounter is defined as

“The COV Counter attribute specifies the number of times the value (attribute PointRealValue, PointStateValue, or PointDiscreteValue) of the IndicationPoint has changed. It is incremented each time the owner sets a new value for the IndicationPoint”.

COV Counter needs to be specifically defined as a running increment counter. If not, the server would have to have multiple instances of the COV Counter, one for each client-defined association. This is unmanageable by a server since it does not know in advance how many instances will be needed, whether those instances will be demand, RBE, periodic, etc.

The running incremented value is reported with the IndicationPoint. A value of 0 is reported when the running count rolls over. On an association failure and restart, the running incremental count is NOT reset. The server should simply keep updating the count as changes occur on the data point. When the association is re-established, the current incremental count is sent to the client. The client can use that (and the previously received value from before the association was lost) to calculate any MCD (Momentary Change Detect) events if desired.

In the case of a restart of the server software where the incremental count is lost, a zero (0) is sent to the client. The client needs to be able to handle receiving a value of 0 at any time.

C.4 Quality code encoding rules

C.4.1 General

The TASE.2 protocol provides a standard format for exchanging data between control centers or utilities. In the TASE.2 standard, information for a point from a SCADA system is stored in a data value object. If agreed upon and configured on both the sending and the receiving TASE.2 sites, the quality condition information of a point may be sent along with the point value as quality attributes of the data value object, as defined in the TASE.2 standard. The SCADA quality conditions need to be translated or converted into the TASE.2 quality attributes prior to sending the data out via the TASE.2 protocol. It is important for the receiving TASE.2 site to be able to understand the quality conditions of a point, as it existed on the sending site from the TASE.2 quality attributes of the received data value object. If the mapping between the SCADA quality conditions and the TASE.2 quality attributes is not clearly understood by the receiving site, the receiving site may not be able to interpret the received TASE.2 quality attributes correctly.

C.4.2 Translation guidelines

The objective of C.4 is to provide suggested guidelines for translating SCADA quality conditions of a point to TASE.2 quality attributes. It is the hope and ultimate goal that the translation will be performed consistently as recommended in all TASE.2 systems.

These guidelines may also apply to TASE.2 vendors and control centre staff that develop the interfaces between SCADA systems and an independent TASE.2 server, for systems that do not have the TASE.2 software integrated as part of the SCADA system.

Please note that this annex provides guidelines only for the translation of SCADA quality conditions to TASE.2 quality attributes but not for vice versa. The translation of TASE.2 quality attributes to SCADA quality codes is not addressed in this document for the following reasons:

- The quality code implementation varies greatly from system to system (especially between systems supplied from different vendors).
- The translation of TASE.2 quality attributes to SCADA quality codes in a system has no effects on external systems (system on the other end of a TASE.2 association) other than the local system. It is a local implementation issue.

In practice, the setting of internal SCADA quality codes should be such that if the value is re-sent via TASE.2, the TASE.2 quality attributes on the resend will be identical to the original sending.

C.4.3 Recommended translation processing

C.4.3.1 General

The following are the quality attributes (of a data value object) as defined in the TASE.2 standard:

1) Validity – this attribute may have one of the following values:

- VALID
- HELD (Not used in this document)
- SUSPECT
- NOT VALID

2) Current Source – this attribute may have one of the following values:

- TELEMETERED
- ENTERED
- CALCULATED
- ESTIMATED

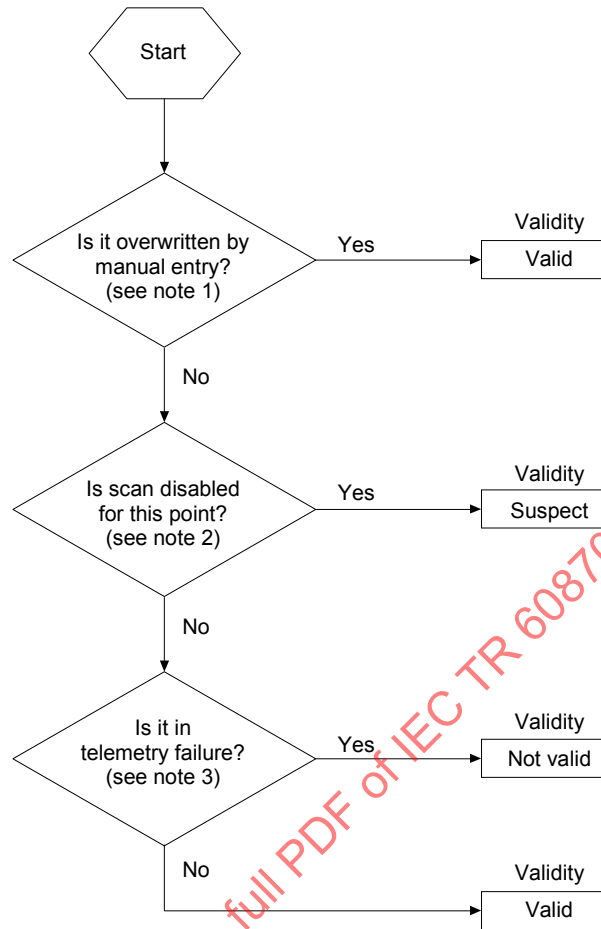
3) Normal Value – this attribute may have one of the following values:

- NORMAL
- ABNORMAL

The recommended algorithms for setting the above three TASE.2 quality attributes based on the SCADA conditions of a point are provided in the flow diagrams. In each case, notes referenced in the diagram explain the operational meaning of each quality determination.

C.4.3.2 Translation processing validity

See Figure C.1.



IEC 1403/05

NOTE 1 Explicit operator entry of a value or implicit acceptance of an existing value when subsequent telemetry will be blocked is to be considered a manual override.

NOTE 2 Scan disabling for the point refers to the condition in which the point is taken off scan individually and manually by the dispatcher/operator. A point is not considered to be scan-disabled if the RTU to which the point belongs is taken off scan or if the scan group to which the point belongs is taken off scan.

NOTE 3 A point is considered to be in telemetry failure if one or more of the following conditions is satisfied:

- The RTU to which the point belongs is taken off scan.
- The scan group (in a RTU) to which the point belongs is taken off scan.
- The value of the point is outside the range of the reasonable limits.
- Inability to scan the point or the RTU successfully by the EMS system (or its front-end processor) such as having communication problems or errors with the RTU or problems with the modem or communication line.

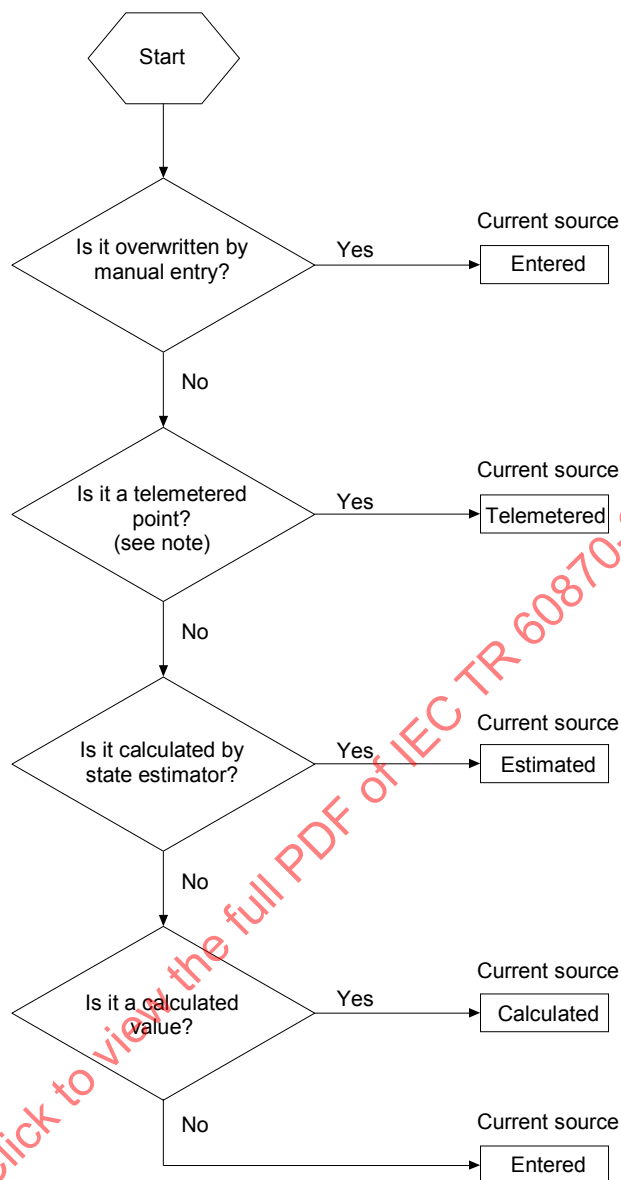
Figure C.1 – Validity processing

If the point is a calculated point, its derived quality is to be the lowest quality of its constituent points. The ranking of qualities is (highest to lowest):

- 1) VALID
- 2) SUSPECT
- 3) NOT VALID

C.4.3.3 Translation processing current source

See Figure C.2.



IEC 1404/05

NOTE A point is considered to be a telemetered point if its value is normally derived from a field device such as a RTU or a programmable controller, or if an alternate data source is substituted from a similar device. A point is considered ENTERED if manually entered by an operator or if it remains the default value specified at database definition time (also known as a pseudo point).

Figure C.2 – Current source processing