

Power systems management and associated information exchange — Data and communications security —

Part 6: Security for IEC 61850

ICS 33.200

National foreword

This Draft for Development is the UK implementation of IEC/TS 62351-6:2007.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application can be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the international organization responsible for its conversion to an international standard. A review of this publication will be initiated not later than 3 years after its publication by the international organization so that a decision can be taken on its status. Notification of the start of the review period will be made in an announcement in the appropriate issue of *Update Standards*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into an international Standard, to extend the life of the Technical Specification or to withdraw it. Comments should be sent to the Secretary of the responsible BSI Technical Committee at British Standards House, 389 Chiswick High Road, London W4 4AL.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 31 July 2007

© BSI 2007

ISBN 978 0 580 56448 2

Amendments issued since publication

Amd. No.	Date	Comments

TECHNICAL SPECIFICATION

IEC TS 62351-6

First edition
2007-06

**Power systems management and
associated information exchange –
Data and communications security –**

**Part 6:
Security for IEC 61850**



Reference number
IEC/TS 62351-6:2007(E)

CONTENTS

1	Scope and object.....	3
1.1	Scope.....	3
1.2	Object	3
2	Normative references	3
3	Definitions	4
4	Security issues addressed by this specification	4
4.1	Operational issues affecting choice of security options	4
4.2	Security threats countered.....	5
4.3	Attack methods countered	5
5	Correlation of IEC 61850 parts and IEC 62351 parts	5
5.1	IEC 61850 security for profiles using ISO 9506 (MMS)	5
5.1.1	General	5
5.1.2	Control centre to substation.....	5
5.1.3	Substation communications	5
5.2	IEC 61850 security for profiles using VLAN IDs	6
6	IEC 61850 security for SNTP	6
7	IEC 61850 security for profiles using VLAN technologies.....	6
7.1	Overview of VLAN usage and IEC 61850 (informative)	6
7.2	Extended PDU.....	6
7.2.1	General format of extended PDU	6
7.2.2	Format of extension octets	7
7.2.3	Substation configuration language.....	10
8	Conformance.....	11
8.1	General conformance	11
8.2	Conformance for implementations claiming ISO 9506 profile security	12
8.3	Conformance for implementations claiming VLAN profile security.....	12
8.4	Conformance for implementations claiming SNTP profile security.....	13
	Bibliography.....	14
	Figure 1 – General format of extended PDU.....	6
	Figure 2 – SCL extensions for certificates.....	10
	Figure 3 – Extension to AccessPoint SCL definition	11
	Table 1 – Scope of application to standards.....	3
	Table 2 – Extract from IEC 61850-9-2 (informative)	9
	Table 3 – Conformance table	12
	Table 4 – PICS for ISO 9506 profile	12
	Table 5 – PICS for VLAN profiles	12
	Table 6 – PICS for SNTP profiles.....	13

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 6: Security for IEC 61850

1 Scope and object

1.1 Scope

This part of IEC 62351 specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the standard IEC 61850. This specification applies to at least those protocols listed in Table 1.

Table 1 – Scope of application to standards

Number	Name
IEC 61850-8-1	Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
IEC 61850-9-2	Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3
IEC 61850-6	Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs

1.2 Object

The initial audience for this specification is intended to be the members of the working groups developing or making use of the protocols listed in Table 1. For the measures described in this specification to take effect, they must be accepted and referenced by the specifications for the protocols themselves. This document is written to enable that process.

The subsequent audience for this specification is intended to be the developers of products that implement these protocols.

Portions of this specification may also be of use to managers and executives in order to understand the purpose and requirements of the work.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850 (all parts), *Communication networks and systems in substations*

IEC 61850-6, *Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-8-1, *Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

IEC 61850-9-1, *Communication networks and systems in substations – Part 9-1: Specific Communication Service Mapping (SCSM) – Sampled values over serial unidirectional multidrop point to point link*

IEC 61850-9-2, *Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

IEC 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS*

ISO 9506 (all parts), *Industrial automation systems – Manufacturing Message Specification*

ISO/IEC 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

ISO/IEC 13239, *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures*

IEEE Std. 802.1Q-2003, *Virtual Bridged Local Area Networks*

RFC 2030, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*

RFC 2313, *PKCS #1: RSA Encryption Version 1.5*

RFC 3447, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*

RFC 4634, *US Secure Hash Algorithms (SHA and HMAC-SHA)*

3 Definitions

For the purposes of this document, the terms and definitions contained in IEC 62351-2 apply.

4 Security issues addressed by this specification

4.1 Operational issues affecting choice of security options

For applications using GOOSE and IEC 61850-9-2 and requiring 4 ms response times, multicast configurations and low CPU overhead, encryption is not recommended. Instead, the communication path selection process (e.g. the fact that GOOSE and SMV are supposed to be restricted to a logical substation LAN) shall be used to provide confidentiality for information exchanges. However, this specification does define a mechanism for allowing confidentiality for applications where the 4 ms delivery criterion is not a concern.

NOTE The actual performance characteristics of an implementation claiming conformance to this technical specification is outside the scope of this specification.