Chinastandards.org

ICS 29.240.01
CCS F 21

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 25320.6-2023

Replacing GB/Z 25320.6-2011

Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850

电力系统管理及其信息交换 数据和通信安全 第6部分：IEC 61850的安全

(English Translation)

Issued on: December 28, 2023 **Implemented on: July 1, 2024**

Issued by: State Administration for Market Regulation, China National Standardization Administration

Preview: page 1 of 5 shown, 25 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-6-2023

Chinastandards.org

Table of Contents

Preface
Introduction
1 Scope and purpose
1.1 Scope
1.2 Namespace names and versions
1.3 Code component release
2 Normative references
3 Terms, definitions and abbreviations
3.1 Terms and definitions
3.2 Abbreviations
4 Security issues addressed by this document
4.1 Operational issues affecting security option selection
4.2 Security threats to deal with
4.3 Attack methods to deal with
5 Relevance between parts of IEC 61850 and various parts of IEC 62351
5.1 Overview
5.2 IEC 61850-8-1 Client/Server Communication Protocol Set
5.3 IEC 61850 security using VLANID specification
5.4 IEC 61850-8-2 Protocol set for client/server communication
5.5 Publisher ID 6 for client/server services
6 Multicast Association Protocol
6.1 Overview
6.2 Anti-replay attacks (ReplayProtection)
7 SNTP Security
8 Introduction to Layer 2 Security of IEC 61850-8-1 GOOSE and IEC 61850-9-2 Sampled Values
8.1 Ethertype overview (informative)
8.2 Extended PDU
9 Substation Configuration Language Extension
9.1 Service capabilities
9.2 Security-enabled publishing
9.3 Use of Simulation

Preview: page 2 of 5 shown, 25 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-6-2023

Chinastandards.org

10 Extensions for LGOS and LSVS

11 Consistency

11.1 Conformance overview

11.2 Declaration of conformance to IEC 61850-8-1 ISO 9506 (application protocol set) security implementation

11.3 Declaring the consistency of VLAN protocol set security implementations

11.4 Declaring the consistency of the security implementation of the SNTP protocol suite

Reference

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents" Drafting:

This document is Part 6 of GB/T (Z) 25320 "Power System Management and Information Exchange Data and Communication Security", GB/T (Z) 25320 the following sections have been published:

---Part 1: Introduction to communication network and system security issues;

---Part 2: Terminology;

---Part 3: Communication network and system security including TCP/IP protocol set;

---Part 4: Protocol set including MMS;

---Part 5: Safety of GB/T 18657 and other standards and their derivatives;

---Part 6: Safety of IEC 61850;

---Part 7: Data Object Model for Network and System Management (NSM);

---Part 11: Security of XML files;

---Part 100-1: Conformance test cases for IEC TS62351-5 and IEC TS60870-5-7;

---Part 100-3: Conformance test cases for IEC 62351-3 and secure communication extensions including the TCP/IP protocol set:

This document replaces GB/Z 25320.6-2011 "Power System Management and Information Exchange Data and Communication Security Part 6:

"Safety of IEC 61850", compared with GB/Z 25320.6-2011, in addition to structural adjustments and editorial changes, the main technical changes are as follows:

a) Changed the scope (see Chapter 1, Chapter 1 of the:2011 edition);

b) Changed the overview of the relevance of IEC 61850 part to IEC 62351 part (see 5.1,

Preview: page 3 of 5 shown, 25 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-6-2023

Chinastandards.org

5:1:1 of the:2011 edition);

c) Added terms, definitions and abbreviations (see Chapter 3);

d) Change the response time of GOOSE and SV from less than 4ms to less than 3ms (see 4.1,:2011 version of 4:1);

e) Added IEC 61850-8-2 client/server communication protocol set (see 5.4);

f) Added publisher ID for client/server services (see 5.5);

g) Added multicast association protocol (see Chapter 6);

h) Added MAC (see 8.2:2:2);

i) Added version, this version is 1 (see 8.2:3:2);

j) Added the current key time (see 8.2:3:3);

k) The next key time is added (see 8.2:3:4);

l) Added initialization vector (see 8.2:3:5);

m) Added key ID (see 8.2:3:6);

n) Added substation configuration language extension (see Chapter 9);

o) Substation Configuration Language (SCL) has been deleted (see 7.2:3 of the:2011 version);

p) Added extensions for LGOS and LSVS (see Chapter 10);

q) Added support for IEC 61850-8-2 and support for the security consistency of routable GOOSE and SV (see 11.1 Table 5);

r) Added TLS using ACSE certification (see Table 7 in 11:1);

s) Added IEC 61850-8-1L2GOOSE safety conformance (see 11.1 Table 9);

t) Added IEC 61850-8-1L2SV safety conformance (see 11.1 Table 10);

u) Added IEC 61850-8-1L2GOOSE routable security consistency (see 11.1 Table 11);

v) Added IEC 61850-8-1L2SV routable safety conformance (see 11.1 Table 12):

This document is equivalent to IEC 62351-6:2020 "Power system management and its information exchange data and communication security Part 6:

Safety of IEC 61850":

Please note that some content in this document may be subject to patents: The publisher of this document assumes no responsibility for identifying patents:

Preview: page 4 of 5 shown, 25 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-6-2023

Introduction

GB/T (Z) 25320 "Power System Management and Information Exchange Data and Communication Security", which aims to reduce communication and computing as much as possible in order to avoid the harm caused by malicious attacks in the computer network to the data and communication security of the power system, it is necessary to improve the communication protocols at all levels used in the power system:

discuss security vulnerabilities and improve the security management of power system information infrastructure: It is planned to consist of the following parts:

---Part 1: Introduction to communication network and system security issues: The purpose is to introduce other parts of GB/T (Z)25320 it mainly introduces readers to all aspects of information security applied to power system operation:

---Part 2: Terminology: The purpose is to introduce the key terms used in GB/T (Z) 25320:

---Part 3: Communication Network and System Security includes the TCP/IP protocol set: The purpose is to specify how transmission is limited to specifications of the messages, processes and algorithms of layer security protocols, and provide security protection for TCP/IP-based protocols so that these protocols can Suitable for IEC TC57 telecontrol environment:

---Part 4: Contains the protocol set of MMS: The purpose is to stipulate the manufacturing message specifications based on GB/T 16720 (ISO 9506) the process, protocol extensions and algorithms for security protection of MMS applications:

---Part 5: Security of GB/T 18657 and other standards and their derivatives: The purpose is to define the application configuration file (a-profile) Secure communication mechanism that specifies the secure operation of all protocols based on or derived from IEC 60870-5 Protected messages, processes and algorithms:

---Part 6: Safety of IEC 61850: The purpose is to specify the operation of all protocols based on or derived from IEC 61850:

Messages, processes and algorithms for security protection:

---Part 7: Data Object Model for Network and System Management (NSM): The purpose is to define the characteristics unique to power system operation:

A data object model for network and systems management:

---Part 8: Role-based access control: The purpose is to provide role-based access control for power system management:

---Part 9: Network security key management of power system equipment: The purpose is to manage by specifying or restricting the keys to be used Options to define requirements and

Preview: page 5 of 5 shown, 25 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-6-2023