DIN EN IEC 62351-6 (VDE 0112-351-6)

DIN

Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation" bekannt gegeben worden.

VDE

ICS 33.200; 35.030; 35.240.50

Einsprüche bis 2019-06-19

Entwurf

Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 6: Sicherheit für IEC 61850 (IEC 57/2033/CDV:2018); Deutsche und Englische Fassung prEN IEC 62351-6:2018

Power systems management and associated information exchange –
Data and communications security –
Part 6: Security for IEC 61850
(IEC 57/2033/CDV:2018);
German and English version prEN IEC 62351-6:2018

Gestion des systèmes de puissance et échanges d'informations associés –
Sécurité des communications et des données –
Partie 6: Sécurité pour l'IEC 61850
(IEC 57/2033/CDV:2018);
Version allemande et anglaise prEN IEC 62351-6:2018

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-04-19 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 64 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

AVA Documents Document Sharing Hub

Full document details: E DIN EN IEC 62351-6:2019-05

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ... .

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments prEN IEC 62351-6:2018 „Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 6: Sicherheit für IEC 61850“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 57/2033/CDV:2018 „Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850“ unverändert in den Entwurf prEN IEC 62351-6:2018 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom TC 57 „Power systems management and associated information exchange“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für dieses Dokument ist das nationale Arbeitsgremium K 952 „Netzleittechnik“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Dies ist eine Überarbeitung der IEC TS 62351-6 zu einer internationalen Norm. Dieser Vorgang führt dazu, dass das Dokument von einer Technischen Spezifikation zu einem internationalen Norm Edition 1 wird.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62351-6:2019-05

Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 6: Sicherheit für IEC 61850

Inhalt

Seite

1 Anwendungsbereich ... 3
2 Normative Verweisungen ... 3
3 Begriffe ... 5
4 In dieser Spezifikation behandelte Sicherheitsthemen ... 5
4.1 Betriebliche Aspekte mit Einfluss auf die Wahl der Sicherheitsoptionen ... 5
4.2 Sicherheitsbedrohungen, denen entgegengewirkt wird ... 5
4.3 Angriffsverfahren, denen entgegengewirkt wird ... 5
5 Zusammenhang zwischen Teilen von IEC 61850 und Teilen von IEC 62351 ... 6
5.1 IEC 61850-8-1 Profil für die Client/Server-Kommunikation ... 6
5.2 IEC 61850-8-2 für die Client/Server-Kommunikation ... 7
5.3 Nutzung der Ursprungskennung für Client/Server-Dienste ... 7
6 Multicast-Assoziationsprotokolle ... 8
6.1 Allgemeines ... 8
6.2 Wiedergabeschutz ... 8
6.2.1 GOOSE-Wiedergabeschutz ... 8
6.2.2 Sampled-Value-Wiedergabeschutz ... 13
7 Sicherheit für SNTP ... 18
8 Layer-2-Sicherheit für Profile für IEC 61850-8-1 GOOSE und IEC 61850-9-2 Sampled Value ... 18
8.1 EtherTyp-Übersicht (informativ) ... 18
2 Normative Verweisungen ... 3
3 Begriffe ... 5
4 In dieser Spezifikation behandelte Sicherheitsthemen ... 5
4.1 Betriebliche Aspekte mit Einfluss auf die Wahl der Sicherheitsoptionen ... 5
4.2 Sicherheitsbedrohungen, denen entgegengewirkt wird ... 5
4.3 Angriffsverfahren, denen entgegengewirkt wird ... 5
5 Zusammenhang zwischen Teilen von IEC 61850 und Teilen von IEC 62351 ... 6
5.1 IEC 61850-8-1 Profil für die Client/Server-Kommunikation ... 6
5.2 IEC 61850-8-2 für die Client/Server-Kommunikation ... 7
5.3 Nutzung der Ursprungskennung für Client/Server-Dienste ... 7
6 Multicast-Assoziationsprotokolle ... 8
6.1 Allgemeines ... 8
6.2 Wiedergabeschutz ... 8
6.2.1 GOOSE-Wiedergabeschutz ... 8
6.2.2 Sampled-Value-Wiedergabeschutz ... 13
7 Sicherheit für SNTP ... 18
8 Layer-2-Sicherheit für Profile für IEC 61850-8-1 GOOSE und IEC 61850-9-2 Sampled Value ... 18
8.1 EtherTyp-Übersicht (informativ) ... 18

AVA Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62351-6:2019-05

Seite

9.3.1 GOOSE ... 26
9.3.2 SMV ... 26
10 Konformität ... 26
10.1 Allgemeine Konformität ... 26
10.2 Für Implementierungen, die die Konformität mit IEC 61850-8-1 Client/Server beanspruchen ... 27
10.2.1 IEC 62351-4 TLS-Konformität für die ACSE-Authentifizierung ... 27
10.2.2 IEC 62351-4 E2E-Sicherheit ... 28
10.3 Für Implementierungen, die die Konformität mit IEC 61850-8-2 Client/Server beanspruchen ... 28
10.4 Für Implementierungen, die die Konformität mit der GOOSE-Sicherheit beanspruchen ... 29
10.5 Für Implementierungen, die die Konformität mit IEC 61850-8-1 SV-Sicherheit beanspruchen ... 29
10.6 Für Implementierungen, die die Konformität mit der SNTP-Profilsicherheit beanspruchen ... 30
Literaturhinweise ... 31

Bilder

Bild 1 – Wiedergabeschutz-Zustandsautomat für GOOSE ... 10
Bild 2 – Wiedergabeschutz-Zustandsautomat für SMV ... 16
Bild 3 – Allgemeines Format der erweiterten PDU ... 19
Bild 4 – Erweiterungslänge ... 19

Tabellen

Tabelle 1 – Anwendungsbereich der Normen ... 3
Tabelle 2 – Konfigurationsoptionen für das IEC 61850-8-1 Sicherheitsprofil ... 6
Tabelle 3 – Auszug aus IEC 61850-9-2 (informativ) ... 13
Tabelle 4 – Zulässige Werte für Berechnungen des MAC-Signaturwerts ... 22
Tabelle 5 – KonformitätsTabelle für Sicherheit nach IEC 61850 ... 27
Tabelle 6 – PICS für IEC 61850-8-1 Client/Server ... 27
Tabelle 7 – PICS für TLS IEC 61850-8-1 Client/Server unter Verwendung der ACSE-Authentifizierung ... 28
Tabelle 8 – PICS für TLS IEC 61850-8-1 Client/Server E2E-Sicherheit ... 28
Tabelle 9 – PICS für IEC 61850-8-2 Client/Server ... 28
Tabelle 10 – PICS für IEC 61850-8-1 GOOSE-Sicherheit ... 29
Tabelle 11 – PICS für Layer 2 IEC 61850-8-1 GOOSE-Sicherheit ... 29
Tabelle 12 – PICS für die Sicherheit routbarer GOOSE nach IEC 61850-8-1 ... 29
Tabelle 13 – PICS für Layer 2 IEC 61850 SV-Sicherheit ... 29
Tabelle 14 – PICS für Layer 2 IEC 61850-8-1 SV-Sicherheit ... 30
Tabelle 15 – PICS für die Sicherheit routbarer SV nach IEC 61850-8-1 ... 30
Tabelle 16 – PICS für SNTP-Profile ... 30

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

1 Anwendungsbereich

Dieser Teil der IEC 62351 legt Nachrichten, Verfahren und Algorithmen für die Sicherung des Betriebs aller Protokolle vor, die auf der Norm IEC 61850 basieren oder davon abgeleitet sind. Diese Spezifikation gilt mindestens für die in Tabelle 1 aufgeführten Protokolle.

Tabelle 1 – Anwendungsbereich der Normen

Nummer	Name
IEC 61850-8-1	Communication networks and systems for power utility automation – 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 61850-8-2	Communication networks and systems for power utility automation - Part 8-2: Specific communication service mapping (SCSM) - Mapping to Extensible Messaging Presence Protocol (XMPP)
IEC 61850-9-2	Communication networks and systems for power utility automation – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3
IEC 61850-6	Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs

Diese Spezifikation wendet sich zunächst an die Mitglieder der Arbeitsgruppen, die die in Dieser Teil der IEC 62351 legt Nachrichten, Verfahren und Algorithmen für die Sicherung des Betriebs aller Protokolle vor, die auf der Norm IEC 61850 basieren oder davon abgeleitet sind. Diese Spezifikation gilt mindestens für die in Tabelle 1 aufgeführten Protokolle entwickeln und verwenden. Damit die Maßnahmen, die in dieser Spezifikation beschrieben werden, ihre Wirkung entfalten können, müssen sie durch die Spezifikationen für die Protokolle selbst akzeptiert und in Bezug genommen werden. Dieses Dokument wird verfasst, um diesen Prozess zu ermöglichen.

Diese Spezifikation wendet sich als Nächstes an die Entwickler von Produkten, die diese Protokolle implementieren.

Teile dieser Spezifikation können außerdem für Geschäftsführer und Führungskräfte von Nutzen sein, die den Zweck und die Anforderungen der Arbeit nachvollziehen wollen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

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

IEC 61850-6:2017, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-7-3:2017, *Communication networks and systems for power utility automation – Part 7-3: Basic Communication structure – Common Data Classes*

IEC 61850-8-1:2017, *Communication networks and systems for power utility automation – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

AVA Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

~~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*~~

Grund für die Entfernung: 61850 ED 2.1 hat Unicast SV entfernt..

IEC 61850-9-2:2017, *Communication networks and systems for power utility automation – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

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

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

Grund für die Entfernung: Absichtlich alle Referenzen auf ISO 9506 entfernen und Referenzen/Nomenklatur für 62351-4, IEC 61850-8-1 und IEC 61850-8-2 verwenden.

IEC 62351-4:2017, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS*

IED 62351-9:2017, *Power systems management and associated information exchange – Data and communications security – Part 9: Key Management*

~~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*~~

Grund für die Entfernung: Absichtlich alle Verweise darauf entfernen und Referenzen/Nomenklatur für 62351-4, IEC 61850-8-1 und IEC 61850-8-2 verwenden.

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

~~IEEE Std. 802.1Q-2012, *Virtual Bridged Local Area Networks*~~

Grund für die Entfernung: Absichtlich alle Verweise darauf entfernen und Referenzen/Nomenklatur für 62351-4, IEC 61850-8-1 und IEC 61850-8-2 verwenden. Ohnehin falsche Referenz.

RFC 5208, *X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification.*

Restricted to SNTP profile only.

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

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

RFC 6234, *US Secure Hash Algorithms (SHA and HMAC-SHA)*

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62351-6:2019-05

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 62351-2 und IEC 61850-2.

SCL Substation Configuration Language

ICT IED Configuration Tool

IED Intelligent Electronic Device

4 In dieser Spezifikation behandelte Sicherheitsthemen

4.1 Betriebliche Aspekte mit Einfluss auf die Wahl der Sicherheitsoptionen

Für Anwendungen, die Layer 2 IEC 61850-8-1 GOOSE und Layer 2 IEC 61850-9-2 Sampled Value nutzen und Reaktionszeiten von 4 ms, Multicast-Konfigurationen und eine geringe Prozessorbelastung erfordern, wird die Verschlüsselung nicht empfohlen. Stattdessen muss der Kommunikationsweg-Auswahlprozess (d. h. die Tatsache, dass Layer 2 GOOSE und SV auf ein logisches Stations-LAN beschränkt werden sollen) angewendet werden, um die Vertraulichkeit des Informationsaustauschs sicherzustellen. Diese Spezifikation legt jedoch keinen Mechanismus zur Sicherstellung der Vertraulichkeit von Anwendungen fest, bei denen das Lieferkriterium von 4 ms kein Problem ist.

ANMERKUNG Die tatsächlichen Kenngrößen einer Implementierung, die sich auf die Konformität mit dieser technischen Spezifikation beruft, liegen nicht im Anwendungsbereich dieser Spezifikation.

Diese Spezifikation beschreibt mit Ausnahme der Vertraulichkeit einen Mechanismus, der die Co-Existenz sicherer und nicht sicherer PDU erlaubt.

4.2 Sicherheitsbedrohungen, denen entgegengewirkt wird

Siehe IEC 62351-1 für eine Diskussion der Sicherheitsbedrohungen und Angriffsverfahren.

Falls keine Verschlüsselung angewendet wird, umfassen die spezifischen Bedrohungen in diesem Teil, denen entgegengewirkt wird:

- die unbefugte Modifikation (Manipulation) von Informationen durch die Authentifizierung von Nachrichten auf Nachrichtenebene.

Falls eine Verschlüsselung angewendet wird, umfassen die spezifischen Bedrohungen in diesem Teil, denen entgegengewirkt wird:

- den unbefugten Zugriff auf Informationen durch Authentifizierung auf Nachrichtenebene und Verschlüsselung der Nachrichten;
- die unbefugte Modifikation (Manipulation) oder den Diebstahl von Informationen durch die Authentifizierung auf Nachrichtenebene und Verschlüsselung der Nachrichten.
- Der Offenlegung von Informationen wird entgegengewirkt.

4.3 Angriffsverfahren, denen entgegengewirkt wird

Den folgenden Sicherheitsangriffsverfahren soll durch die entsprechende Implementierung der in diesem Dokument enthaltenen Spezifikationen/Empfehlungen entgegengewirkt werden:

- Janusangriff: Dieser Bedrohung wird durch Benutzung eines Mechanismus mit Nachrichten-authentifizierungscode, der in diesem Dokument festgelegt ist, entgegengewirkt;
- Manipulationserkennung/Nachrichtenintegrität: Diesen Bedrohungen wird durch einen Algorithmus zur Erstellung des in diesem Dokument beschriebenen Authentifizierungsmechanismus entgegen-gewirkt;

AVA Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

- Wiedergabe: Dieser Bedrohung wird durch die Verwendung spezieller Verarbeitungszustands-automaten wie in IEC 62351-4 und diesem Dokument beschrieben entgegengewirkt.

5 Zusammenhang zwischen Teilen von IEC 61850 und Teilen von IEC 62351

Es bestehen vier Interaktionsebenen zwischen den Teilen von IEC 62351 und von IEC 61850. Diese Teile betreffen:

- Die Kommunikationsprofilsicherheit in Bezug auf:
  - IEC 61850-8-1 Anwendungsprofil für die Client/Server-Kommunikation
  - IEC 61850-8-2 Anwendungsprofil für die Client/Server-Kommunikation
  - IEC 61850-8-1 Layer 2 T-Profil für GOOSE/GSE
  - IEC 61850-8-1 Layer 2 T-Profil für Multicast Sampled Values
  - IEC 61850-8-1 Layer 3 Routbare GOOSE und Sampled Values
- Erforderliche Konfigurationserweiterungen für die betreffenden Anwendungs- und Transportkommunikationsprofile. Diese Erweiterungen würden sich auf IEC 61850-6 auswirken.
- Objektdefinitionen in Bezug auf die Sicherheit und Identifizierung, die bei Laufzeit offengelegt werden, als Teil der Objektzuordnungen nach IEC 61850-8-1 und IEC 61850-8-2.
- Die Anbindung von Ursprungskennungswerten an authentifizierte Partner für Client/Server-Dienste.

Der Anwendungsbereich dieser Spezifikation umfasst Sicherheitsspezifikationen zur Anwendung innerhalb eines elektronischen Sicherheitsbereichs (en: Electronic Security Perimeter) (ESP) und zwischen ESP.

5.1 IEC 61850-8-1 Profil für die Client/Server-Kommunikation

Implementierungen von IEC 61850, die für sich die Konformität mit dieser Spezifikation in Anspruch nehmen und die Unterstützung des IEC 61850-8-1 A-Profils für die Client/Server-Kommunikation erklären, müssen den ACSE-Authentifizierungsmechanismus und TLS nach IEC 62351-4 implementieren.

Optional kann die komplette Anwendungssicherheitsebene nach IEC 62351-4 unterstützt werden.

Implementierungen, die für sich die Konformität in Anspruch nehmen, müssen TLS 1.2 unterstützen. Die Anwendung von TLS 1.0 und TLS 1.1 sollte nicht unterstützt werden, da bekannte Sicherheitsschwachstellen bestehen.

Implementierungen, die die Konformität mit diesem Abschnitt beanspruchen, müssen so konfiguriert werden können, dass sie die Kombinationen aus Authentifizierung und TLS-Konfigurierbarkeit nach Tabelle 2 unterstützen.

Tabelle 2 – Konfigurationsoptionen für das IEC 61850-8-1 Sicherheitsprofil

	Authentifizierung	TLS	Unterstützung
Nicht sicher	Keine	Keine	Verbindlich
Für die Anwendung über VPN oder die Kommunikation zwischen ESP	Ja	Keine	Verbindlich
Nicht zulässig	Keine	Ja	Ausgeschlossen
Sicher	Ja	Ja	Verbindlich

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62351-6:2019-05

Implementierungen, die die Konformität mit diesem Abschnitt beanspruchen, müssen zur nicht sicheren Kombination zurückkehren, wenn keine gültigen privaten X.509-Zertifikate in der lokalen Konfiguration verfügbar sind.

5.2 IEC 61850-8-2 für die Client/Server-Kommunikation

Implementierungen von IEC 61850, die für sich die Konformität mit dieser Spezifikation in Anspruch nehmen und die Unterstützung des IEC 61850-8-2 A-Profils für die Client/Server-Kommunikation erklären, müssen den kompletten Sicherheitsmechanismus nach IEC 62351-4 implementieren.

Da IEC 61850-8-2 ACSE nicht unterstützt, wird der Sicherheitsmechanismus der ACSE-Authentifizierung nach IEC 62351-4 weder implementiert noch unterstützt.

Darüber hinaus nutzt IEC 61850-8-2 ein aus XMPP bestehendes T-Profil, das wiederum TLS steuert. Die in IEC 62351-4 spezifizierten Sicherheitsmechanismen und Verschlüsselungs-Suiten liegen daher nicht im Anwendungsbereich von IEC 61850-8-2.

5.3 Nutzung der Ursprungskennung für Client/Server-Dienste

IEC 61850-7-3 definierte mehrere Common Data Classes (CDC) und Dienst-Tracking-Funktionen, die explizit die Fähigkeit, Informationen über den Absender der Kontrolle oder des Dienstes zu liefern, definieren. Der tatsächliche Wert der initiierenden Instanz in IEC 61850-8-1 und IEC 61850-8-2 ist die Ursprungskennung und ein 64-Achtbit-Achtbitstring.

Die Anwendung einer starken zertifikatbasierten Authentifizierung und Sicherheit bietet einen Mechanismus für die Lieferung maßgebender Informationen in Bezug auf den Urheber. Die Größenbeschränkung der Ursprungskennung ist jedoch nicht groß genug, um die Exposition des Emittenten und der Seriennummer zu gewährleisten. Aus diesem Grund werden Implementierungen, die die Konformität mit dieser Norm beanspruchen, den CDC nach IEC 61850-7-3 ein weiteres folgendes Datenattribut hinzufügen: CST,BTS, UTS, LTS, GTS, MTS, NTS und STS.

Das Datenattribut muss als certIssuer bezeichnet und vom Attributtyp Unicode255 sein. Die funktionelle Beschränkung muss Sr sein und das Datenattribut muss am Ende der aktuellen Tracking-CDC nach IEC 61850-7-3 hinzugefügt werden.

Die Verwendung des Wertes des certIssuer-Datenattributs ist wie folgt:

- Der Wert muss eine Verkettung der Namenswert-Sequenz sein, die gegebenenfalls im Urheberfeld (en: Issuer) enthalten ist. Wenn die Sequenz mehr als einen Namen enthält, muss das „\"-Zeichen als Verkettungs-Token genutzt werden. Der Längenwert muss null (0) betragen, wenn die Client-Assoziation nicht authentifiziert ist.
- Der Wert muss x.509 Urhebername (en: Issuer Name) für eine authentifizierte Client-Assoziation entsprechen.
- Wenn ein verketteter Wert mehr als 255 Zeichen hat, muss er auf 255 Zeichen begrenzt werden.
- Wenn die Client-Assoziation nicht durch die Anwendung von Zertifikaten authentifiziert wurde, muss die Länge von certIssuer null (0) betragen und der Wert muss daher NULL sein. Alle Achtbit-Bytes in dem Wert müssen auf 0 initialisiert werden.

Implementierungen, die die Konformität mit dieser Norm beanspruchen, müssen darüber hinaus das Datenattribut der Ursprungskennung wie folgt nutzen:

- Wenn der certIssuer-Wert nicht NULL ist, muss der Wert der X.509-Zertifikat-Seriennummer für den Wert der Client-Assoziationen, die durch ein Zertifikat authentifiziert wurden, verwendet werden. Eine Zertifikat-Seriennummer ist ein codierter ganzzahliger positiver Wert. Der codierte Wert muss in den Ursprungskennungswert ohne den Tag oder die Länge kopiert werden.
- Wenn der certIssuer-Wert NULL ist, darf der Wert der Ursprungskennung „unbekannt" mit „u" als signifikantestem Achtbit-Byte des Werts sein. Andere Werte sind eine lokale Funktion.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

6 Multicast-Assoziationsprotokolle

6.1 Allgemeines

IEC 61850-8-1 und IEC 61850-9-2 legen zwei verschiedene Anwendungsprotokolle fest, die das Multicast-Assoziationsmodell nach IEC 61850 nutzen. Diese sind GSE (z. B. GOOSE) und Multicast Sampled Values. Diese Anwendungsprotokolle werden über zwei verschiedene T-Profil-Zuordnungen zugeordnet.

Die festgelegten T-Profile bieten eine Layer-2- und routbare Zuordnung des Anwendungsprotokolls. Die Kombination aus A-Profilen und T-Profilen wird allgemein als Layer 2 oder routbar (z. B. Layer 2 GOOSE oder routbares GOOSE) bezeichnet. Diese Norm legt gemeinsame Sicherheitsverhaltensweisen ungeachtet des T-Profils und der spezifischen Sicherheitsprotokoll-Erweiterungen für die Layer-2-T-Profile fest.

Dieser Abschnitt legt die erwarteten Verhaltensweisen für den Wiedergabeschutz für GOOSE und Multicast Sampled Values ungeachtet des verwendeten T-Profils fest.

6.2 Wiedergabeschutz

Der Wiedergabeschutz kann für GOOSE- und Sampled-Value-A-Profile mit oder ohne Sicherheitserweiterungen implementiert werden. Die in den folgenden Abschnitten festgelegten Wiedergabeschutz-Algorithmen richten sich an Subscriber, die die Konformität mit diesem Teil beanspruchen, sodass der Wiedergabeschutz ungeachtet der Sicherheit der veröffentlichten GOOSE- oder Sampled-Value-APDU implementiert werden muss. Der Wiedergabeschutz-Algorithmus wird durch den Subscriber implementiert.

6.2.1 GOOSE-Wiedergabeschutz

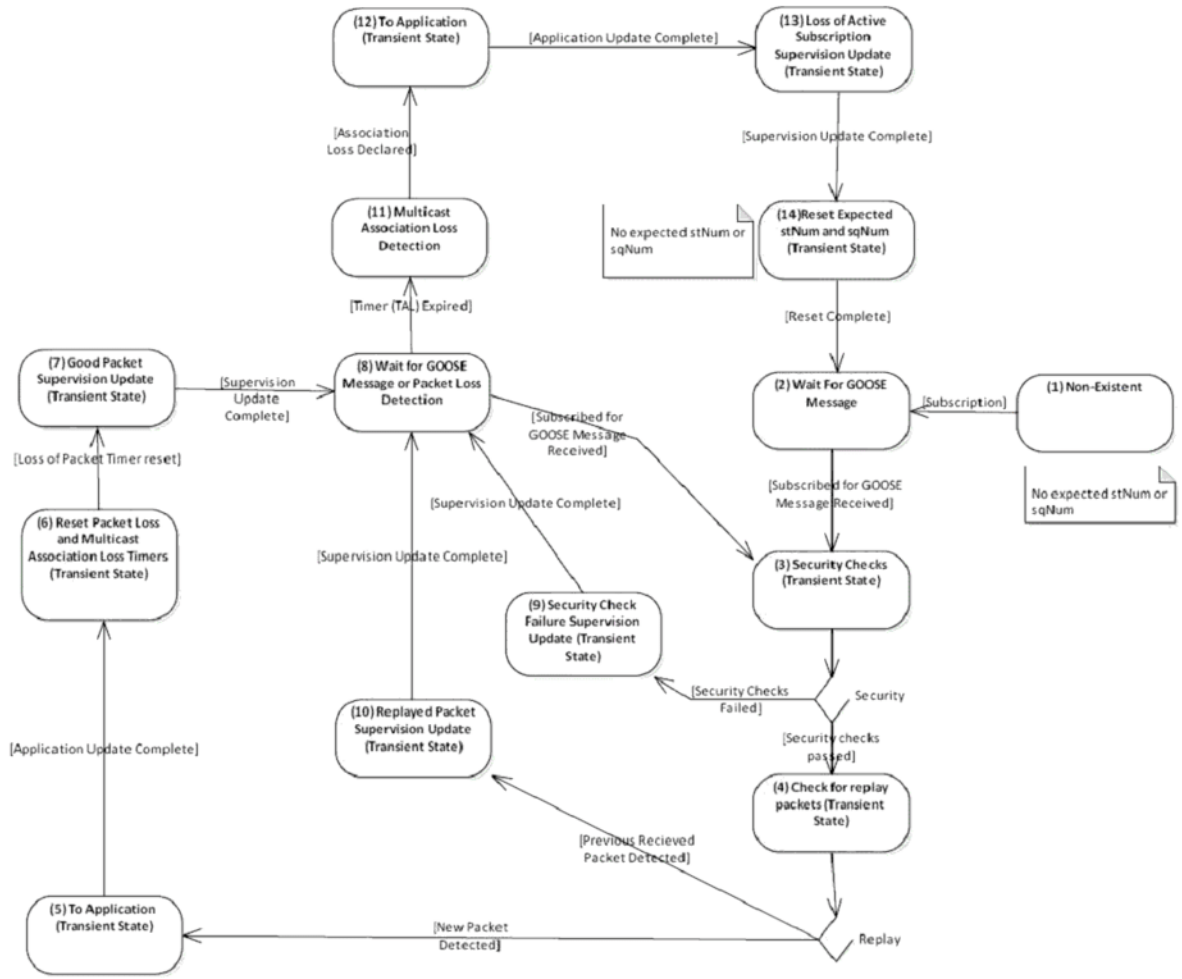
6.2.1.1 Allgemeines

Der übliche GOOSE-Subscriber-Zustandsautomat in IEC 61850-8-1 beschreibt nicht die Zustandsübertragung im Fall des Empfangs von Störungszustandszahlen (stNum) oder Sequenznummern (SqNum).

Implementierungen, die die Konformität mit dieser Norm beanspruchen, müssen den in Bild 1 gezeigten Zustandsautomaten implementieren. Zusätzliche Sicherheits- und Wiedergabeprüfungen dürfen implementiert werden.

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62351-6:2019-05



Englisch	Deutsch
(12) To Application (Transient State)	(12) Zur Anwendung (Übergangszustand)
[Application Update Complete]	[Aktualisierung der Anwendung abgeschlossen]
(13) Loss of Active Subscription Supervision Update (Transient State)	(13) Verlust der Aktualisierung der aktiven Abonnement-Überwachung (Übergangszustand)
[Association Loss Declared]	[Assoziationsverlust angegeben]
[Supervision Update Complete]	[Überwachungsaktualisierung abgeschlossen]
(11) Multicast Association Loss Detection	(11) Multicast-Assoziationsverlust erkannt
No expected stNum or sqNum	Kein stNum oder sqNum erwartet
(14) Reset Expected stNum and sqNum (Transient State)	(14) Rücksetzung erwartet für stNum und sqNum (Übergangszustand)
[Timer (TAL) Expired]	[Timer (TAL) abgelaufen]
[Reset Complete]	[Rücksetzung abgeschlossen]
(7) Good Packet Supervision Update (Transient State)	(7) Gute Paket-Überwachungsaktualisierung (Übergangszustand)
(8) Wait for GOOSE Message or Packet Loss Detection	(8) Warten auf GOOSE-Nachricht oder Paketverlust-Erkennung
[Subscribed for Goose Message Received]	[Abonnierte GOOSE-Nachricht erhalten]
(2) Wait for GOOSE Message	(2) Auf GOOSE-Nachricht warten
[Subscription]	[Abonnement]
(1) Non-Existent	(1) Nicht existent

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

Englisch	Deutsch
[Loss of Packet Timer reset]	[Verlust der Paket-Timer-Rücksetzung]
[Subscribed for GOOSE Message Received]	[Abonnierte GOOSE-Nachricht erhalten]
N expected stNum or sqNum	N erwartete stNum oder sqNum
(6) Reset Packet Loss and Multicast Association Loss Timers (Transient State)	(6) Rücksetzung-Paketverlust und Multicast-Assoziationsverlust Timer (Übergangszustand)
(3) Security Checks (Transient State)	(3) Sicherheitsprüfungen (Übergangszustand)
(9) Security Check Failure Supervision Update (Transient State)	(9) Sicherheitsprüfung Ausfall der Überwachungs-Aktualisierung (Übergangszustand)
[Security Checks Failed]	[Sicherheitsprüfungen fehlgeschlagen]
Security	Sicherheit
[Application Update Complete]	[Aktualisierung der Anwendung abgeschlossen]
(10) Replayed Packet Supervision Update (Transient State)	(10) Paketwiedergabe-Überwachungs-Aktualisierung (Übergangszustand)
[Security Checks passed]	[Sicherheitsprüfungen bestanden]
[Previous Received Packet Detected]	[zuvor erhaltenes Paket erkannt]
(4) Check for replay packets (Transient State)	(4) Prüfung auf Wiedergabe-Pakete (Übergangszustand)
(5) To Application (Transient State)	(5) Zur Anwendung (Übergangszustand)
[New Packet Detected]	[neues Paket erkannt]
Replay	Wiederholung

Bild 1 – Wiedergabeschutz-Zustandsautomat für GOOSE

Bild 1 ist für GOOSE-Nachrichten relevant, für die der Subscriber über ein aktives Abonnement verfügt, das manuell oder durch SCL und einen ICT konfiguriert werden kann. Implementierungen, die die Konformität mit diesem Abschnitt beanspruchen, müssen mindestens die folgenden internen Zustandsautomaten-Variablen haben: die zuletzt erhaltene stNum (lastRcvStNum), die zuletzt erhaltene sqNum (lastRcvSqNum), den zuletzt erhaltenen Zeitstempel (lastRcvT) und einen internen Time Allowed to Live (intTAL)-Wert. Die Zustände und ihre Übergänge sind wie folgt festgelegt:

(1) Der „Nicht vorhanden"-Zustand (en: Non-Existent) ist der Zustand, in dem kein GOOSE-Abonnement besteht.

(2) Bei der Aktivierung des Abonnements (z. B. Einschalten oder Konfiguration des Abonnements) setzt der Zustandsautomat intern lastRcvStNum, lastRcvSqNum, lastRcvT und intTAL auf ungültig, da keine GOOSE-Nachricht erhalten wurde, und der Zustandsautomat wechselt in den Zustand „auf GOOSE-Nachricht warten".

Bei Erhalt der abonnierten GOOSE-Nachricht muss der Subscriber in den Sicherheitsprüfungs-zustand (en: Security Checks) (Schritt 3) wechseln.

(3) Die Verarbeitung des Security-Checks-Zustands wird in Abschnitt 6.2.1.2 beschrieben.

Werden die Sicherheitsprüfungen bestanden, muss der Zustandsautomat zur Prüfung der wieder-gegebenen Pakete wechseln (Schritt 4).

Wenn die Sicherheitsprüfungen fehlschlagen, muss der Zustandsautomat in den Zustand „Security Check Failure Supervision Update" wechseln (Zustand 9).

(4) Im „Check for Replay"-Zustand muss die Verarbeitung nach Abschnitt 6.2.1.3 erfolgen.

Wenn keine Wiedergabe erkannt wird, muss der Wechsel in den Zustand „Application Update" erfolgen (Zustand 5).

Wenn eine Wiedergabe erkannt wird, muss der Wechsel in den Zustand „Replayed Packet Supervision" erfolgen (Zustand 10).

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

(5) Der Zustand „To Application“ muss das GOOSE-Paket entschlüsseln. Die entschlüsselten Informationen müssen an die Anwendung übermittelt werden, wenn die entschlüsselte stNum nicht lastRcvStNum entspricht. Die Überwachungsinformationen sind auf der Grundlage der erhaltenen neuen Paketinformationen zu aktualisieren. Siehe 6.2.1.4 für die Verarbeitungsanforderungen. Sobald die Überwachungsinformationen aktualisiert wurden, erfolgt ein Übergang in den Zustand 8.

Die Werte für lastRcvStNum und lastRcvSqNum müssen durch die entschlüsselten Werte aus dem GOOSE-Paket aktualisiert werden.

Der Zustand muss in den Zustand 6 wechseln.

(6) Der intTAL-Wert muss auf den entschlüsselten Time Allowed to Live (TAL)-Wert gesetzt werden. Der „Association Loss“-Zeitüberschreitungswert muss ebenfalls auf einen lokal bestimmten Wert zurückgesetzt werden.

(7) Die Überwachungsinformationen müssen auf der Grundlage der neuen erhaltenen Paketinformationen aktualisiert werden. Die Verarbeitungsanforderungen sind in Abschnitt 6.2.1.4 beschrieben.

Sobald die Überwachungsinformationen aktualisiert wurden, erfolgt der Wechsel in den Zustand 8.

(8) Der Wert für intTAL muss zur Entdeckung von Paketverlusten verwendet werden. Der Zustand muss eine Ablaufzeit auf der Grundlage des aktuellen Werts von intTAL starten.

Wenn der Wert von intTAL null (z. B. abgelaufen) ist, muss ein Wechsel in den Zustand 11 erfolgen.

Wenn das abonnierte GOOSE-Paket empfangen wird, muss der Zustand in den Zustand 3 wechseln.

(9) Die Überwachungsinformationen müssen auf der Grundlage der erhaltenen Informationen über die fehlgeschlagene Sicherheitsprüfung aktualisiert werden. Die Verarbeitungsanforderungen sind in Abschnitt 6.2.1.4 beschrieben.

Sobald die Überwachungsinformationen aktualisiert wurden, erfolgt der Wechsel in den Zustand 8. intTAL darf nicht zurückgesetzt oder verändert werden.

(10) Die Überwachungsinformationen müssen auf der Grundlage der erhaltenen Wiedergabeerkennungsinformationen aktualisiert werden. Die Verarbeitungsanforderungen sind in Abschnitt 6.2.1.4 beschrieben.

Sobald die Überwachungsinformationen aktualisiert wurden, erfolgt der Wechsel in den Zustand 8. intTAL darf nicht zurückgesetzt oder verändert werden.

(11) Dieser Zustand wird genutzt, um zu erkennen, wenn ein Abonnement nicht länger aktiv ist. Er unterscheidet sich dahingehend von der Paketverlusterkennung, dass er eine lokale Funktion ist.

Sobald festgestellt wurde, dass das Abonnement nicht länger aktiv ist, wechselt der Zustand in den Zustand 12 und die erwartete stNum/sqNum muss zurückgesetzt werden.

(12) Die Anwendung muss so aktualisiert werden, dass sie erkennt, dass das Abonnement nicht mehr gültig ist. Die hierfür genutzte Funktion ist daher eine lokale Funktion.

Im Anschluss an die Aktualisierung der Anwendung muss der Zustand in den Zustand 13 wechseln.

(13) Die Überwachungsinformation muss auf der Grundlage des Verlusts des aktiven Abonnements aktualisiert werden (z. B. muss LGOS.St den Zustand ändern). Die Verarbeitungsanforderungen sind in Abschnitt 6.2.1.4 beschrieben.

Sobald die Überwachungsinformationen aktualisiert wurden, erfolgt der Wechsel in den Zustand 14. intTAL darf nicht zurückgesetzt oder verändert werden.

(14) Die Werte von lastRcvStNum und lastRcvSqNum müssen auf ungültig gesetzt werden und der Wechsel in den Zustand 2 muss erfolgen.

6.2.1.2 Sicherheitsprüfungs-Schutzanforderungen

Dieser Abschnitt legt die erforderliche Verarbeitung für die Prüfung der GOOSE-Sicherheitsparameter fest.

- Der Subscriber muss prüfen, ob der AuthenticationValue (siehe 7.2.2.3) erwartet wird.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

- Wenn der AuthenticationValue durch die Konfiguration von GSEControl.securityEnabled erwartet und kein AuthenticationValue geliefert wird, muss dies zu einer fehlgeschlagenen Sicherheitsprüfung führen und keine weitere Sicherheitsprüfungsverarbeitung ist erforderlich.
- Wenn kein AuthenticationValue erwartet und trotzdem übermittelt wird, muss dieser verarbeitet werden und der Wert des AuthenticationValue darf nicht geprüft werden. Gleichzeitig darf dies nicht als fehlgeschlagene Sicherheitsprüfung gelten.
- Wenn ein AuthenticationValue weder erwartet wird noch vorhanden ist, darf dies nicht als fehlgeschlagene Sicherheitsprüfung gelten.
- Wenn ein AuthenticationValue besteht und der Subscriber keine Authentifizierung unterstützt, darf dies nicht als fehlgeschlagene Sicherheitsprüfung gelten.

- Wird eine Verschlüsselung angewendet, muss das Paket entschlüsselt werden.

Wenn keine Sicherheitsprüfung fehlschlägt, muss der Zustandsautomat in den nächsten Zustand wechseln.

6.2.1.3 Verarbeitungsanforderungen an die Prüfung des Wiedergabezustands

Dieser Abschnitt legt die erforderliche Verarbeitung für die Prüfung der GOOSE-Paketwiedergabe fest.

- Der Subscriber muss den erhaltenen Zeitstempel (t) in der GOOSE-Nachricht mit lastRcvT vergleichen. Die Verarbeitung stellt sich wie folgt dar:
  - Wenn der Subscriber einen ungültigen Wert für lastRcvT hat, muss der Subscriber den Wert von lastRcvT mit dem in der GOOSE-Nachricht erhaltenen Wert von „t“ aktualisieren.
  - Wenn ein gültiger Wert für lastRcvT und lastRcvStNum vorliegt:
    - Wenn der Wert von lastRcvStNum geringer ist als der erhaltene stNum-Wert, muss der Subscriber prüfen, dass der erhaltene Wert von „t“ nicht höher ist als der ältere oder neuere konfigurierte Zeitversatzwert als die lokale Zeit des Subscribers. Wenn der Wert „t“ außerhalb dieses Bereichs liegt, gilt dies als Fehler und es ist keine weitere Verarbeitung des Wiedergabeschutzes erforderlich, da dieser bereits fehlgeschlagen ist.

      Der Zeitversatz muss konfigurierbar sein und einen Mindestwert von 10 Sekunden unterstützen. Der konfigurierbare Höchstwert muss 30 Sekunden betragen. Dieser Wert muss durch SCL als Teil des GOOSE-Abonnementmechanismus konfigurierbar sein (siehe Abschnitt 9.1).

- Der Subscriber muss den erhaltenen Wert von stNum und sqNum in der GOOSE-Nachricht prüfen. Die Verarbeitung stellt sich wie folgt dar:
  - Wenn der Subscriber ungültige Zustände für lastRcvStNum und lastRcvSqNum hat, muss der Subscriber-Zustandsautomat die Werte auf Folgendes einstellen:
    - lastRcvStNum muss auf den in dem GOOSE-Paket erhaltenen Wert von stNum gesetzt werden.
    - lastRcvSqNum muss auf den in dem GOOSE-Paket erhaltenen Wert von sqNum gesetzt werden.

      Weitere Wiedergabeprüfungen sind nicht erforderlich.
  - Wenn gültige Werte für lastRcvStNum und lastRcvSqNum vorliegen, muss der Subscriber:
    - Feststellen, ob eine überlappende Eingabe von sqNum bevorstand. Wenn der erhaltene Wert von stNum null (0) war, müssen die Werte von lastRcvStNum und lastRcvSgNum durch die erhaltenen Werte von stNum und sqNum aktualisiert werden.

      Weitere Wiedergabeprüfungen sind nicht erforderlich.
    - Wenn der erhaltene Wert von stNum geringer ist als lastRcvStNum oder sqNum geringer ist als lastRcvSqNum, könnte dies durch einen der beiden folgenden Faktoren verursacht worden sein:

      Eine Paketwiedergabe oder ein verzögertes Multipath-Paket. In beiden Fällen darf die erhaltene GOOSE nicht an die Anwendung übermittelt werden und der Zustandsautomat muss sich so verhalten, als handele es sich bei dem Paket um eine Wiedergabe. Es ist jedoch eine lokale Funktion, wenn der Überwachungszustand diesen Fall als Wiedergabe klassifiziert.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

6.2.1.4 Verarbeitungsanforderungen an den Überwachungsaktualisierungszustand

Der Überwachungsaktualisierungszustand ist ein Übergangszustand und wird verwendet, um die lokale Aktualisierung des LGOS, der lokalen Protokolle, der standardisierten Sicherheitsprotokolle, der eigenen Netzwerkverwaltungs-MIB und der Erstellung von Sicherheitsereignissen sowie der nach IEC 62351-7 genormten MIB darzustellen.

6.2.2 Sampled-Value-Wiedergabeschutz

IEC 61850-9-2 beschreibt nicht den Übergang im Fall der Handhabung einer Störmeldung. In einigen Fällen stellt die Übermittlung der Störnachricht keine Wiedergabe dar und könnte einfach auf Multipath-Übertragungsverzögerungen basieren. Anders als GOOSE haben Sampled Values kein Zustands-/Sequenznummernkonstrukt für die Verwendung im Wiedergabeschutz. Implementierungen, die die Konformität mit dieser Norm beanspruchen, müssen daher Folgendes implementieren.

6.2.2.1 Publisher

Um SVreplay zu verhindern, muss das Sicherheitsfeld des SVprotocol vorhanden sein (siehe Tabelle 3).

Tabelle 3 – Auszug aus IEC 61850-9-2 (informativ)

ASN.1 Basic Encoding Rules (BER) SavPdu::= **SEQUENCE {**
noASDU [0] IMPLICIT INTEGER (1..65535),
security [1] ANY OPTIONAL,
asdu [2] IMPLICIT SEQUENCE OF ASDU **}**

Um die Wiedergabe zu verhindern, muss der Publisher das optionale Sicherheitsfeld in SavPdu einfügen und eine Form des Integritätsschutzes wie für die verschiedenen T-Profile vorgegeben (z. B. Layer 2 oder routbar) implementieren.

Das SavPdu-Sicherheitsfeld darf nicht vorhanden sein, wenn die SampledValue-Sicherheit in einer bestimmten Nachricht nicht gegeben ist. Wenn die Sicherheit für die Nachricht genutzt wird, muss das Feld vorhanden sein und folgenden Inhalt haben:

IMPORT

security::= [0] IMPLICIT SEQUENCE {
timestamp [0] IMPLICIT OCTETSTRING, --time of send
…
}

&timestamp

Das Zeitstempel-Attribut muss den ungefähren Zeitpunkt der Formatierung des SV-Frames angeben.

Das Achtbit-Format nach IEC 61850-8-1 muss für den Zeitstempel verwendet werden.

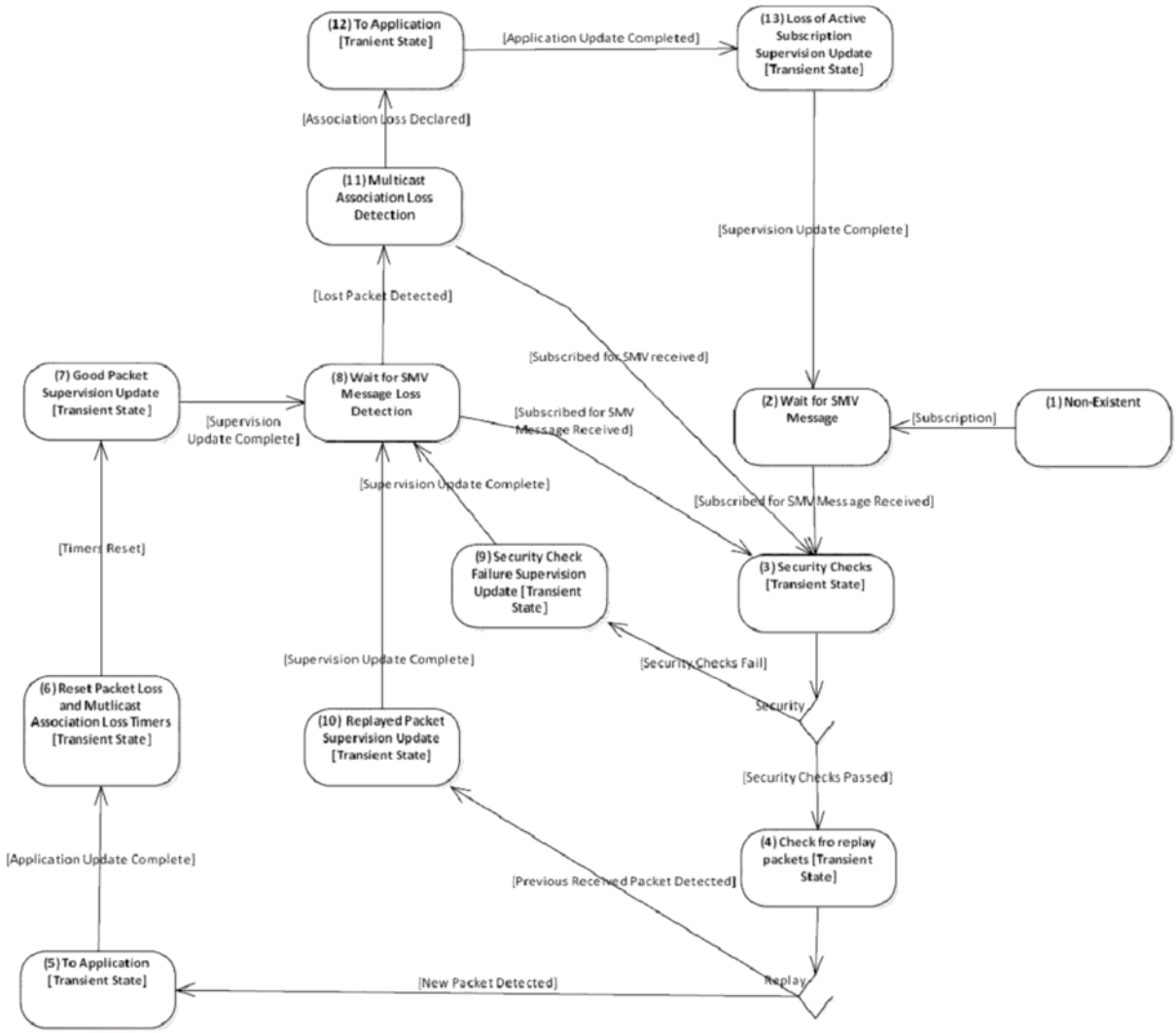
Die Genauigkeit des Zeitwerts muss mindestens 250 usec betragen.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

6.2.2.2 Subscriber

Je nach vorhandenem SVsecurity-Feld oder der Verwendung des routbaren SMV gelten die folgenden Zustandsautomaten-Regeln:

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05



Englisch	Deutsch
(12) To Application [Transient State]	(12) Zur Anwendung [Übergangszustand]
[Application Update Completed]	[Aktualisierung der Anwendung abgeschlossen]
(13) Loss of Active Subscription Supervision Update [Transient State]	(13) Verlust der Aktualisierung der aktiven Abonnement-Überwachung [Übergangszustand]
[Association Loss Declared]	[Assoziationsverlust angegeben]
(11) Multicast Association Loss Detection	(11) Multicast-Assoziationsverlust erkannt
[Supervision Update Complete]	[Überwachungsaktualisierung abgeschlossen]
[Lost Packet Detected]	[verlorenes Paket erkannt]
(7) Good Packet Supervision Update (Transient State)	(7) Gute Paket-Überwachungsaktualisierung (Übergangszustand)
[Supervision Update Complete]	[Überwachungsaktualisierung abgeschlossen]
(8) Wait for SMV Message Loss Detection	(8) Warten auf SMV-Nachricht-Verlusterkennung
[Subscribed for SMV received]	[Abonnierte SMV erhalten]
[Subscribed for SMV Message Received]	[Abonnierte SMV-Nachricht erhalten]
(2) Wait for SMV Message	(2) Auf SMV-Nachricht warten
[Subscription]	[Abonnement]

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

Englisch	Deutsch
(1) Non-Existent	(1) Nicht existent
[Timers Reset]	[Timer zurückgesetzt]
(9) Security Check Failure Supervision Update [Transient State]	(9) Sicherheitsprüfungsausfall-Überwachungs-Aktualisierung [Übergangszustand]
(9) Security Checks [Transient State]	(9) Sicherheitsprüfungen [Übergangszustand]
[Security Checks Fail]	[Sicherheitsprüfungen fehlgeschlagen]
(6) Reset Packet Loss and Multicast Association Loss Timers [Transient State]	(6) Rücksetzung-Paketverlust und Multicast-Assoziationsverlust Timer [Übergangszustand]
(10) Replayed Packet Supervision Update [Transient State]	(10) Paketwiedergabe-Überwachungs-Aktualisierung [Übergangszustand]
Security	Sicherheit
[Security Checks passed]	[Sicherheitsprüfungen bestanden]
[Application Update Complete]	[Aktualisierung der Anwendung abgeschlossen]
[Previous Received Packet Detected]	[zuvor erhaltenes Paket erkannt]
(4) Check for replay packets [Transient State]	(4) Prüfung auf Wiedergabe-Pakete [Übergangszustand]
(5) To Application [Transient State]	(5) Zur Anwendung [Übergangszustand]
[New Packet Detected]	[neues Paket erkannt]
Replay	Wiederholung

Bild 2 – Wiedergabeschutz-Zustandsautomat für SMV

Bild 2 ist für SV-Nachrichten relevant, für die der Subscriber über ein aktives Abonnement verfügt, das manuell oder durch SCL und einen ICT konfiguriert werden kann. Implementierungen, die die Konformität mit dieser Norm beanspruchen, müssen mindestens die folgenden internen Zustandsautomaten-Variablen haben: letzter erhaltener Sicherheitszeitstempelwert (lastRcvT) und Zeitverzögerung, bis das nächste Paket erwartet wird (expNxtPkt). Die Zustände und ihre Übergänge sind wie folgt festgelegt:

(1) Der „Nicht vorhanden“-Zustand (en: Non-Existent) ist der Zustand, in dem kein SV-Abonnement besteht.

(2) Bei der Aktivierung des Abonnements (z. B. Einschalten oder Konfiguration des Abonnements) stellt der Zustandsautomat intern lastRcvT und expNxtPk ein und wechselt in den Zustand „auf SV-Nachricht warten“.

Bei Erhalt der abonnierten SV-Nachricht muss der Subscriber in den Sicherheitsprüfungs-zustand (en: Security Checks) (Schritt 3) wechseln.

(3) Die Verarbeitung des Security-Checks-Zustands wird in Abschnitt 6.2.2.2.1 beschrieben.

Wenn die Sicherheitsprüfungen bestanden werden, muss der Zustandsautomat zur Prüfung auf wiedergegebene Pakete (Schritt 4) wechseln.

Wird die Sicherheitsprüfung nicht bestanden, muss die Maschine in den Zustand der Überwachungsaktualisierung des Sicherheitsprüfungsfehlers wechseln (Schritt 9).

(4) Im „Check for Replay“-Zustand muss die Verarbeitung nach Abschnitt 6.2.2.2.2 erfolgen.

Wenn keine Wiedergabe erkannt wird, muss der Wechsel in den Zustand „Application Update“ erfolgen (Zustand 5).

Wenn eine Wiedergabe erkannt wird, muss der Wechsel in den Zustand „Replayed Packet Supervision“ erfolgen (Zustand 10).

(5) Der „To Application“-Zustand muss das SV-Paket entschlüsseln. Die entschlüsselten Informationen müssen an die Anwendung übermittelt werden.

Der Zustand muss in den Zustand 6 wechseln.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

(6) Der expNxtPkt-Wert muss anhand der folgenden Berechnung festgelegt werden:

Die dynamische Berechnung von expNxtPk ist für Systeme zulässig, deren Konfiguration nicht auf SCL basiert. Der dynamische Wert für expNxtPk wird auf dieselbe Weise berechnet, basiert aber auf den in actualSVAPDU erhaltenen Werten.

Der Wert von expNxtPk ist festgelegt als:

Für smpMod = SmpPerSec:

expNxtPk = (noASDU/smpRate) * 2

Für smpMod = SecPerSmp:

expNxtPk = smpRate * noASDU * 2

Für smpMod = SmpPerPeriod:

expNxtPk = ((noASDU/smpRate)/(nominal frequency)) * 2

Der Ablauf des Timers führt zu einem Wechsel in einen Zustand, der eine zusätzliche Verzögerung zu der tatsächlichen Erklärung, dass ein Verlust des Multicast-Abonnements aufgetreten ist, hinzufügt.

Der „Association Loss“-Zeitüberschreitungswert muss ebenfalls auf einen lokal bestimmten Wert zurückgesetzt werden.

(7) Die Überwachungsinformationen müssen auf der Grundlage der neuen erhaltenen Paketinformationen aktualisiert werden. Die Verarbeitungsanforderungen sind in Abschnitt 6.2.1.4 beschrieben.

Sobald die Überwachungsinformationen aktualisiert wurden, erfolgt der Wechsel in den Zustand 8.

(8) Wenn das abonnierte SV-Paket empfangen wird, muss der Zustand in den Zustand 3 wechseln.

Der Timer für die Erkennung des lokalen Multicast-Assoziationsverlusts muss gestartet werden. Sobald der Timer abläuft, muss in den Zustand 11 gewechselt werden.

(9) Die Überwachungsinformationen müssen auf der Grundlage der erhaltenen Informationen über die fehlgeschlagene Sicherheitsprüfung aktualisiert werden. Die Verarbeitungsanforderungen sind in Abschnitt 6.2.2.2.3 beschrieben.

Sobald die Überwachungsinformationen aktualisiert wurden, erfolgt der Wechsel in den Zustand 8.

(10) Die Überwachungsinformationen müssen auf der Grundlage der erhaltenen Wiedergabeerkennungsinformationen aktualisiert werden. Die Verarbeitungsanforderungen sind in Abschnitt 6.2.2.2.3 beschrieben.

Sobald die Überwachungsinformationen aktualisiert wurden, erfolgt der Wechsel in den Zustand 8.

(11) Dieser Zustand wird genutzt, um zu erkennen, wenn ein Abonnement nicht länger aktiv ist. Er unterscheidet sich dahingehend von der Paketverlusterkennung, dass er eine lokale Funktion ist.

Wenn die abonnierte SV-Nachricht empfangen wird, muss der Zustand in den Zustand 3 wechseln.

(12) Die Anwendung muss so aktualisiert werden, dass sie erkennt, dass das Abonnement nicht mehr gültig ist. Die hierfür genutzte Funktion ist daher eine lokale Funktion.

Im Anschluss an die Aktualisierung der Anwendung muss der Zustand in den Zustand 13 wechseln.

(13) Die Überwachungsinformation muss auf der Grundlage des Verlusts des aktiven Abonnements aktualisiert werden (z. B. muss LSVS.St den Zustand ändern). Die Verarbeitungsanforderungen sind in Abschnitt 6.2.2.2.3 beschrieben.

6.2.2.2.1 Sicherheitsprüfungs-Schutzanforderungen

Dieser Abschnitt legt die erforderliche Verarbeitung für die Prüfung der SV-Sicherheitsparameter fest.

- Der Subscriber muss prüfen, ob der AuthenticationValue (siehe 7.2.2.3) erwartet wird.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-6:2019-05

- Wenn der AuthenticationValue erwartet und kein AuthenticationValue geliefert wird, muss dies zu einer fehlgeschlagenen Sicherheitsprüfung führen und keine weitere Sicherheitsprüfungsverarbeitung ist erforderlich.
- Wenn kein AuthenticationValue erwartet und trotzdem übermittelt wird, muss dieser verarbeitet werden und der Wert des AuthenticationValue darf nicht geprüft werden. Gleichzeitig darf dies nicht als fehlgeschlagene Sicherheitsprüfung gelten.
- Wenn ein AuthenticationValue weder erwartet wird noch vorhanden ist, darf dies nicht als fehlgeschlagene Sicherheitsprüfung gelten.
- Wenn ein AuthenticationValue besteht und der Subscriber keine Authentifizierung unterstützt, darf dies nicht als fehlgeschlagene Sicherheitsprüfung gelten.

- Wird eine Verschlüsselung angewendet, muss das Paket entschlüsselt werden.

Wenn keine Sicherheitsprüfung fehlschlägt, muss der Zustandsautomat in den nächsten Zustand wechseln.

6.2.2.2.2 Verarbeitungsanforderungen an die Prüfung des Wiedergabezustands

Dieser Abschnitt legt die erforderliche Verarbeitung für die Prüfung der SV-Paketwiedergabe fest.

- Der Subscriber muss den erhaltenen Zeitstempel (t) in der SV-Nachricht mit lastRcvT vergleichen. Die Verarbeitung stellt sich wie folgt dar:
  - Wenn der Subscriber einen ungültigen Wert für lastRcvT hat, muss der Subscriber den Wert von lastRcvT mit dem in der SV-Nachricht erhaltenen Wert des Sicherheitszeitstempels aktualisieren.

6.2.2.2.3 Verarbeitungsanforderungen an den Überwachungsaktualisierungszustand

Der Überwachungsaktualisierungszustand ist ein Übergangszustand und wird verwendet, um die lokale Aktualisierung des LSVS, der lokalen Protokolle, der standardisierten Sicherheitsprotokolle, der eigenen Netzwerkverwaltungs-MIB und der Erstellung von Sicherheitsereignissen sowie der nach IEC 62351-7 genormten MIB darzustellen.

7 Sicherheit für SNTP

IEC 61850-8-1 und IEC 61850-8-2 legen die Nutzung von SNTP für die Zwecke der Zeitsynchronisierung fest.

Implementierungen, die die Konformität mit dieser Norm beanspruchen, müssen das RFC-5905-Profil für SNTP einschließlich der verbindlichen Nutzung von Authentifizierungsmechanismen implementieren.

8 Layer-2-Sicherheit für Profile für IEC 61850-8-1 GOOSE und IEC 61850-9-2 Sampled Value

8.1 EtherTyp-Übersicht (informativ)

Diese Spezifikation gilt für übliche Layer 2 IEC 61850 GOOSE und Layer 2 IEC 61850-9-2 Sampled Measured Value PDU. ~~Eine Beschreibung einer PDU für GSE-Management und GOOSE ist in Anhang C zu IEC 61850-8-1 enthalten~~.

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62351-6:2019-05