DHBW CAS
Duale Hochschule
Baden-Württemberg
Center for Advanced Studies

Energieinformationstechnik
Teil 2.3 Anwendungsprotokolle

Dr. Leonhard Stiegler

www.dhbw-stuttgart.de

Kursinhalt

- Einführung
- Übersicht Protokolle
  - Stationsautomatisierung IEC 61850
  - Common Information Model IEC 61970
  - Sicherheit IEC 62351
- Anwendungsbeispiel
  - IEC 61850 Raspberry Pi Client – Server Implementierung

Aufgabe von Standards

Internationale Standards

- ermöglichen Interoperabilität und Integration unterschiedlicher Herstellersysteme
- sind hierarchisch und strukturiert aufgebaut und legen fest:
  - Datenstrukturen und Formate
  - Kommunikations-Methoden, Nachrichten und
  - Prozeduren
- erlauben eine effektive System-Konfiguration
- erlauben effektive effektive System-Kommunikation
- ermöglichen einfaches Modellieren von Geräten und Daten
- ermöglichen kostengünstige und skalierbare Lösungen

Normatives Umfeld

Übersicht - Themen der Arbeitsgruppen des IEC TC 57:

- IEC 61850:
  - netzwerkbasierter Feldbus für Schaltanlagen mit Datenmodell (Communications and Associated Data Models)

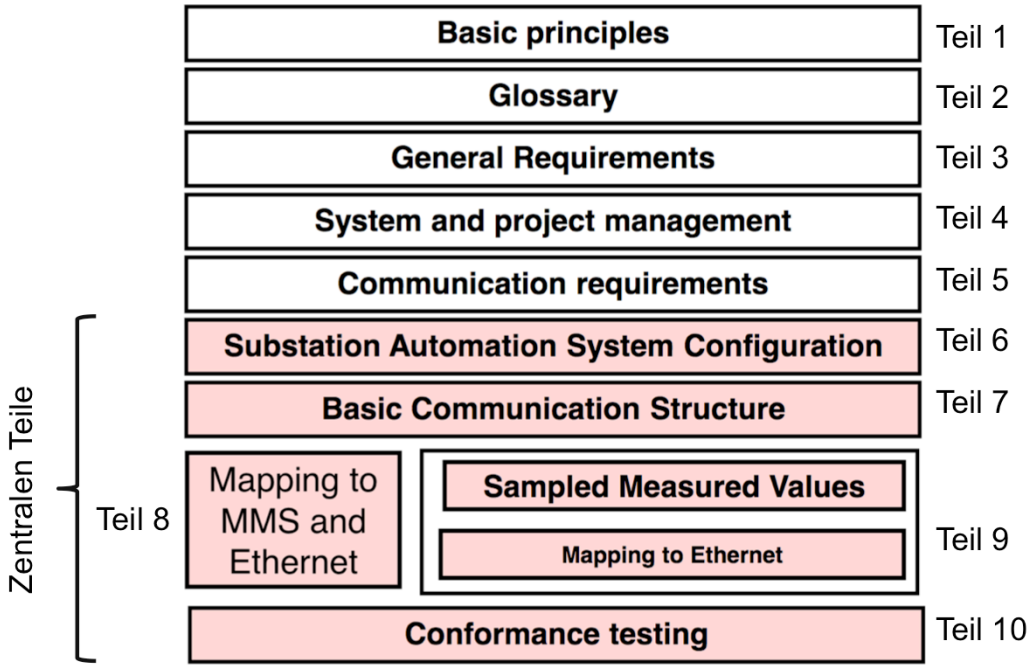
- IEC 61970 Common Information Model:
  - Datenmodelle für den Austausch von Informationen über primäre Betriebsmittel
  - Energy Management Systems – Application Programming Interfaces (API)

TC: Technical Comittee

Kursinhalt

- Einführung
- Übersicht der Protokolle
  - Stationsautomatisierung IEC 61850
  - Common Information ModelI IEC 61970
  - Sicherheit IEC 62351
- Anwendungsbeispiel
  - IEC 61850 Raspberry Pi Client – Server API

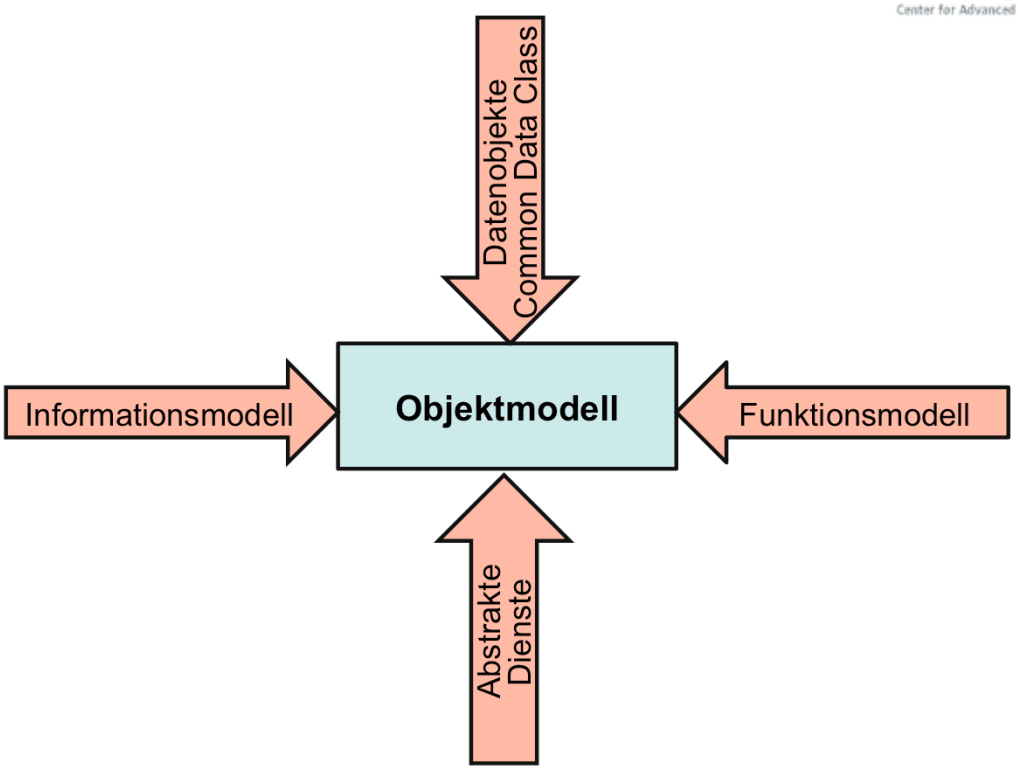
IEC61850 Aufbau des Standards



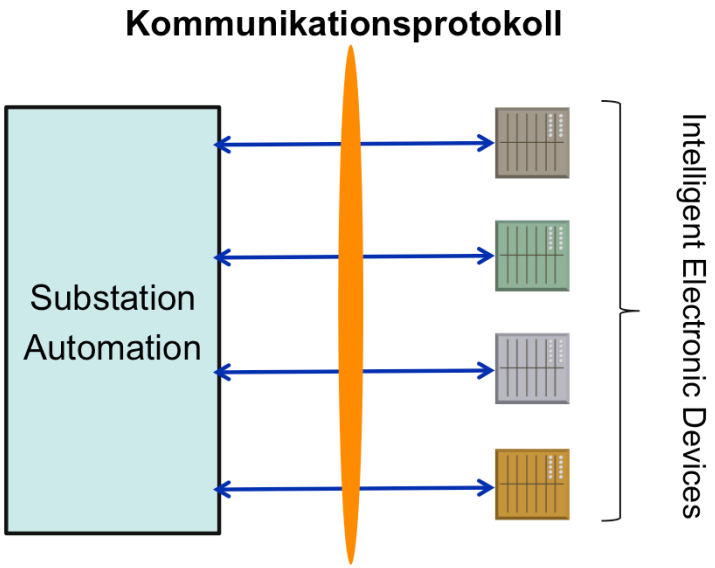
Zentrale Teile des IEC 61850 Standards

Part 6-1:	Substation Configuration Language (SCL)
Part 7-2:	Abstract Communications Service Interface (ACSI) and base types
Part 7-3:	Common Data Classes (CDC)
Part 7-4:	Logical Nodes
Part 8-1:	Specific Communications Service Mappings (SCSM) MMS & Ethernet
Part 9-2:	SCSM Sampled Values over Ethernet
Part 10-1:	Conformance Testing

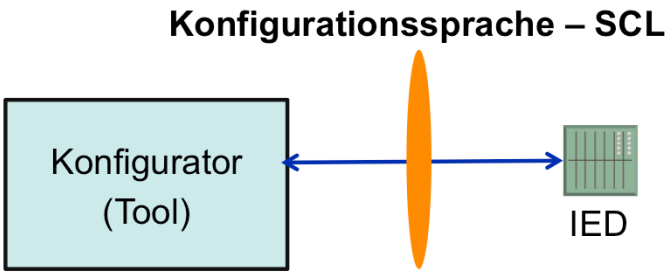
IEC 61850 Kernkomponenten (1)



IEC 61850 Kernkomponenten (2)



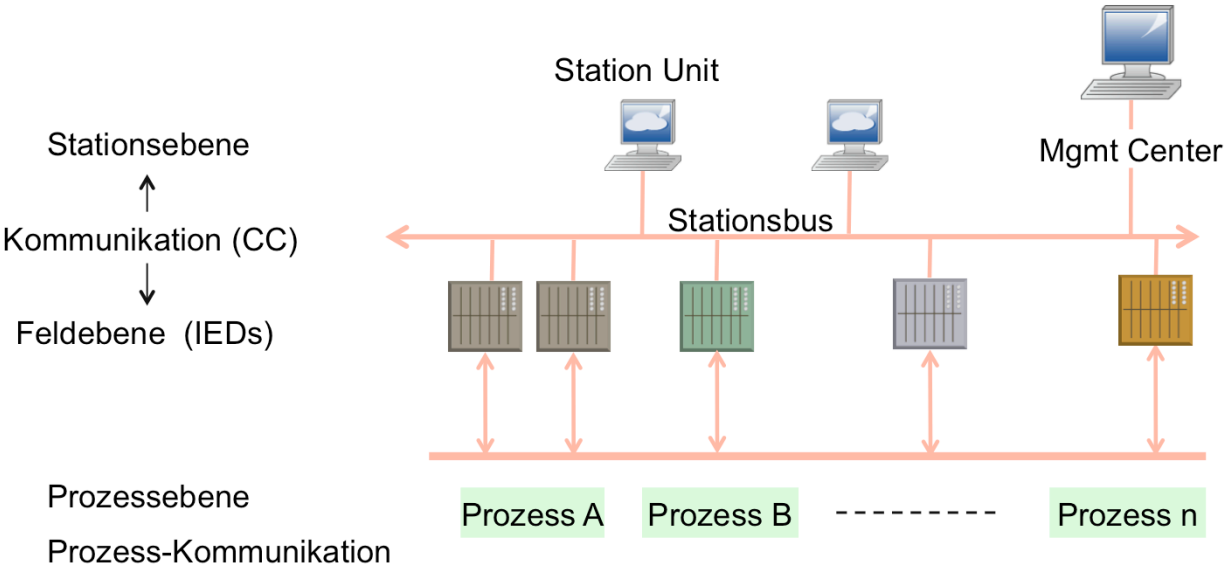
IEC 61850 Kernkomponenten (3)



IED = Intelligent Electronic Device

IEC 61850 Übersicht

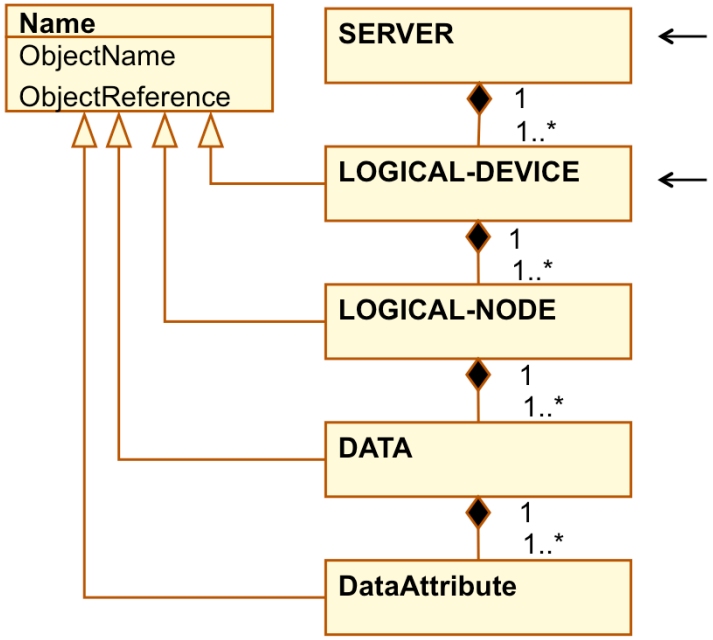
Die Norm IEC 61850 definiert die Kommunikation zwischen Geräten in der Stationsautomatisierung elektrischer Stromerzeuger



IEDs :

- sind Microprocessor-basierte Geräte, wie z.B. Leistungsschalter, Schutzrelais, etc.
- empfangen Daten z.B. von Sensoren oder Messeinrichtungen
- aktivieren Steuerungskommandos in geeigneten Situationen zur Aufrechterhaltung der gewünschten Systemzustände

IEC 61850 Objektmodell : Klassen



Physical Device:
Zugang über die Netzadresse

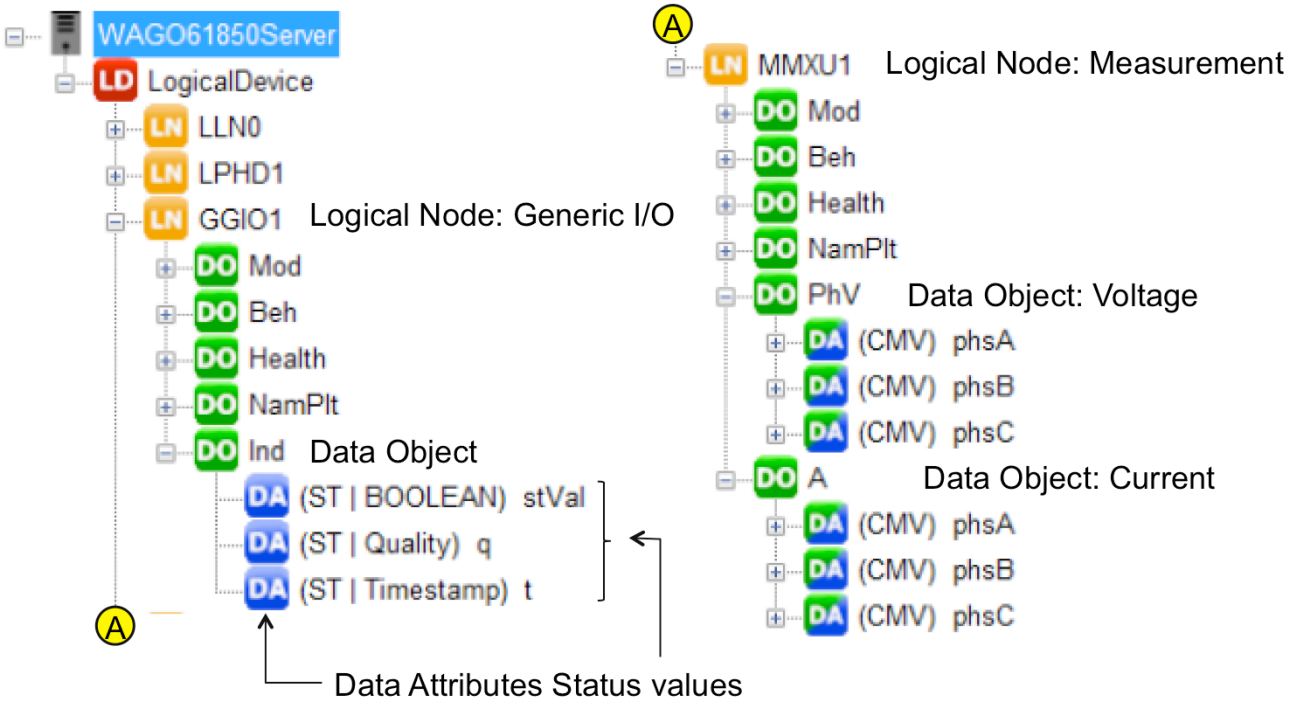
Daten mehrerer Logical Devices können in einem einzigen Physical Device zusammenfließen (data concentrator)

Notes:

Objektmodell : Logical Node Types

Name	Funktion
Axxx	Automatic Control (4). ATCC (tap changer), AVCO (volt. ctrl.), etc.
Cxxx	Supervisory Control (5). CILO (Interlocking), CSWI (switch ctrl), etc.
Gxxx	Generic Functions (3). GGIO (generic I/O), etc.
Ixxx	Interfacing/Archiving (4). IARC (archive), IHMI (HMI), etc.
Lxxx	System Logical Nodes (2). LLN0 (common), LPHD (Physical Device)
Mxxx	Metering & Measurement (8). MMXU (meas.), MMTR (meter.), etc.
Pxxx	Protection (28). PDIF, PIOC, PDIS, PTOV, PTOH, PTOC, etc.
Rxxx	Protection Related (10). RREC (auto reclosing), RDRE (disturbance)..
Sxxx	Sensors, Monitoring (4). SARC (archs), SPDC (partial discharge), etc.
Txxx	Instrument Transformer (2). TCTR (current), TVTR (voltage)
Xxxx	Switchgear (2). XCBR (breaker), XCSW (switch)
Yxxx	Power Transformer (4). YPTR (transformer), YPSH (shunt), etc.
Zxxx	Other Equipment (15). ZCAP (cap ctrl), ZMOT (motor), etc.
Wxxx	Wind (Set aside for other standards)
Oxxx	Solar (Set aside for other standards)
Hxxx	Hydropower (Set aside for other standards)
Nxxx	Power Plant (Set aside for other standards)
Bxxx	Battery (Set aside for other standards)
Fxxx	Fuel Cells (Set aside for other standards)

Datenobjekte - Beispiel

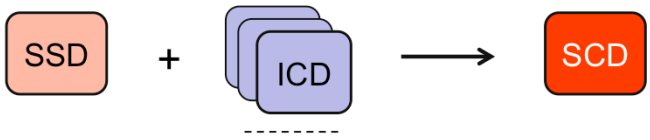


Substation Configuration Language – SCL

- IEC61850-6-1 **SCL**
- Beschreibungssprache für die IED Kommunikation
- XML basiert
- Erlaubt die formale Beschreibung eines:
  - Substation Automation System und die
  - Konfiguration eines IED

Substation Configuration – SCL

- Substations (IEDs) werden mittels der SCL – Sprache (Substation Configuration Language) beschrieben
- SCL ist durch IEC61870-6 spezifiziert
- SCL Dateiarten:
  - **ICD** (IED Capability Description)
    enthält die Systemkonfiguration eines IED, opt. Kommunikation
  - **SSD** (System Specification Description)
    logical nodes, data type templates
  - **SCD** (Substation Configuration Description)
    alle Informationen (data types, IED, communication, logical nodes



Configured IED Description (CID)

Instantiated IED Description (IID) file:

System Exchange Description (SED) file

Kommunikationsmodell : IEC 61850-7

Der Teil IEC 61850-7 (Basic Communication Structure) definiert und spezifiziert :

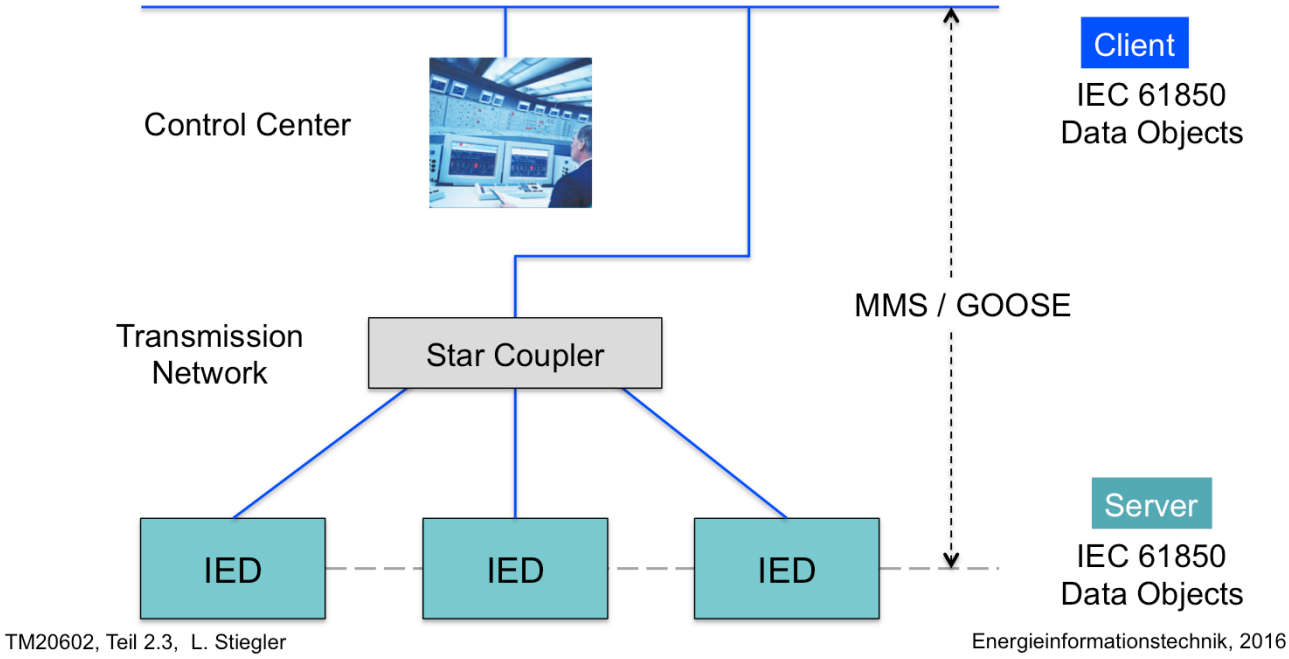
- die grundlegende Kommunikationsstruktur
- das grundlegende Objektmodell
- Kommunikationsprinzipien
- die abstrakte Schnittstelle (API) für Kommunikationsdienste
- die Kommunikationsdienste
- ein Modell der Server-Datenbank
- abstrakte gemeinsame Datenklassen
- das Konzept der logische Knoten (logical nodes)

Kommunikationsrollen

- **Client**
  - empfängt Daten vom Server (z.B. Mess- und Statistik-Daten, ...)
  - aktiviert Prozeduren (z.B. Steuerung, Abfragen, ...)
  - verarbeitet Mess- und Statistik-Daten
  - besitzt i.d.R. Management-Funktion
- **Server**
  - kontrolliert physikalische Schnittstellen
  - führt Steuerungskommandos durch
  - verarbeitet Messdaten (Umrechnungen, Grenzwertanalyse, ...)
  - besitzt i.d.R IED Funktion
- **API**
  - Programmierschnittstelle zwischen Client und Server
  - führt das Kommunikationsprotokoll durch
  - wird durch eine SCD-Datei beschrieben

IEC 61850 Kommunikationsmodell

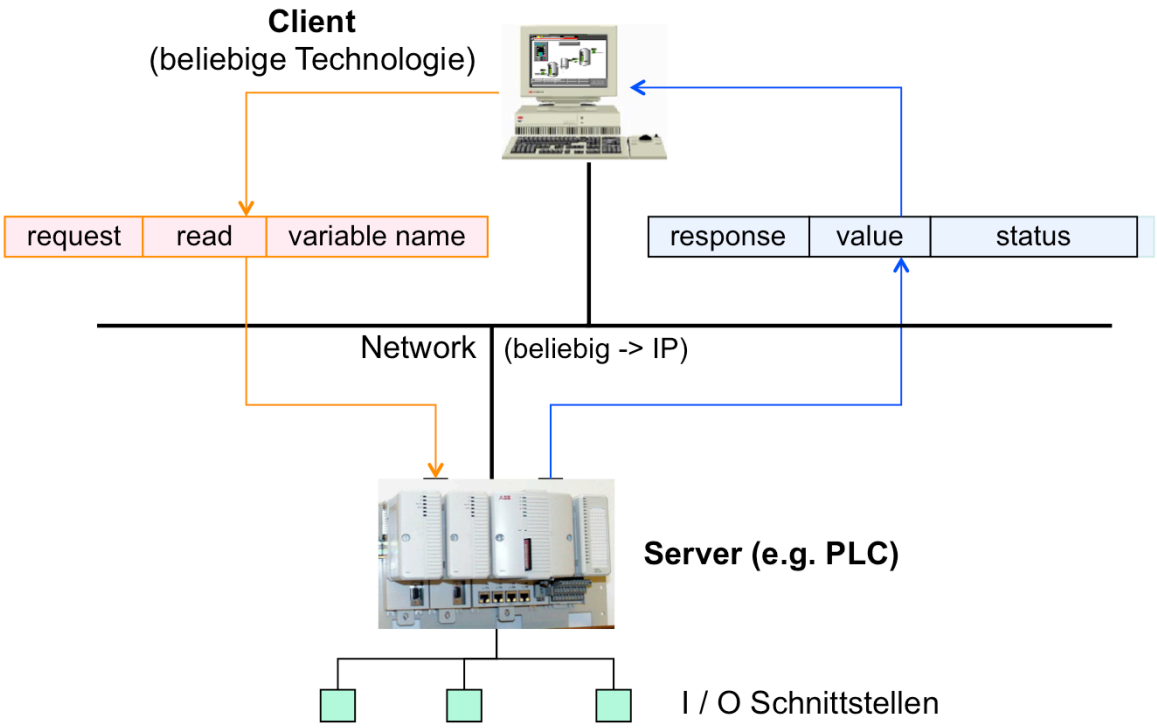
IEC 61850 Client – Server Kommunikation zwischen IED und Control Center



This system must have software that can interpret the IEC 60870-5-103 communication messages

IEC 60870-5-103 defines communication for a serial, unbalanced link only. Communication speeds are defined as either 9600 or 19200 baud

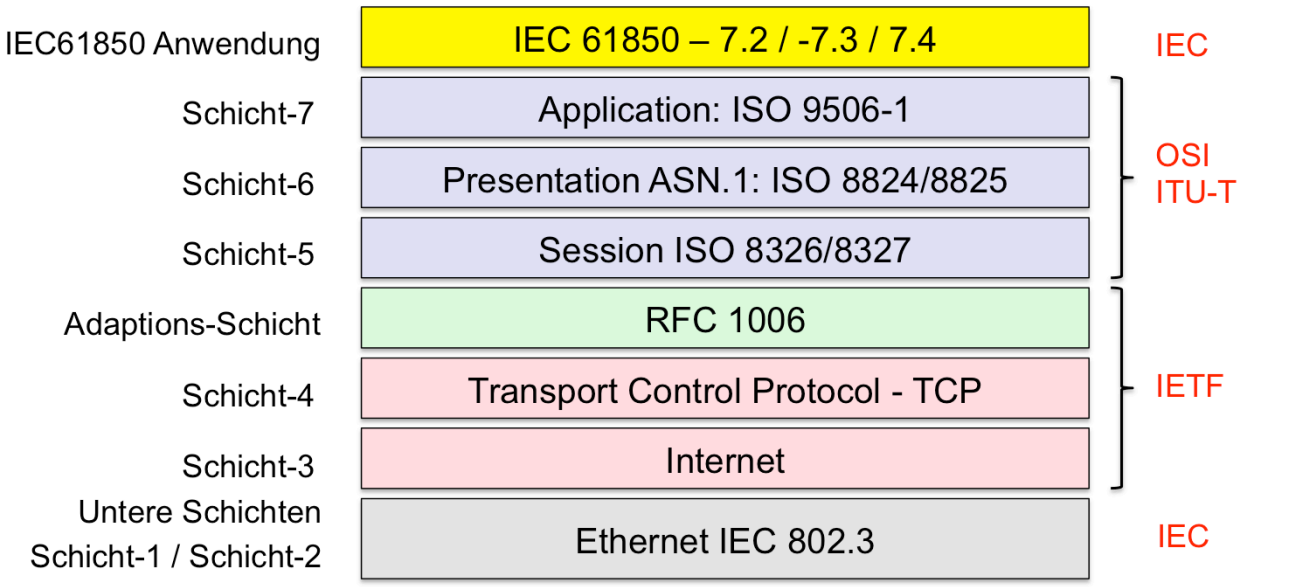
MMS – Kommunikation



PLC = Programmable Logical Controller
MMS: R/W Gerätevariablen mittels Standard-Nachrichten (Protocol Data Units = PDU)

MMS Protokollschichten

Spezifikation: IEC 61850 Part 8-1:
Specific communication service mapping (SCSM) – Mappings to **MMS** (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3



Developed 1980 (!) for the MAP project (General Motor's flexible manufacturing initiative)
Originally unluckily tied to the OSI communication stack and Token Bus (IEEE 802.4)
Reputed for being heavy, complicated and costly due to poor implementations.
Boeing adopted MMS as TOPs (MMS on Ethernet) - a wise step.
Adopted by the automobile industry, aerospace industry, and PLC manufacturers: Siemens, Schneider, Daimler, ABB.
Standardized since 1990 as: ISO/IEC 9506-1 (2003): Industrial Automation systems - Manufacturing Message Specification -
Part 1: Service Definition
Part 2: Protocol Specification

MMS has been during its 15 years of existence a reference model for industry rather than an actual implementation.
Its high complexity makes it very general, but the requested bandwidth and computing power were out of reach until few years ago.
It is - sometimes as a proprietary version - part of every PLC today.
It gave rise to several other "simpler" models (DLMS, BacNet, FMS....)
It is the base of IEC 61850 „Communication networks and systems in substations", which bases on TCP/IP/Ethernet.

Kursinhalt

- Einführung
- Übersicht Protokolle
  - Stationsautomatisierung IEC 61850
  - Common Information Model IEC 61970
  - Sicherheit IEC 62351
- Anwendungsbeispiel
  - IEC 61850 Raspberry Pi Client – Server Implementierung

Common Information Model – CIM

- CIM ist ein Satz von Standards, der eine Systemintegration und einen Informationsaustausch basierend auf einer gemeinsamen „Sprache“ ermöglicht.
- Hauptstandards:
  - IEC 61970
    EMS Application Program Interface (EMS-API)
  - IEC 61968
    System Interfaces for Distribution Management
  - IEC 62325
    Framework for Energy Market Communication
- Ziel:
  - gemeinsames Informationsmodell, welches das elektrische Netz definiert
- Schnittstellen werden über Profile definiert

Informationsmodell:
- Allgemeines Modell aller Objekte eines EVU und deren Beziehungen untereinander
- Anwnedungsunabhängig

Kontextabhängigkeit:
- legt fest, welche CIM-Teile für ein bestimmtes Profil benutzt werden
- besteht aus vorgeschriebenen und optionalen Informationen und Einschränkungen
- erzeugt jedoch keine zusätzlichen Informationen

Die **Syntax** beschreibt das Format für die Instanzdaten

Ein **Profil**
- ist eine kontextabhängige, auf einen konkreten Anwendungsfall bezogene Untermenge des darunterliegenden semantischen Modells.
- spezifiziert die Informationsstruktur der auszutauschenden Information
- betrifft in der Regel mehrere Schnittstellen
- wird als Funktionsmerkmale von Produkten unterstützt z.B. CIM/XML Import/Export, ESB Adapter

Profile bilden die Grundlage für Interoperabilitätstests (IOP)

CIM – Beschreibung

- CIM wurde entwickelt durch die Technical Committee TC 57 der IEC
- CIM ist durch den IEC-Standard 61970 spezifiziert
- CIM beschreibt die Programmierschnittstelle (API) für Energie-Managementsysteme
- CIM ist objekt-orientiert, UML-Objekte und Datenaustauschformate für
  - Übertragung,
  - Verteilung und
  - Erzeugung von Energie
- IEC TC 57 Arbeitsgruppen:
  - WG 13 : IEC 61970
    Energy management systems - Application Program Interfaces
  - WG10 : IEC 61850
    IED communications & associated data models in power systems

Klassen beschreiben :
- Objekte
- ihre Eigenschaft und
- ihre Beziehungen mit anderen Objekten

Beispiel: Transformator – in Unterstationen enthalten – besitzen eindeutige Namen – arbeiten unter Betriebsspannungen, etc.

Instanzen beschreiben die spezifischen Objekte einer Klasse, die im System existiert

IEC 61850 und IEC 61970 CIM

IEC 61850

- Einheitliche Darstellung der Sekundärtechnik (Schutz, Regler, Überwachung)
- Schwerpunkt: Schaltanlagen (Feldebene)
- Datenmodell als Dokument verfügbar (IEC Standard)

IEC 61970 Common Information Model (CIM)

- Einheitliche Darstellung der Primärtechnik (IEC 61970-301 definiert CIM)
- Schwerpunkt: Leittechnik (Betrieb) und Pflege der Betriebsmittel
- Datenmodell direkt im UML-Format verfügbar (IEC Standard)

Kursinhalt

- Einführung
- Übersicht Protokolle
  - Stationsautomatisierung IEC 61850
  - Common Information Model IEC 61970
  - Sicherheit IEC 62351
- Anwendungsbeispiel
  - IEC 61850 Raspberry Pi Client – Server Implementierung

Sicherheit in Energiemanagementsystemen

- **IEC 62351** wurde von der WG 15 der IEC TC 57 entwickelt
- **IEC 62351** behandelt die Sicherheit der TC 57 Standards
- **IEC 62351** ist der aktuellste Standard für Sicherheit in Energiemanagementsystemen
- **IEC 62351** umfasst auch die Datenkommunikation
- **IEC 62351** beschreibt Maßnahmen zur Erfüllung der Grundforderungen an sichere Datenkommunikation / Datenverarbeitung:
  - Vertraulichkeit
  - Datenintegrität
  - Authentifizierung und
  - Unleugbarkeit (non-Repudiation)
- **IEC** 62351 definiert Rollenprofile mit unterschiedlichen Zugriffsrechten

IEC 62351 schließt die Standard-Serien: IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970 und IEC 61968 ein.

IEC 62351 Aufbau des Standards (1)

- Teil-1
  - Übersicht über das Gesamtdokument **IEC 62351** und Einführung in die informationstechnischen Sicherheitsaspekte für den Betrieb von Stromversorgungsanlagen
- Teil-2:
  - Glossar
- Teil-3:
  - Ende-zu-Ende Absicherung des Datenverkehrs für TCP/IP-basierte Verbindungen
  - Verwendung von TLS [RFC5246]
  - Client und Server Authentifizierung auf Basis von X.509-Zertifikaten

IEC 62351 Aufbau des Standards (2)

- Teil-4
  - Sicherheitsmaßnahme für MMS-basierte Protokolle (z.B. IEC 60870-6, IEC 61850)
  - Absicherung der Transportschicht gemäß IEC 62351-3
  - Definition eines Authentifizierungsmechanismus "SECURE" auf der Anwenderschicht für MMS-Assoziationen unter Verwendung von X. 509-Zertifikaten
- Teil-5:
  - Sicherheit für IEC 60870-5 und abgeleitete Protokolle (z.B. IEC 60870-5-104 / IEC 60870-5-101 / DNP 3.0) auf der Anwenderschicht
  - Zugriffsberechtigung auf kritische Ressourcen einer Unterstation
  - Rollen-basierten Zugriffsbeschränkungen (RBAC) und Erfassung sicherheitsrelevanter Ereignisse in Statistiken.

IEC 62351 Aufbau des Standards (3)

- Teil-6
  - Sicherheit für das IEC61850-Protokoll
  - Einsatz von VLAN-Markierungen und X.509-Signaturen bei GOOSE- und SMV-Telegrammen
- Teil-7
  - Sicherheit durch Einsatz von Tools zur Netzwerk- und Systemverwaltung, um eine
  - Überwachung der Stromnetz-Infrastruktur
  - Verwendung von MIB-Definitionen für IEDs
  - herstellerunabhängige relevante Systeminformationen bezüglich des Gerätes und der Kommunikationslinien
  - Verwendung des SNMP-Protokolls zum Austausch von MIB-Objekten

MIB: Management Information Base

IEC 62351 Aufbau des Standards (3)

- Teil-8
  - IEC 62351-8
    Definition von Methoden zur Verarbeitung und Verwaltung von Zugriffsrechten für Benutzer und Dienste
  - Rollen-basierten Zugriffskontrollsystems (RBAC)
  - vordefinierte Standard-Rollen und die Zugriffsrechte im Kontext von IEC 61850 (z.B. Auflistung aller Objekte in einem "Logischen Gerät")
  - Austausch von Identitätsinformation und Rollenname als ASN.1 Zugriff-Token
  - zentrale Verwaltung der Zugangsdaten über ein LDAP-System
  - Zugriff (PUSH- / PULL-Mechanismus) auf die Identitätsinformation des Kommunikationspartners

Die Identitätsinformation sowie der Rollenname wird in einem Zugriff-Token (ASN. 1-Syntax) abgelegt, der mit Hilfe verschiedener Transportmechanismen (X.509-Zertifikate, X.509-Attribut-Zertifikate, Software-Token) auf eine kryptographisch sichere Art zwischen den Systemen ausgetauscht

IEC 62351 Vordefinierte Rollen und Rechte

Value	Right / Role	VIEW	READ	DATASET	REPORTING	FILEREAD	FILEWRITE	FILEMNGT	CONTROL	CONFIG	SETTING GROUP	SECURITY
<0>	VIEWER	X			X							
<1>	OPERATOR	X	X		X				X			
<2>	ENGINEER	X	X	X	X		X	X		X		
<3>	INSTALLER	X	X		X		X			X		
<4>	SECADM	X	X	X			X	X	X	X	X	X
<5>	SECAUD	X	X		X	X						
<6>	RBACMNT	X	X					X		X	X	
<7 ... 32767>	Reserved	For future use of IEC defined roles.										
<32768 ... -1>	Private	Defined by external agreement. Not guaranteed to be interoperable.										

IEC 62351 Aufbau des Standards (4)

- Teil-9 : „Cyber Security“
  - Schlüssel-Management für Stromversorgungsanlagen,
  - korrekten und sicheren Umgang mit sicherheitskritischen Parametern, z.B. Passwörter, Verschlüsselungsschlüssel
  - Lebenszyklus von kryptografischer Information: Anmeldung, Erstellung, Verbreitung, Installation, Verwendung, Lagerung und die Entfernung
  - Umgang mit digitalen Zertifikaten (öffentlicher / privater Schlüssel)
  - Infrastruktur (PKI, X.509-Zertifikate) für asymmetrische Verschlüsselungsverfahren
  - Mechanismen bezüglich:
    - Zertifikatsanforderung (SCEP, CMP)
    - Zertifikatssperrung (CRL, OCSP)

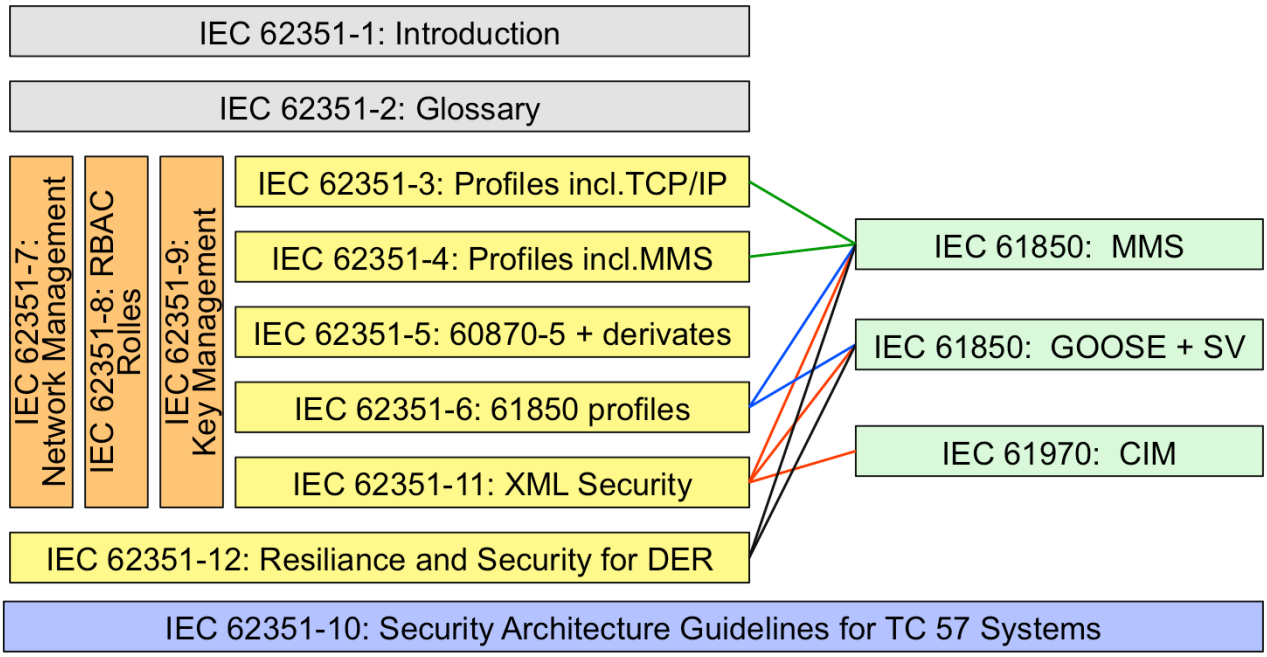
Bei Verwendung von symmetrischen Schlüsseln (z.B. Sitzungsschlüssel) wird ein Mechanismus zur sicheren Verteilung basierend auf GDOI [RFC6407] und IKEv2 [RFC7427] vorgestellt.

IEC 62351 Aufbau des Standards (5)

- Teil-10 : Sicherheitsarchitekturen
  - Sicherheits-Architekturen für die gesamte IT-Infrastruktur,
  - spezielle Sicherheitsanforderungen aus dem Umfeld der Stromerzeugung.
  - Identifizierung kritischer Stellen in der Kommunikationsarchitektur (z.B. Leitstelle zum Umspannwerk, Umspannwerk-Automatisierung)
  - geeignete Sicherheitsmechanismen (z.B. Datenverschlüsselung, Benutzerauthentifizierung)
  - Anwendung des Mechanismus' aus **IEC 62351** und bewährte Standards aus dem IT-Bereich (z.B. VPN Tunnel, Secure FTP, HTTPS)
- Teil-11
  - Sicherheit für XML-Dateien
  - Einbettung des originalen XML-Inhalts in einen XML-Container

Der XML Container ermöglicht wahlweise Verschlüsselung, X.509-Signatur für die Authentizität der XML-Daten

IEC 62351 Zuordnung



DER: Distributed Energy Resources

Weitere IEC 62391 Technical Reports und Standards:

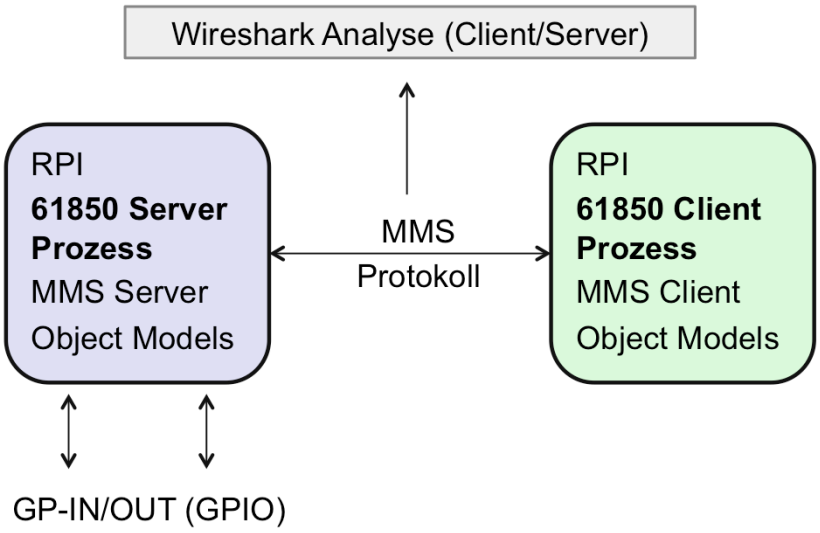
- IEC/TR 62351-13: Guidelines on What Security Topics Should Be Covered in Standards and Specifications
- IEC/TR 62351-90-1: Guidelines for Using Part 8 Roles
- IEC 62351-100-1: Conformance test cases for IEC 62351-5 and companion standards
- IEC 62351-14 Security Event Logging and Reporting
- IEC/TR 62351-90-2 Deep Packet Inspection

Kursinhalt

- Einführung
- Übersicht Protokolle
  - Stationsautomatisierung IEC 61850
  - Common Information Model IEC 61970
  - Sicherheit IEC 62351
- Anwendungsbeispiel
  - IEC 61850 Raspberry Pi Client – Server Implementierung

Open Source Bibliothek : libIEC61850

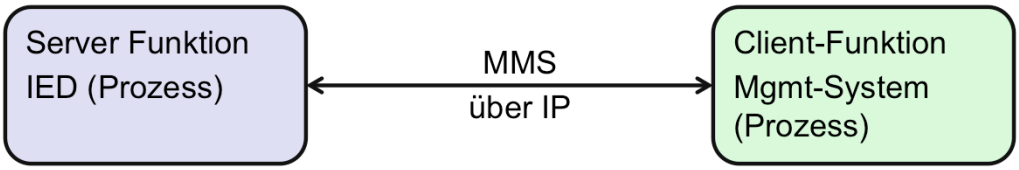
- IEC 61850 Client API mit MMS-client API
- IEC 61850 Server API mit MMS-server API



Notizen:

libice61850 Software

- API für Raspberry PI
- Application Programming Interface – API Implementierung
  - Client – Server Impelentierung für IEC 61850 Anwendungen
  - MMS Protokollstack für TCP/IP und GOOSE
  - Substation Configuration Description (SCD-File) wird bei der Software Produktion (nicht während der Kommunikation) verarbeitet



- Client / Server – Beispielprogramme
- Automatische Generierung des Server-Modell Codes static_model.c und static_model.h aus der icd - Datei

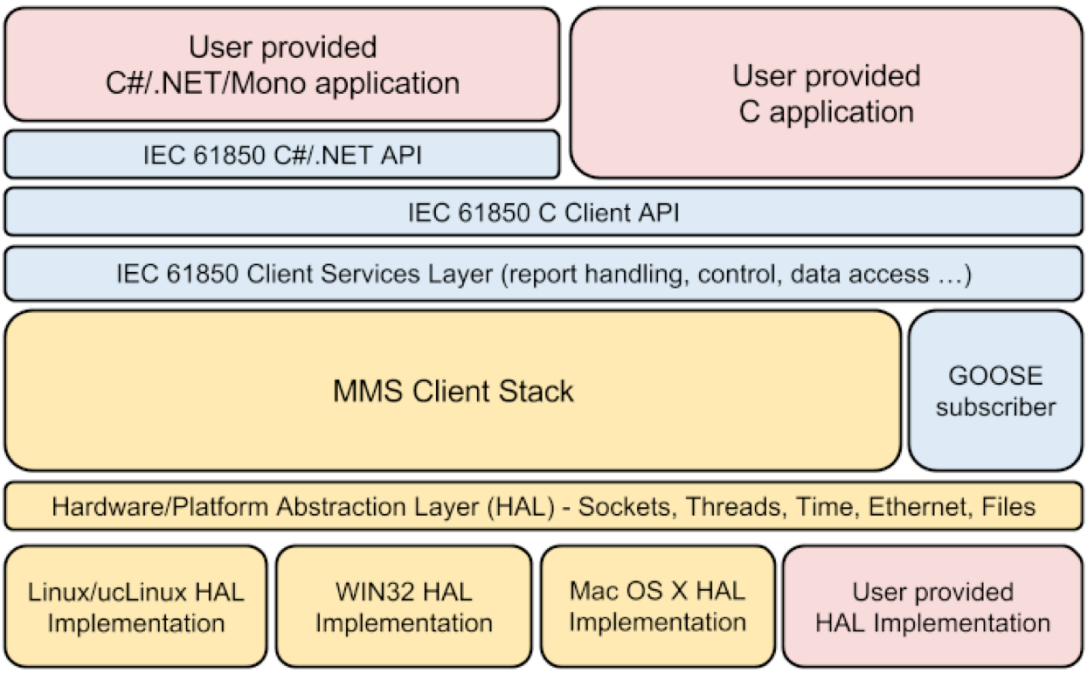
Für die Software gibt es verschiedene Testbeispiele:

- iec61850_client_example1
- iec61850_client_example2
- iec61850_client_example3 <- kann für alle Server-Beispiele verwendet werden
- iec61850_client_example4
- iec61850_client_example5

- server_example1
- server_example2
- server_example3
- server_example4
- server_example5

} IED Funktion / Konfiguration

Client Protokollstack

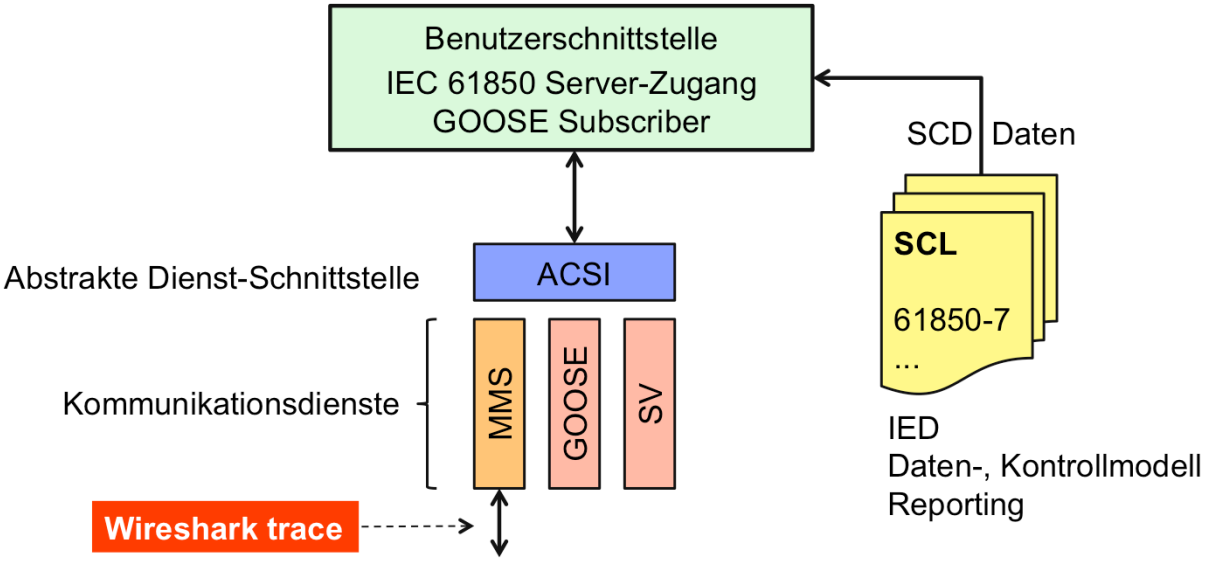


HAL-Schichten: Hardware Abstraction Layer
Anpassungsschicht an die jeweils verwendeten Betriebssysteme

MMS Server Stack: MMS-Protokollschichten

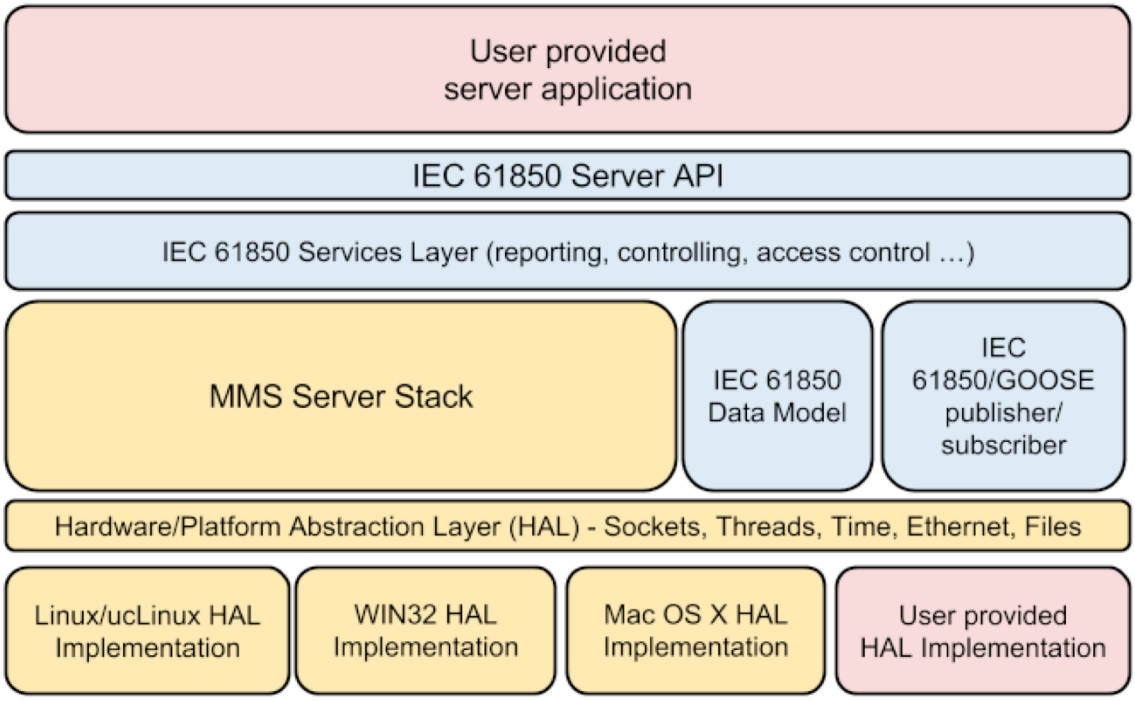
Client Anwendung

- Client API gemäß IEC 61850 ACSI (Abstract Communication Service Interface IEC 61850-7-2)
  - Kommunikationsmethoden: MMS, GOOSE, SV



Als Benutzerschnittstelle wird während des Tests die Unix-Shell verwendet.
Client und Server befinden sich auf der selben Raspberry Hardware und kommunizieren intern über das Loopback-Interface (127.0.0.1).
Die Kommunikation wird mittels Wireshark überprüft.

Server Protokollstack

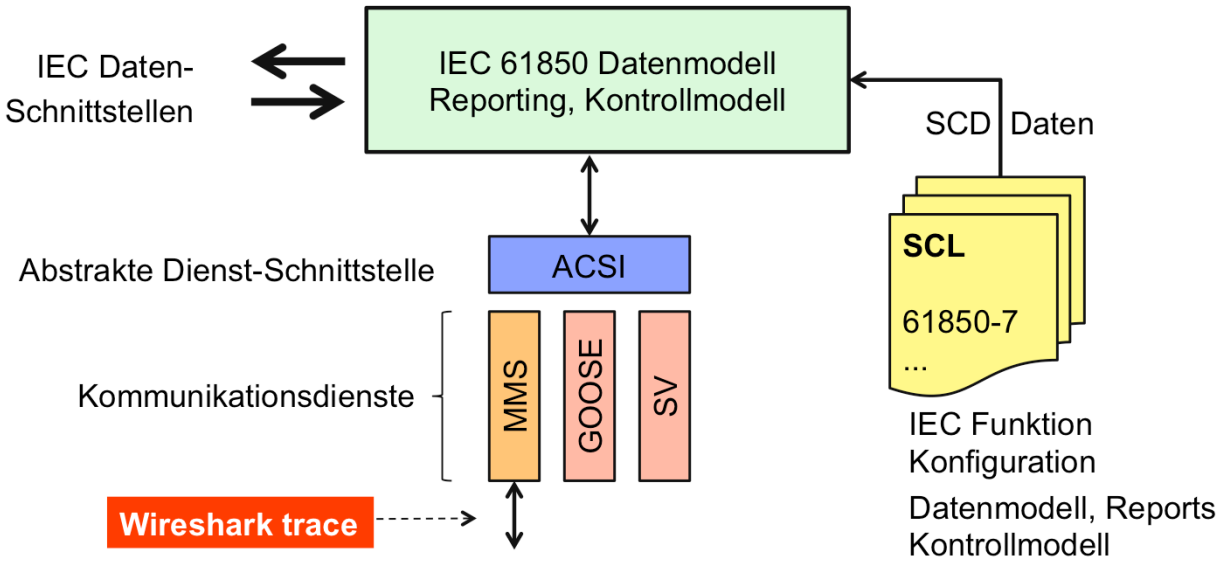


HAL-Schichten: Hardware Abstraction Layer unterstützt die Portierung auf unterschiedliche Hardware Plattformen
Anpassungsschicht an die jeweils verwendeten Betriebssysteme

MMS Server Stack: MMS-Protokollschichten
IEC 61850 Datenmodell: wird durch Konfigurationsdateien (SCD, ICD, CID) beschrieben

Server Anwendung (IDE)

- Server API gemäß IEC 61850 ACSI (Abstract Communication Service Interface IEC 61850-7-2)
  - Kommunikationsmethoden: MMS, GOOSE, SV



Die Server-Anwendung bildet die IED-Funktionen ab.
Client und Server befinden sich auf der selben Raspberry Hardware und kommunizieren intern über das Loopback-Interface (127.0.0.1).
Die Kommunikation wird mittels Wireshark überprüft.

Die IED-Testbeispiele verwenden keine Raspberry – Ressourcen, wie z.B. GPIO-Pins Systemdaten, etc. Die Testbeispiele können durch die Implementierung entsprechender Software-Funktionen erweitert werden.

Zugang zum Raspberry Pi

- Zugang über **Putty** (ssh) oder über ein Linux **shell-Fenster**
  - ssh pi@<IP-Adresse des Raspberry Pi>
  - Passwort: raspi
  - Raspberry Pi Kommando-Promt

  } ssh remote access
- Alternativ: über eine Remote Desktop (xrdp) Verbindung
- **Protokollanalyse – Tool für MMS-Nachrichten**
  - Analysetool: wireshark
    - Raspberry – Version kann MMS (noch) nicht dekodieren
  - **Workaround**:
    - Verwendung der dumpcap – Trace-Funktion:
      Programmaufruf ohne Parameter: **sudo dumpcap - i lo**
      erzeugt ein pcap-Dateiformat im /tmp-Verzeichnis
    - kopieren der pcap-Datei auf den PC (mit mc etc.)
      Analyse auf dem lokalen PC mit Wireshark

Verwendung der libice61850 Beispiele

- Verzeichnis auf dem Raspberry Pi:
  - /home/pi/IEC61850/libiec61850-0.9.2.1

- Verzeichnis der **Beispiele:**
  - libiec61850-0.9.2.1/examples

- Die Beispiele bestehen aus Client – Server Programmen die auch auf einem Raspberry (IP = 127.0.0.1 localhost) gegeneinander ablaufen können
  - **Client-Dateien**: Iec61850_client_example1 ... 5
  - **Server-Dateien**: server_example1 ... 5
  - **MMS-Utility**: (Client-Funktion): examples/mms_utility

iec61850 Beispiele

- Inhalt der Verzeichnisse
  - **Client** :

Verzeichnis:	z.B. *iec61850_client_example2*
ausführbare Datei:	client_example2
C-Code:	client_example2.c
Compiler-Dateien:	Makefile und CMakeLists

  - **Server**:

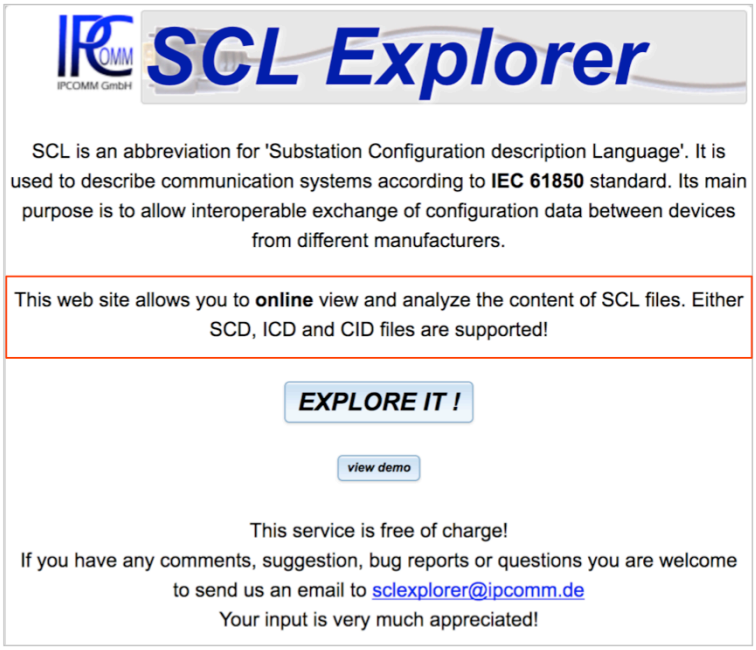
Verzeichnis:	z.B. *server_example3*
ausführbare Datei:	server_example3
C-Code:	server_example3.c
Datenmodell-Beschreibung:	static_model.h, static_model.c
ICD-Datei:	simpleIO_direct_control.icd
Compiler-Dateien:	Makefile und CMakeLists

- Auswertung / Analyse der ICD-Datei mit Hilfe von Tools wie z.B. IEDScout oder der Online-Analyse von IPComm.

Darstellung der ICD – Struktur

Auswertung von SCL-Dateien (alternativ auch über IEDScout):

- http://www.scl61850.com/-XbgiB-3_View



ICD Analyse:

- Analysieren Sie die Struktur der ICD-Datei von Server3:
  - Datenobjekte in LLN0
  - Kommunikations-Parameter
  - LN-Types
  - Data Type Templates

Die verwendeten IED-Funktionen können mittels SCD-, ICD-, oder CID-File beschrieben werden. Die vorliegenden Beispiele verwenden das ICD-Fileformat.

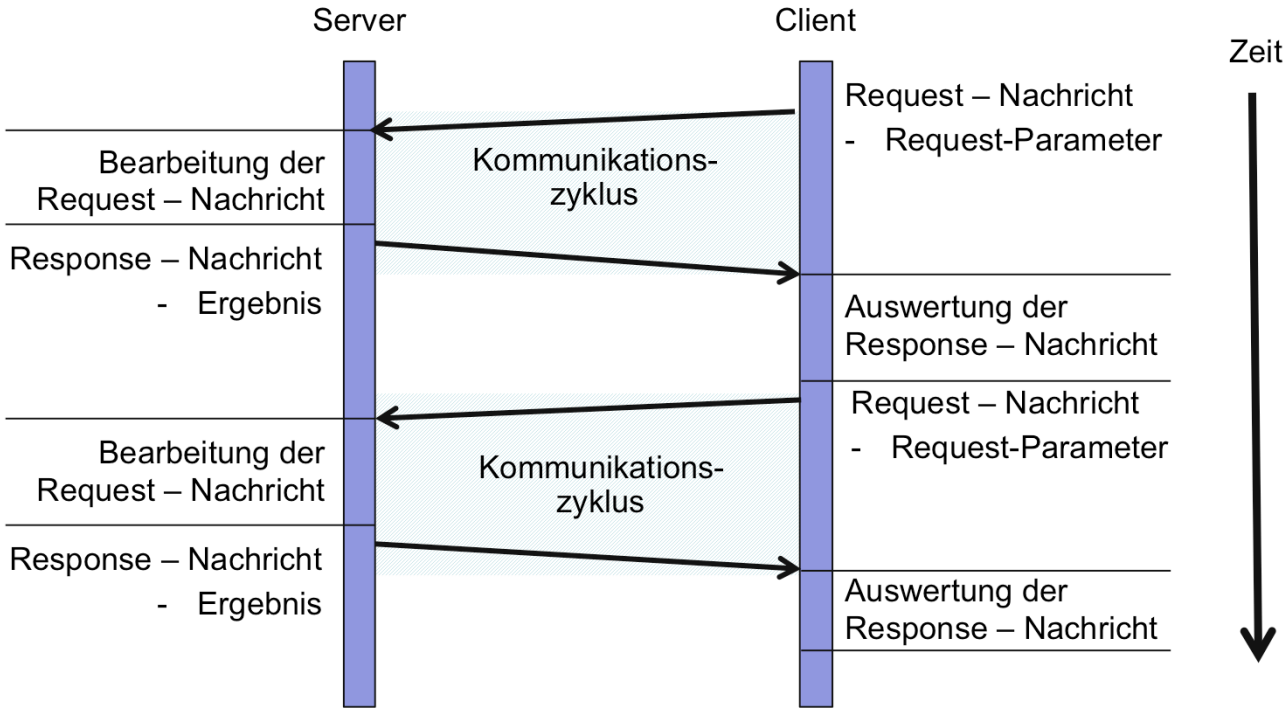
Änderungen können mittels geeigneter Tools (IEDScout) durchgeführt werden. Kleinere Anpassungen manuell in der XML-Datei.

MMS – Analyse (1)

- Mit dem Raspberry verbinden über ssh oder remote desktop
  3 Verbindungen: Fenster1: **client** Fenster2: **server** Fenster3: **wireshark**
- Wechseln Sie zum **Server-Fenster** in das Verzeichnis:
  cd /home/pi/IEC61850/libiec61850-0.9.2.1/examples/server_example3
- Wechseln Sie zum **Client-Fenster** in das Verzeichnis:
  cd /home/pi/IEC61850/libiec61850-0.9.2.1/examples/iec61850_client_example2
- Aktivieren Sie zunächst den Server:
  sudo ./server_example3 -> Ausgabe: *Using libIEC61850 version 0.9.2*
- Wechseln Sie zum **WiresharkFenster:**
  dumpcap -i lo
- Wechseln Sie zum Client Fenster und aktivieren Sie den Client:
  sudo ./client_example2
- Wechseln Sie zum **wireshark-Fenster**:
  Beenden Sie den Prozess mit *Ctr-C*

Die Eingaben sind kursiv dargestellt.
Alle Programme müssen mit Root-Rechten ausgeführt werden den Kommandos immer ein „sudo“ vorangestellt.

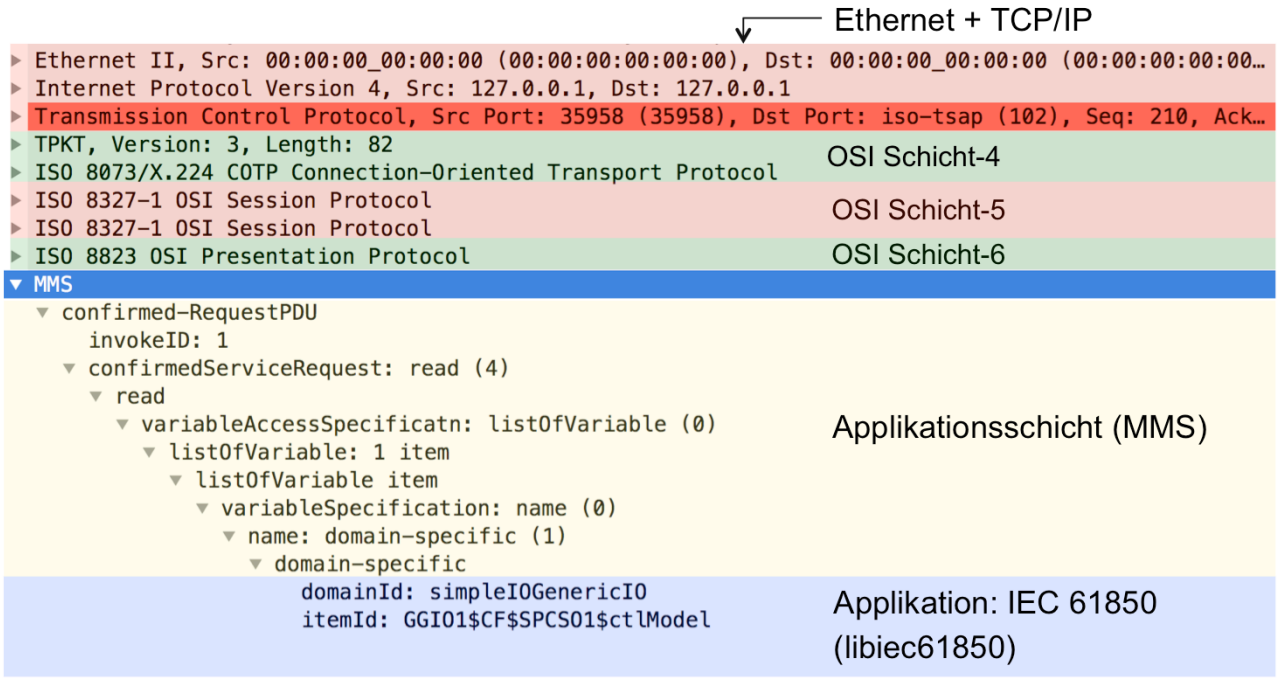
Client – Server Kommunikation



MMS – Analyse (2)

- Kopieren Sie die wireshark Trace-Datei auf einen USB-Stick:
  - USB-Stick lokalisieren: *ls - l /media/pi* -> USB-Stick Verzeichnis z.B.: B2E7-2AD3
  - *cp tmp/wireshark* /media/pi/B2E7-2AD3*
  - Wireshark auf dem PC öffnen und Trace-Datei auswählen z.B: *wireshark_pcapng_Loopback_20160909204456_ENtGPg*
- Identifizieren Sie den MMS-Verbindungsaufbau
  - Welche Protokollschichten werden dargestellt ?
- Identifizieren Sie die MMS-Kommunikation
  - Welche Protokoll-Operationen sind im Trace dargestellt?

Wireshark Trace Beispiel



Protokollschichten:

Schicht-1 und Schicht-2:	Ethernet Protokoll: IEEE 802.3
Schicht-3:	Internet
Schicht-4:	TCP (IETF Transportschicht)
Schicht-4: Adaption	ISO Transport Service on Top of TCP RFC 2126 (Weiterentwicklung von RFC 1006)
Schicht-4: Adressierung	ISO 8073 (TSAP-adressing <-> Port addressing) X.224 (OSI Transport-Schicht)
Schicht-5:	Session Protocol (connection oriented)
Schicht-6:	Presentation Protocol (connection oriented)
Schicht-7:	MMS (Applikationsschicht = IEC 61850-8-1)
Applikation:	IEC 61850

MMS – Analyse (3)

- Weitere Client – Server Kommunikationsbeispiele:
  - server_example3 mit:
    - Iec61850:client_example2
      Welche MMS-Funktion wird aktiviert?
    - Iec61850:client_example4
      Welche MMS-Funktion wird aktiviert?
    - mms_utility
      Pogrammaufruf mit Parameter: -h
      zeigt die Liste der verfügbaren Funktionsaufrufe
    - Probieren Sie die Funktionen aus und erstellen Sie für jede einen Wireshark Trace