DHBW CAS
Duale Hochschule
Baden-Württemberg
Center for Advanced Studies

Energieinformationstechnik

Teil 1

Stationsautomatisierung

Ausgabe 0.5, 31.10.2024
Autoren: Stephan Rupp

Kontakt: stephan.rupp@srupp.de
Web: http://www.srupp.de

Inhaltsverzeichnis

1. ...

1.1. ...

...

1.2. ...

...

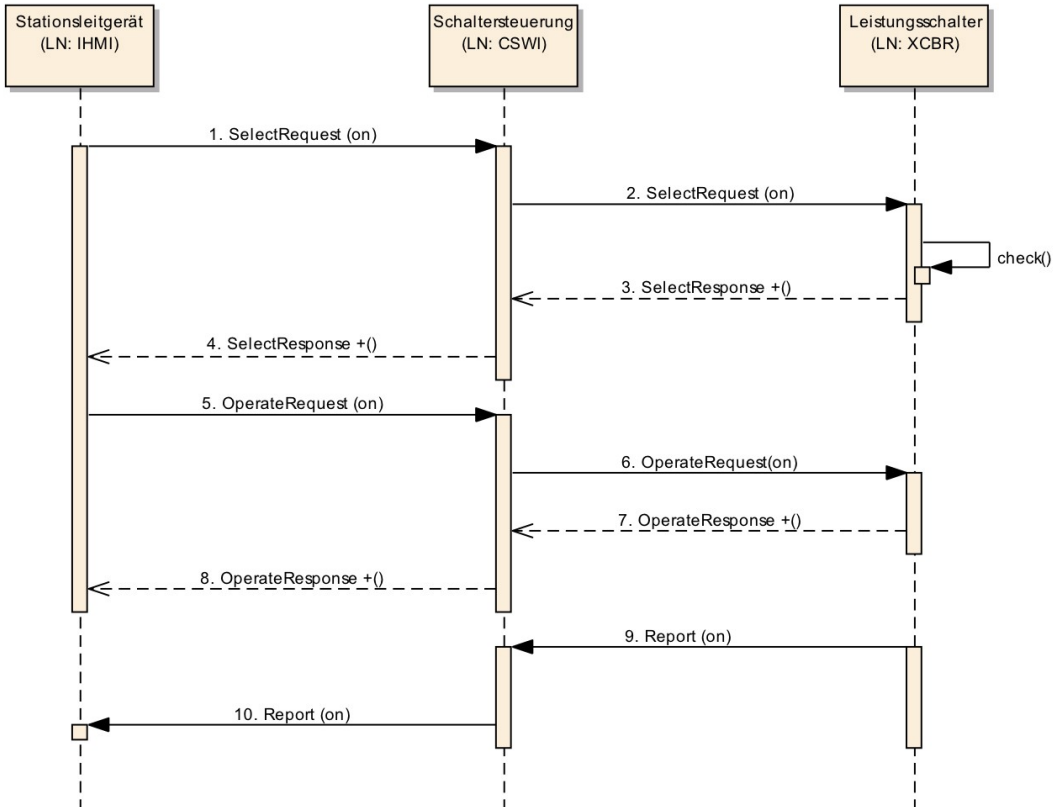
...

1.3. ...

…

1.4. Stationsautomatisierung

In einem zur Stationsautomatisierung in der elektrischen Energieversorgung eingesetzten Feldbus werden zum Lesen und Schreiben von Datenobjekten Nachrichten nach einem vorgege-benen Muster ausgetauscht, wie in folgender Abbildung gezeigt.



Frage 1.7.1: Rekonstruieren Sie dieses Muster für den Nachrichtenaustausch aus dem Sequenz-diagramm in der Abbildung.

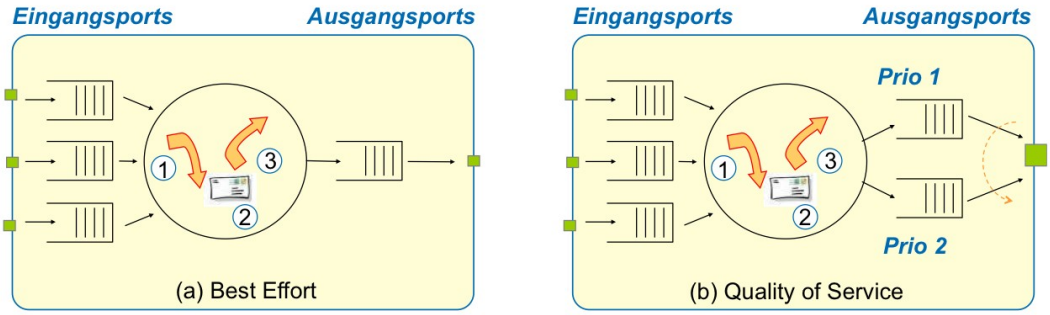
Lösung: Das Muster für den Nachrichtenaustausch arbeitet in 3 Phasen: (1) Select - Auswahl einer Funktion, (2) Operate - Ausführen einer Instruktion, (3) Report - Bericht über das Ergebnis der Ausführung. In den Phasen (1) und (2) sind Nachrichten für die Anforderungen (Request) und die Quittierung der Anforderung (Response) vorgesehen.

Frage 1.7.2: Welche weitere Vereinbarungen sind erforderlich, damit der Aufruf von Methoden zwischen den Geräten funktionieren kann?

Lösung: (1) Wenn die Methodenaufrufe über ein Netz erfolgen, ist eine Pfadangabe erforderlich, bestehend aus Protokoll, Netzadresse und Objektname (für die Methode). Eine solche Pfadangabe kann in einem IP-Netz beispielsweise durch eine URL erfolgen, bzw. ein TCP-Socket bzw. UDP-Socket. (2) Ausserdem sind Vereinbarungen über den Methodenaufruf erforderlich, d.h. die Namen der Methode, der Übergabeparameter, der Rückgabewerte und die jeweils zugehörigen Datentypen

Frage 1.7.3: Echtzeitverhalten. Die Steuergeräte kommunizieren über eine Kette von Ethernet-Switches. Auf Schicht 2 variieren die Paketlängen zwischen 64 Bytes pro Nachricht und maximal 1500 Bytes pro Nachricht. Es wird Fast Ethernet verwendet (100 Mbit/s). Die Prozess-daten verwenden stets kurze Pakete von 64 Bytes.

Es wird überlegt, ob ein Best Effort Verfahren genügt (Fall (a), linker Teil der Abbildung) oder eine Einteilung in 2 Verkehrsklassen mit Priorisierung eingeführt werden soll (Fall (b), rechter Teil der Abbildung). Erläutern Sie beide Verfahren sowie die Unterschiede.



(1) Best Effort Verfahren: Alle Pakete bzw. hier Ethernet-Rahmen werden in der Reihenfolge ihres Eintreffens an den Ausgangsport gegeben. Ein kurzer Rahmen mit zeitkritischen Prozessdaten wird daher am Ausgangsport unter Umständen hinter langen Rahmen mit Überwachungsinformationen oder sonst welchen Daten, die nicht zeitkritisch sind.

(2) Quality-of-Service Verfahren: Es werden mehrere Klassen von Daten eingeführt, beispielsweise Klasse 1: Prozessdaten, Klasse 2: alle anderen Daten. Rahmen mit Prozess-daten werden markiert (z.B. Tag, Eintrag im Type-of-Service Feld) und in den Switches bevorzugt behandelt. Die Bevorzugung besteht in der Einordnung der Prozessdaten in einer höher priorisierten Warteschlange am Ausgangsport (Prio 1 Schlange). Somit wird die Dauer der Abfertigung von der Reihenfolge des Eintreffens entkoppelt. Dadurch wird die Situation vor allem bzgl. die langen, niedrig priorisierten Rahmen verbessert (Prio 2 Schlange). Beim Arbeiten mit mehreren Verkehrsklassen (Quality-of-Service Verfahren), wird in jedem Knoten (Switch) der Verkehr gemäß Verkehrsklassen neu sortiert.

Frage 1.7.4: Die Signalkette enthält bis zu 10 Knoten (Switches), wobei jeder Knoten über 3 Eingangsports verfügt, über die sowohl regulärer Verkehr als auch Prozessdaten kommuniziert werden. Vergleichen Sie die maximalen Laufzeitschwankungen für beide Verfahren (Fall (a) und Fall (b)) aus der Perspektive der Prozessdaten.

Bei 3 Eingangsports besteht der ungünstigste Fall darin, dass an jedem Fall ein maximal langer Rahmen mit unkritischen Daten eintrifft, bevor an einem der Ports ein kurzer Rahmen mit kritischen Prozessdaten eintrifft. (Bemerkung: Vorausgesetzt, die Ankunftsrate ist niedrig im Vergleich zur Service-Rate, d.h. Systemausnutzung unter 50%, andernfalls kann es beliebig lange Warteschlangen an den Eingangsports geben).

Fall (a), Best Effort: Anordnung am Ausgangsport gemäß Reihenfolge beim Eintreffen, d.h. der Rahmen mit Prozessinfo kommt erst auf die Leitung, nachdem die 3 langen Rahmen übertragen sind. Im

ungünstigsten Fall bei 10 Knoten: 3 * 10 * Latenz (1500 Bytes bei 100 Mbit/s) = 30 * 0,120 ms = 3,6 ms. In der Realität ergeben sich Laufzeitschwankungen bis zu diesem Wert.

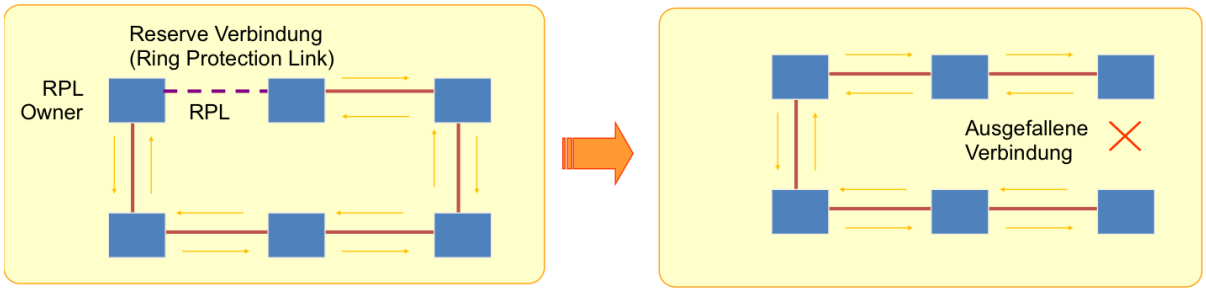
Fall (b), Quality-of-Service mit 2 Verkehrsklassen: Die drei langen Rahmen mit unkritischen Daten landen in der Reihenfolge ihres Eintreffens in der Prio 2 Schlange am Ausgangsport. Der Rahmen mit Prozessdaten wird nach Eintreffen in der Prio 1 Schlange platziert. Zu diesem Zeitpunkt ist allerdings einer der langen Rahmen bereits in Bearbeitung. Allerdings erfolgt die Übertragung des Rahmens mit Prozessdaten unmittelbar dann, wenn diese Übertragung beendet ist. Der Rahmen mit Prozessdaten kommt somit auf die Leitung, sobald 1 langer Prio 2 Rahmen übertragen ist. Im ungünstigsten Fall bei 10 Knoten: 1 * 10 * Latenz(1500 Bytes bei 100 Mbit/s) = 10 * 0,120 ms = 1,2 ms.

Verbesserung von (b) gegenüber (a): Latenz(b)/Latenz(a) = 3

Frage 1.7.5: Durch welche Massnahmen lassen sich die Laufzeitschwankungen weiter reduzieren?

- Reduktion der Knoten in Reihe (z.B. weniger als 10 Switches in der Kette)
- Reduktion der Eingangsports (z.B. 2 statt 3 Eingangsports)
- Einschränkungen der maximal erlaubten Rahmenlänge (z.B. max 512 Bytes pro Rahmen)
- Erhöhung der Übertragungsrate (z.B. 1Gbit/s statt 100 Mbit/s)
- Einsatz von Sammelpaketen (vgl. Ethercat) Zeitmultiplex (vgl. Profinet)

Frage 1.7.6: Redundanz. Zur Verbesserung der Ausfallsicherheit wird die lineare Verbindung zwischen den Switches auf eine Ringkonfiguration erweitert. Die Netztopologie bleibt hierbei linear, d.h. es gibt eine physikalisch vorhandene Reserveverbindung.



Beschreiben Sie, was beim Ausfall einer Verbindung geschieht (d.h. den Übergang auf den in der Abbildung links gezeigten Zustand auf den Zustand rechts).

(1) Überwachung der Funktion des Ringes durch einen ausgewählten Switch (den RPL-Owner): beispielsweise durch Senden und Empfangen von von Kontrollnachrichten in beiden Richtungen (auch über die für regulären Verkehr nicht benutzte Reserveverbindung).

(2) Ausfall einer Verbindung: Wird durch die Überwachung (vom RPL-Owner) bemerkt.

(3) Aktivieren der Reserveverbindung

(4) Inbetriebnahme der neuen Topologie (z.B. durch Spanning-Tree Algorithmus)

Frage 1.7.7: Welchen Nachteil hat dieses Verfahren bzgl. des Echtzeitverhaltens des Netzes?

(1) Das Verfahren ist mit Umschaltzeiten verbunden (Schritte (1) bis (4) oben, speziell Schritt (4) erfordert einige Zeit).

(2) Während dieser Zeit ist keine reguläre Zustellung des Verkehrs möglich. Zwar gehen für Anwendungen keine Daten verloren, da die höheren Protokollschichten diese nochmals anfordern, allerdings werden während des Umschaltvorgangs vereinbarte Antwortzeiten nicht eingehalten. Somit ist ein Echtzeitbetrieb (= Einhaltung vereinbarter Antwortzeiten) nur sehr eingeschränkt möglich.

(3) Die Dauer der Umschaltung ist abhängig von der Topologie und Größe des Netzes.

Frage 1.7.8: Erhöhte Anforderungen an die Verfügbarkeit. Die Anbindung an die übergeordnete Leitebene hat noch höhere Anforderungen bzgl. der Verfügbarkeit. Daher wird hierfür eine Aus-führung als echter Doppelring vorgeschlagen, wie in der folgenden Abbildung gezeigt.

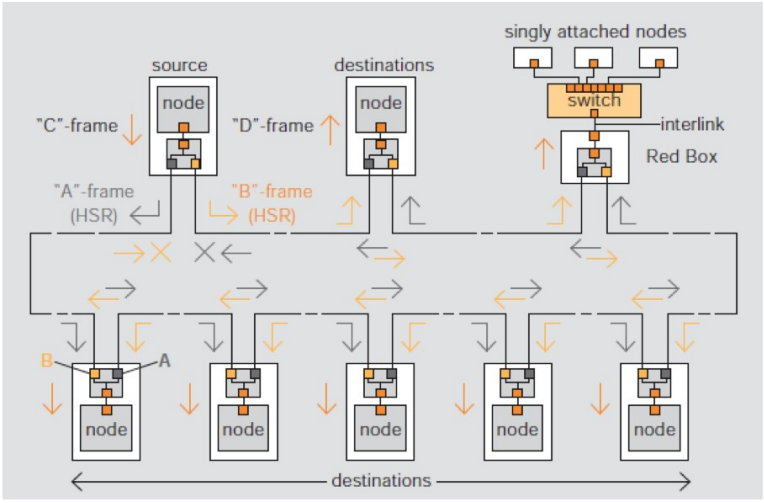
Vergleichen Sie die echte Doppelring-Konfiguration mit einfachen der Konfiguration als Ring bzgl. Ausfallsicherheit und Aufwand. Beschreiben Sie das Verhalten im Fehlerfall.

- Ausfallsicherheit: besser, da (1) doppelte Verbindungen statt doppelt betriebener Verbindungen, (2) Ausfall einzelner Switches betreffen nur einen Ring (statt beider Ringe)
- Aufwand: (1) doppelter Hardware-Aufwand (Knoten, Verbindungsleitungen, Trassen), (2) keine komplexe Konfiguration (zwei wirkliche LANs statt VLAN), (3) leichterer Austausch von Komponenten (z.B. fehlerhafte Verbindungsleitungen und Knoten)

Ringredundanz mit zwei gleichzeitig betriebenen VLANs

Red Box: Ringswitch mit Dopplung der Anschlüsse für Geräte mit einfachem Anschluss (SAN - Single Attached Node)

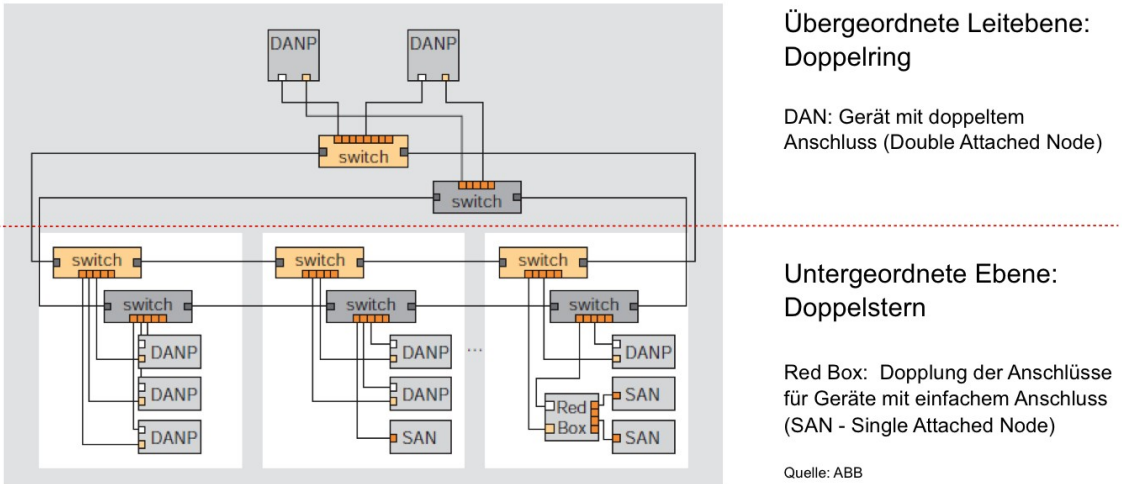
Node: Geräte (Feldbus-Controller, Schutzgeräte, Messgeräte)



Quelle: ABB

- Verhalten im Fehlerfall: unterbrechungsfreier Betrieb; bei Einzelfehlern weiterhin Redundanz im verbliebenen Ring verfügbar (z.B. mit Verfahren nach Teil 1)

Frage 1.7.9: Höchste Verfügbarkeit. Die Anbindung an die übergeordnete Leitebene hat noch höhere Anforderungen bzgl. der Verfügbarkeit. Daher wird hierfür eine Ausführung als echter Doppelring vorgeschlagen, wie in der folgenden Abbildung gezeigt.



Übergeordnete Leitebene: Doppelring

DAN: Gerät mit doppeltem Anschluss (Double Attached Node)

Untergeordnete Ebene: Doppelstern

Red Box: Dopplung der Anschlüsse für Geräte mit einfachem Anschluss (SAN - Single Attached Node)

Quelle: ABB

Vergleichen Sie die echte Doppelring-Konfiguration mit der Konfiguration oben bzgl. Ausfallsicherheit und Aufwand. Beschreiben Sie das Verhalten im Fehlerfall.

- Ausfallsicherheit: besser, da (1) doppelte Verbindungen statt doppelt betriebener Verbindungen, (2) Ausfall einzelner Switches betreffen nur einen Ring (statt beider Ringe)
- Aufwand: (1) doppelter Hardware-Aufwand (Knoten, Verbindungsleitungen, Trassen), (2) keine komplexe Konfiguration (zwei wirkliche LANs statt VLAN), (3) leichterer Austausch von Komponenten (z.B. fehlerhafte Verbindungsleitungen und Knoten)
- Verhalten im Fehlerfall: unterbrechungsfreier Betrieb; bei Einzelfehlern weiterhin Redundanz im verbliebenen Ring verfügbar (z.B. mit Verfahren nach Teil 1)

Frage 1.7.10: Als Alternative zu der oben vorgeschlagenen speziellen Ringkonfiguration wird in dem weiter unten gezeigten Vorschlag auf der untergeordneten Ebene eine Variante mit doppelter Sternkonfiguration gezeigt. Vergleichen Sie die Doppelsternkonfiguration mit der Konfiguration in Teil 2 bzgl. Ausfallsicherheit und Aufwand. Beschreiben Sie das Verhalten im Fehlerfall.

Frage 1.7.11: In den oben beschriebenen Verfahren werden Ethernet Rahmen dupliziert. Beschreiben Sie eine Methode, mit der ein Gerät auf möglichst einfache Weise Duplikate erkennen und ggf. verwerfen kann.

- Sequenznummern für jedes Frame (anwendungsspezifische Erweiterung, bzw. spezifisch für dieses Verfahren zur Erzeugung redundanter Rahmen)
- MAC-Adresse der Quelle (Standard Ethernet)
- Rahmen von der gleichen Quelle mit gleicher Sequenznummer können verworfen werden.
- Bemerkungen: (1) Rahmen werden erst verworfen, nachdem der Empfang eines Duplikat festgestellt wurde. (2) Solch einfache Verfahren lassen sich hardware-nah implementieren. Auf Anwendungsebene gibt es natürlich weitere Möglichkeiten. (3) Das Verfahren sollte möglichst wenige falsch negative Identifikationen liefern, d.h. möglichst wenige gültige Rahmen, die irrtümlich als Duplikate verworfen werden. Hierzu ist erforderlich, dass einerseits die Tabellen mit gültigen Sequenznummern altern, andererseits die Sequenznummer hinreichend viele Stellen besitzt (z.B. 16 Bits), um fehlerhafte Identifikationen bedingt durch Zählerüberlauf auszuschließen.

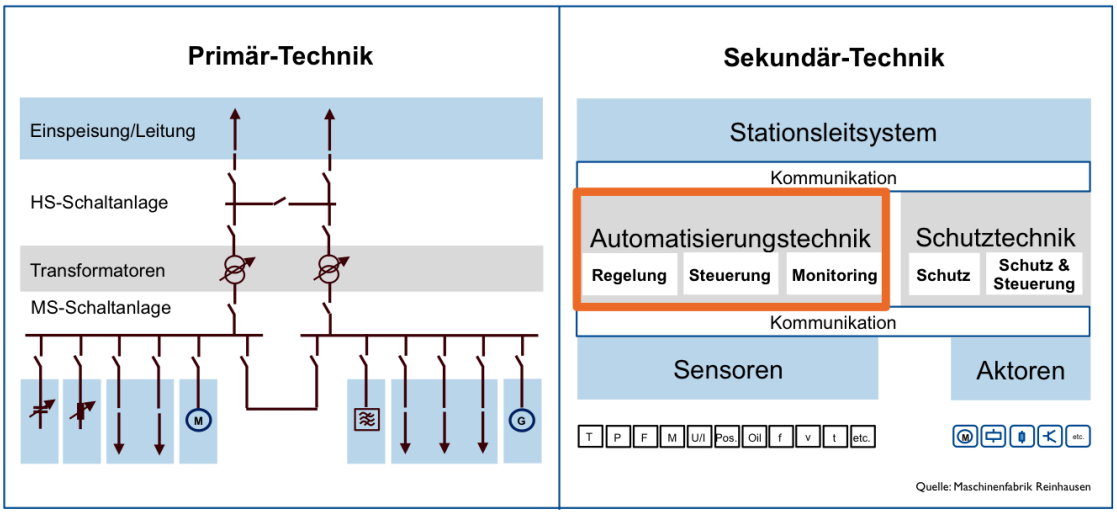
Frage 1.7.12: Erläutern Sie mögliche Einsatzfälle für die bisher genannten Verfahren in der Stationsautomatisierung.

2. …

5. Leittechnik

5.1. Primärtechnik und Sekundärtechnik

Folgende Abbildung zeigt eine Übersicht über den Aufbau einer Umspannstation.



Betriebsmittel

Informations- und Kommunikationstechnik

Die linke Seite der Abbildung zeigt den Aufbau der Anlage: Leitungen auf der Hochspan-nungsseite werden auf eine Sammelschiene geführt (HS-Schaltanlage). Zwei Transformatoren binden diese an zwei Sammelschienen der Mittelspannungsebene an (MS-Schaltanlage). Auf der Seite der Mittelspannung sind Lasten, Erzeuger und Leitungen angeschlossen.

Frage 5.1.1: Primärtechnik. Die Betriebsmittel der Anlage, die im Stromkreis liegen, werden als Primärtechnik bezeichnet. Woher kommt diese Bezeichnung? Welche Betriebsmittel sind sekundär?

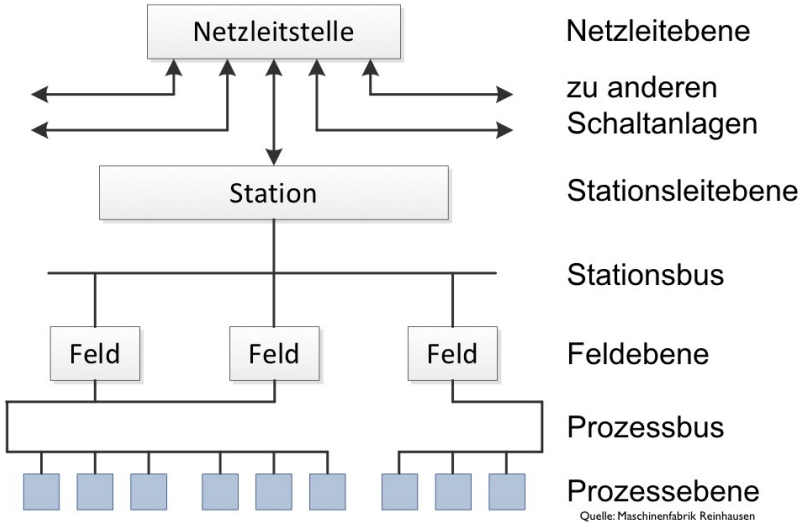
Frage 5.1.2: Sekundärtechnik. Unter Sekundärtechnik werden die Betriebsmittel verstanden, die zur Steuerung der Anlage dienen, d.h. die Informations- und Kommunikationstechnik. Erläutern Sie die Funktion der auf der rechten Seite der Abbildung gezeigten Komponenten. Welche Aufgaben hat die Automatisierungstechnik? Welche Anlagen im Umspannwerk werden hierdurch betrieben? Welche Aufgaben hat die Schutztechnik?

Frage 5.1.3: Mengengerüst. Die Leistung zur Hauptbetriebsstunde im deutschen Stromnetz beträgt ca 80 GW. Ein Mittelspannungstransformator (HS/MS) hat eine typische Leistung von 40 MVA. Wie viele Umspannwerke gibt es demnach schätzungsweise im deutschen Stromnetz? Sind diese Umspannwerke bemannt? Wie werden Umspannwerke betrieben? Welche Aufgaben besitzt eine Leitstelle? Wie weit ins Stromnetz reicht der unmittelbare Einfluss einer Leitstelle?

Frage 5.1.4: Redundanz. In der Abbildung sind alle Betriebsmittel gedoppelt. Welchen Zweck verfolgt diese Redundanz? Recherchieren Sie im Web nach Umspannwerken und verschaffen Sie sich einen Überblick über deren Aufbau. Wie sehen Schutzgeräte aus? Wo finden sich Geräte zur Automatisierung?

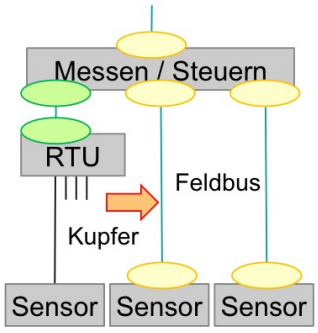
5.2. Entwicklung der Leittechnik

Die Leittechnik in einem Umspannwerk ist hierarchisch aufgebaut und umfasst die Sensoren, Aktoren, Geräte auf Feldebene und übergeordnete Geräte. Folgende Abbildung zeigt eine Übersicht.



Frage 5.2.1: Vergleichen Sie den Aufbau der Leittechnik mit der Automatisierung in der industriellen Fertigungstechnik bzw. mit der Leittechnik für ein Schienenfahrzeug oder Strassenfahrzeug. Welche Unterschiede bestehen? Welche Ähnlichkeiten gibt es? Was versteht man unter einem Feld bzw. einem Feldgerät?

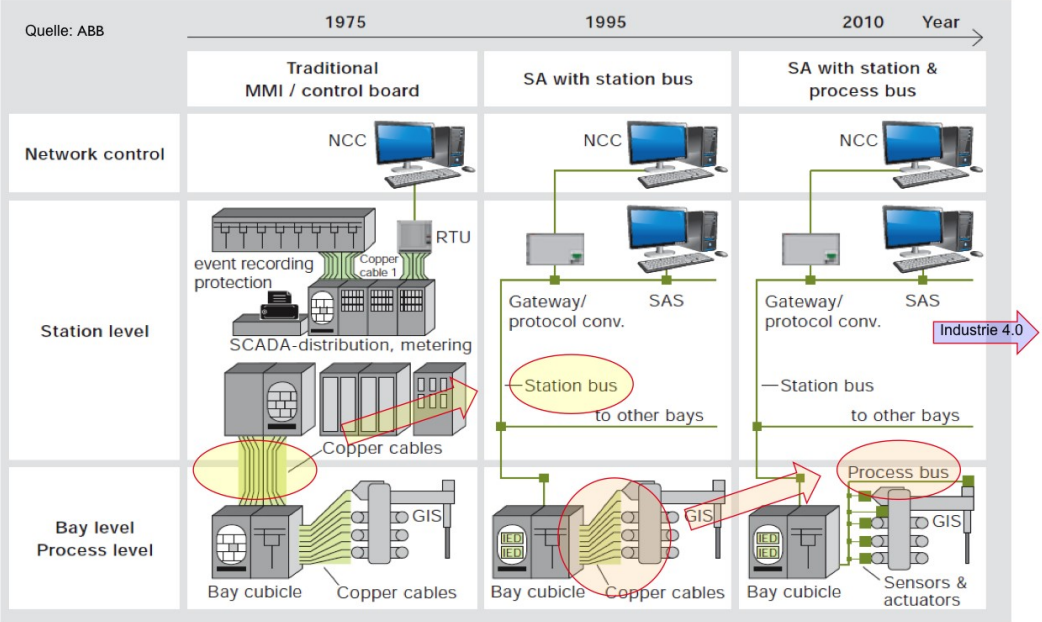
Frage 5.2.2: Technische Entwicklung. Traditionell wurden Sensoren (Stromwandler, Spannungswandler, Thermometer, Melder über Schalterzustände etc.) mittels Kupferdrähten angeschlossen und zu Stationsgeräten, Mosaiktafeln oder über Konzentratoren (abgesetzte Einheit, RTU = Remote Terminal Unit) zur nächsten Ebene verdrahtet, ganz wie in der industriellen Produktion. Die Kupferleitungen zwischen Stationsgeräten und zu den Sensoren und Aktoren im Feld werden zunehmend durch Feldbusse abgelöst. Folgende Abbildung zeigt das Prinzip dieser Entwick-lung.



Welchen Vorteil bietet ein Feldbus zwischen Stationsgerät und abgesetzter Einheit? Welchen Vorteil bietet ein Feldbus zu Sensoren und Aktoren? Welche Voraussetzungen sind hierfür erforderlich? Welche Nachteile hat der Feldbus gegenüber der Kupferschnittstelle?

Lösung: (1) Vorteile: Wesentlich geringerer Verdrahtungsaufwand (Investitionskosten und laufende Kosten), (2) Vorraussetzungen für Sensoren und Aktoren am Feldbus: Verfügbarkeit intelligenter Sensoren (Sensoren mit Mikrocontroller), (3) Nachteile: Die Kupferschnittstelle mit Stromvorgabe (z.B. 1A) ist unter allen Herstellern universell und kompatibel. Bei einem Feldbus müssen Protokolle und Inhalte der Nachrichten spezifiziert werden zur Interoperabilität zwischen Geräten unterschiedlicher Hersteller.

Frage 5.2.3: Von der Kupferleitung zum Feldbus. Folgende Abbildung zeigt die historische Entwicklung etwas mehr im Detail. Erläutern Sie die Historie der Stationsautomatisierung (SA).

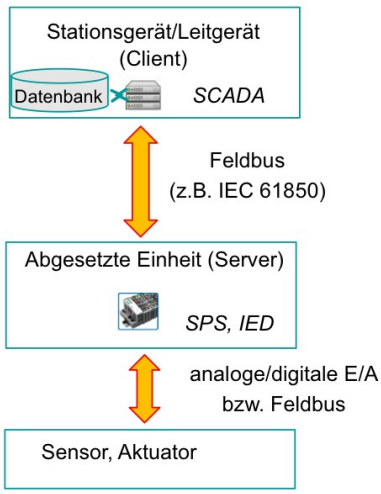


Was ist mit Stationsbus bzw. Prozessbus bezeichnet? Wie schätzen sie die weitere Entwicklung in den kommenden 25 Jahren ein?

Frage 5.2.4: Hierarchie der Systeme. Welchen Zweck verfolgt die Hierarchie der Systeme in der Sta-ti-on? Nennen Sie Beispiele. Welche Aufgaben können auf Stationsniveau durchgeführt werden? Welche Aufgaben lassen sich von der Leitwarte aus durchführen? Wann ist ein Einsatz vor Ort (auf der Station) sinnvoll?

5.3. Aufbau der Informationssysteme

Die folgende Abbildung zeigt den Aufbau einer Informationskette von den Sensoren und Aktoren zur ersten und zweiten Ebene der Automatisierung.



Die erste Ebene wird hierbei als Feldebene beschrieben, die zweite Ebene aus Steuerungsebene. Im Einzelfall können Feldebene und Steuerungsebene ebenfalls hierarchisch aufgebaut sein.

Frage 5.3.1: (1) Welche Aufgaben hat die Feldebene? (2) Welche Aufgaben hat die Steuerungsebene? (3) Welche Unterschiede bestehen zu anderen Anwendungen der Automatisierung z.B. in der industriellen Produktion, für Schienenfahrzeuge oder Strassenfahrzeuge? (4) Was bedeuten die Begriffe Client und Server?

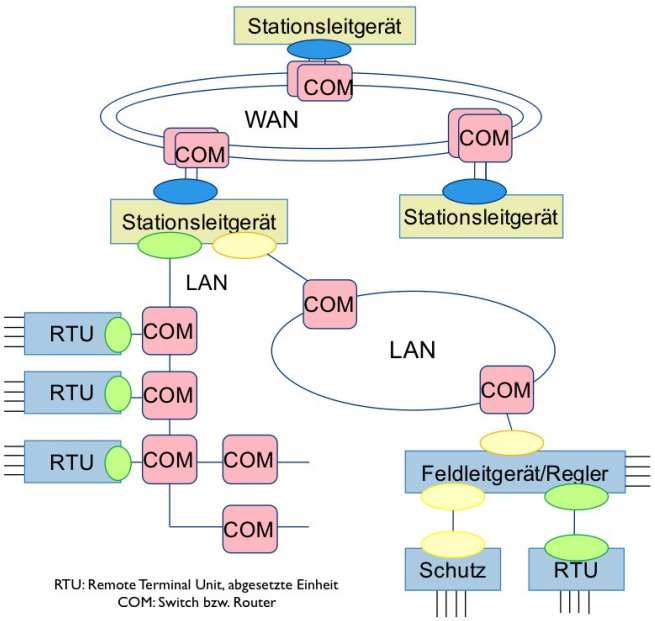
Lösung: (1) Feldebene: Messen, Regeln und Steuern mit Hilfe einer SPS (Speicherprogrammierbare Steuerung) bzw. eines IED (Intelligent Electronic Device = Feldleitgerät). Sensoren und Aktoren sind entweder über Klemmleisten angeschlossen (digitale oder analoge Eingänge und Ausgänge) bzw. über Feldbusse (z.B. IEC61850 mit Datenmodell zur Interoperabilität von Geräten).

(2) Steuerungsebene: Das Stationsleitgerät repräsentiert eine sogenannte SCADA (Supervisory Control and Data Acquisition). Diese Bezeichnung deutet darauf hin, dass hier mehrere Feldgeräte angeschlossen sind, die gesteuert werden und von denen Daten erhoben werden. Als Protokolle zu den Feldgeräten bzw. zur Leitwarte kommen Feldbusse wie IEC 61850 oder IEC 60870-5 in Frage.

(3) Unterschiede zu anderen Automatisierungsanwendungen: Grundsätzlich keine, jedoch sind in allen Anwendungsfällen anwendungsspezifische Feldbusse im Einsatz. Diese Feldbusse haben sich aus seriellen Feldbussen weiter zu netzwerkfähigen Feldbussen entwickelt.

(4) Client und Server: Bedeuten unterschiedliche Kommunikationsbeziehungen. Der Server wartet auf Anfragen der Clients (passiver Teil der Kommunikation). Der Client fragt eigenständig Server ab (aktiver Teil der Kommunikation). Beispiel: Ein Telefon stellt beide Funktionen zur Verfügung (Client = jemanden anrufen, Server = angerufen werden und ans Telefon gehen).

Frage 5.3.2: Folgende Abbildung zeigt die physikalische Anbindung der Geräte in der Station.



Hierbei wird unter dem Block „COM“ ein Ethernet-Switch bzw. ein Router verstanden. Erläutern Sie den Aufbau des Systems. Wie werden Prozessdaten (Messwerte, Steuerbefehle) kommuniziert?

Frage 5.3.3: Bus-Topologien. Welche Bus-Topologien erkennen Sie? Welche Schnittstellen müssen jeweils miteinander kompatibel sein?

Frage 5.3.4: Redundanz. Welche Anforderungen an die Verfügbarkeit bestehen für folgende Geräte: (1) Leistungsschalter, (2) Trennschalter, (4) Ölthermometer, (4) Spannungsregler (Regler für einen Laststufenschalter), (5) Schutzvorrichtung. Wo würden Sie diese Geräte anbinden?

5.4. Feldbusse

Viele der in der Stationsautomatisierung eingesetzten Feldbusse wurden und werden von der Arbeitsgruppe TC 57 (TC = Technical Committee) der IEC definiert. Hierzu gehören:

- IEC 60870-5: Fernwirkprotokoll (Telecontrol & Teleprotection)
- 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)
- IEC 61968: Schnittstellen zum Common Information Model (Application Integration at Electric Utilities – System Interfaces for Distribution Management)

Neben den Feldbussen der TC 57 sind in der Stationsautomatisierung auch andere Feldbusse im Einsatz, die sich in der industriellen Produktion bzw. in Fahrzeugen etabliert haben (z.B. Modbus, Profibus, DNP, CAN-Bus).

Frage 5.4.1: Welche Aufgaben hat ein Feldbus in der Stationsautomatisierung?

Frage 5.4.2: Architektur. Was versteht man unter einem Prozessbus? Was versteht man unter einem Stationsbus? Was versteht man unter horizontaler bzw. vertikaler Integration? Wie wird die technische Entwicklung weiter fortschreiten?

Lösung: (1) Prozessbus: Verbindung zum Prozess (Schalten, Messen, Schützen).

(2) Stationsbus: Kommunikation zwischen den Automatisierungssystemen.

(3) horizontale Integration: Zusammenfassen von Funktionen (aus dem Bereich Schutz, Steuerung und Überwachung) in weniger Systemen; vertikale Integration: Informationen werden durch die Hierarchieebenen durchgereicht und werden auf allen Ebenen verfügbar. Ziel ist die Vereinfachung der Systeme für Betrieb und Wartung.

(4) technische Entwicklung: zur Diskussion.

Frage 5.4.3: Netzwerk oder serieller Bus. Ältere, serielle Feldbusse werden zunehmend durch netzwerkfähige Feldbusse abgelöst. Erläutern Sie die technischen Unterschiede zwischen seriellen und netzwerkfähigen Feldbussen. Welche Vorteile und Nachteile haben beide Lösungen? Wie beurteilen Sie beide Lösungen bzgl. der Sicherheit (Security)?

Frage 5.4.4: Physical Layer. Welche Übertragungsmedien auf der physikalischen Schicht gibt es für Feldbusse in der Stationsautomatisierung? Erläutern Sie Vorteile und Nachteile.

Lösung: Kabel, Lichtwellenleiter, Funk.

Frage 5.4.5: Interoperabilität. Was muss spezifiziert werden, damit Geräte unterschiedlicher Hersteller über einen Feldbus miteinander kommunizieren können?

Lösung: Erforderlich ist eine Beschreibung der Schnittstelle, d.h. alle Protokollschichten bis zur Anwendungsebene, Nachrichtenformate inkl. Datentypen und Bedeutung der Nachrichten.

Frage 5.4.6: Prozessbild. Das Stationsleitgerät bzw. die Leitwarte erzeugt aus den Meldungen von der Station ein sogenanntes Prozessbild. Welche Informationen werden hierfür typischerweise benötigt?

Lösung: Zustände wie z.B. Schalterstellungen (ein, aus) oder Betriebszustände (lokaler Betrieb, ferngesteuert, blockiert, simuliert) der Leistungsschalter und Trennschalter, Position der Stufenschalter, Messwerte (Strom, Spannung, Frequenz, Wirkleistung, Blindleistung), Meldungen der Systeme (Schutzanregung, Schutzauslösung, Ereignisse, Fehler).

5.5. IEC 60870-5

Der Feldbus nach dem Standard IEC 60870 wird als Stationsbus in Schaltanlagen eingesetzt und besitzt folgende Eigenschaften:

- Fernwirkprotokoll (Telecontrol Equipment and Systems)
- Lange etabliert als serieller Bus zur Kommunikation zwischen Steuergeräten in Schaltanlagen und der Leittechnik.
- Reines Feldbus-Protokoll (signalorientiert, ohne Datenmodell, ursprünglich serieller Bus)
- IEC60870-5-104: netzwerkbasierte Version (Ethernet, TCP/IP)
- Weitere relevante Spezifikationen:
  - IEC60870-5-101: Rahmenspezifikation für den seriellen Bus
  - IEC60870-5-102: Erweiterung für die Übertragung von Zählerständen
  - IEC60870-5-103: Erweiterungen für Schutzgeräte

  Der Feldbus nach der Norm IEC 60870 wurde ab 1988 spezifiziert und ist seither im Einsatz.

Frage 5.5.1: Was versteht man unter einem Fernwirkprotokoll? Wo werden solche Protokolle typischerweise eingesetzt?

Lösung: Mit Fernwirken wird eine größere Entfernung angesprochen. Anwendungsfälle sind die Kommunikation zwischen Station und Leitwarte und zwischen Stationen (Stationsbus). Auch Verbindungen zu Endkunden (Nachtspeicherheizungen, Straßenlaternen, Erzeuger und Verbraucher) wären unter dem Begriff Fernwirken zu finden.

Frage 5.5.2: Welche Informationen transportiert ein Stationsbus? Welche Einrichtungen sind typischerweise angeschlossen? Worauf ist hierbei speziell zu achten?

Lösung: (1) Zustandsinformationen und Steuerbefehle. (2) Schaltanlagen, Fernwirktechnik, Netzleittechnik in Umspannwerken und Leitwarte im Stromnetz, sowie auch im Gasnetz und Wassernetz. (3) Sicherheit, da hier eine versorgungskritische Infrastruktur gesteuert wird.

Frage 5.5.3: Was versteht man unter einer signalorientierten Schnittstelle?

Lösung: Es werden Nachrichtenformate definiert zum Transport von Meldungen bzw. für Steuerinformation, sowie zur Verwaltung der Schnittstelle (Quittungen, Fehlerindikationen, Prüfsummen zur Fehlersicherung). Außerdem Adressen, wenn mehrere Geräte den Feldbus teilen.

Frage 5.5.4: Auf welcher Protokollschicht findet sich typischerweise ein serieller Bus? Welcher Unterschied besteht zu einem netzwerkbasierten Bus? Welchen Zweck verfolgt die netzwerkfähige Version des IEC 60870?

Lösung: (1) Protokollschicht: Schicht 2. Hier genügt ein Rahmenprotokoll zur Übertragung der Nachrichten. Die Verbindung ist eine Punkt-zu-Punkt Verbindung, geht also von einem zum anderen Ende der Leitung. Wird ein gemeinsames Übertragungsmedium genutzt, ist auch die Adressierung unterschiedlicher Geräte möglich (Schicht 3). Jedoch ist der Aktionsradius auf die Verbreitung des gemeinsamen Mediums beschränkt. (2) Netzwerkbasierte Schnittstelle: Schicht 3. Entweder über Ethernet (MAC-Adressierung) oder mit Hilfe von IP-Adressen können Geräte im gemeinsamen Adressraum (= Netz) erreicht werden. (3) Netzweite Erreichbarkeit.

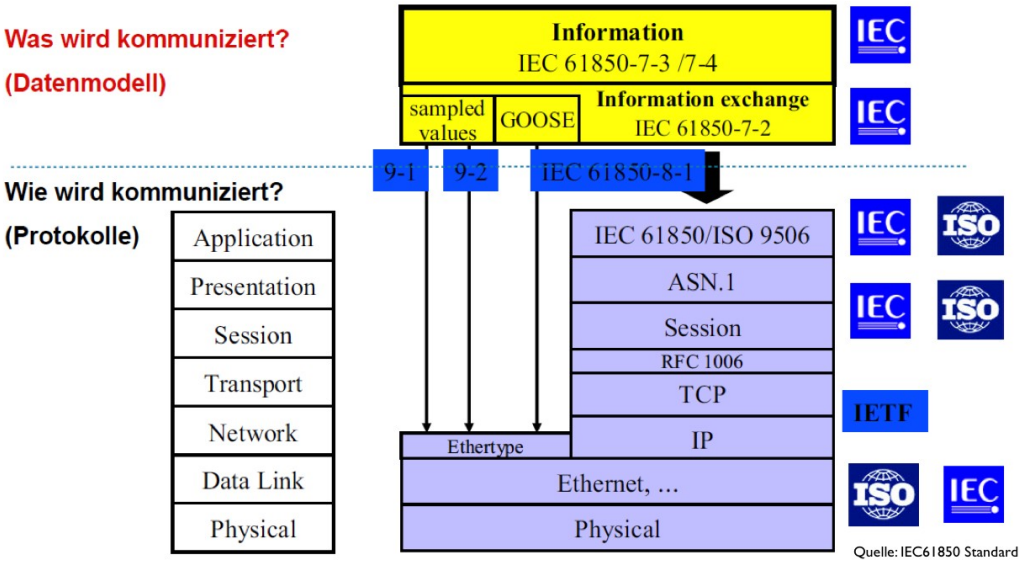
5.6. IEC 61850

Der Feldbus nach dem standard IEC 61850 wird als Prozessbus und als Stationsbus eingesetzt. Im Unterschied zu anderen Feldbussen definiert die Norm nicht nur die Kommunikationsprotokolle, sondern auch die Bedeutung der kommunizierten Nachrichten mit Hilfe eines Datenmodells:

- Protokolle: Wie wird kommuniziert? (Nachrichtenformate, Meldungen, Adressen, Schichten)
- Datenmodelle: Was wird kommuniziert? (Kennzeichnungssystem für Informationen)

Übersicht

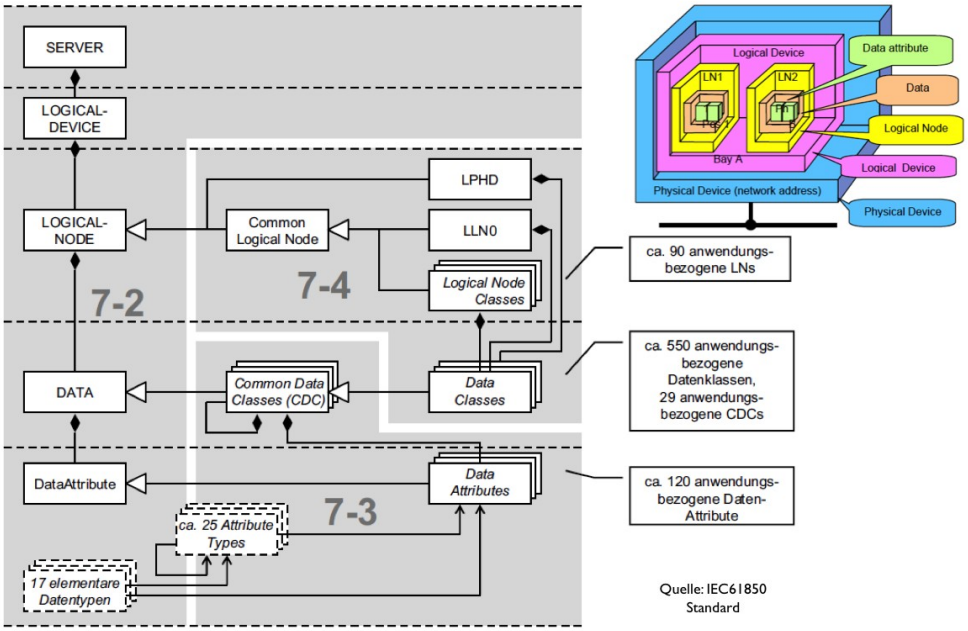
Folgende Abbildung zeigt eine Übersicht.



Der untere Teil der Abbildung zeigt hierbei die verwendeten Protokolle. Der Standard verwendet hierzu unmittelbar auf Ethernet basierende Schnittstellen für schnelle, lokale Anwendungen (wie z.B.-Schutzgeräte oder Messreihen), sowie ein auf TCP/IP basiertes Protokoll für netzweite Anwendungen.

Auch bei Verwendung eines standardisierten Protokolls sind Anwendungen verschiedener Hersteller noch lange nicht miteinander kompatibel: Kommuniziert ein Feldgerät z.B. eines Messwert, so ist dieser im empfangenden Gerät als solcher überhaupt nicht festgelegt, weder im Datentyp (Integer, Floating-Point), noch in der Bedeutung (z.B. Spannung des Transformators T1 auf der Oberspannungsseite, Phase 1).

Aus diesem Grund geht die Norm IEC 61850 weiter und definiert Datenmodelle für die Sekundärtechnik nach dem in folgender Abbildung gezeigten Schema.



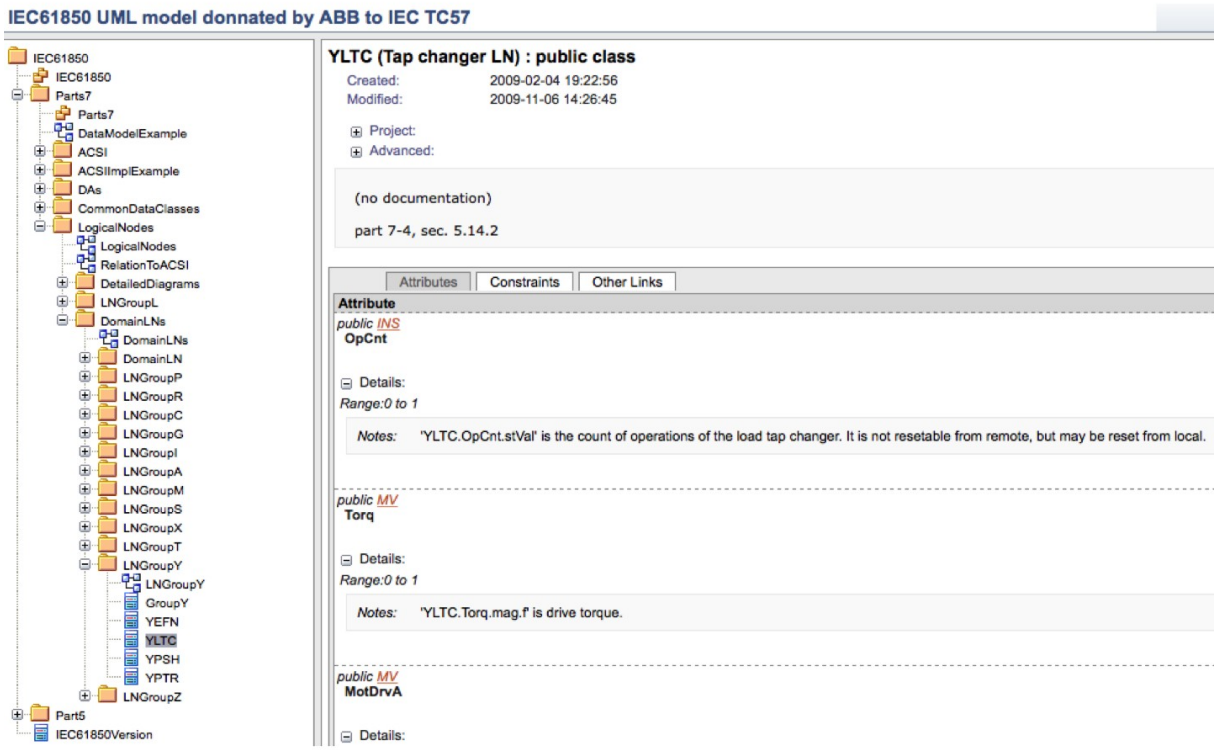
Hierbei entsteht ein Abbild der physikalischen Welt in die Welt der Daten im Sinne von Klassen und Objekten (als Klasseninstanzen) nach einem objektorientierten Schema. Die in der Abbildung

oben bezeichneten Teile 7-2, 7-3 und 7-4 sind Abschnitte des Teils 7 der Norm mit Titel Basic Communication Structure, der die Datenmodelle beinhaltet (siehe auch Teil 2 dieser Vorlesung, Abschnitt 2.3 Anwendungsprotokolle).

Aufbau der Norm

Frage 5.6.1: Recherchieren Sie nach dem Standard IEC 61850, speziell nach dem Aufbau gemäß der oben gezeigten Abbildung. Hinweis: Im Literaturverzeichnis unter [3] findet sich eine URL, die es ermöglicht, den Aufbau der Norm IEC 61850 mit Hilfe eines Browsers zu erkunden. Ergründen Sie den Aufbau des Standards. Wo finden sich Abbilder der physikalischen Systeme? Welche Vereinbarungen hierüber gibt es?

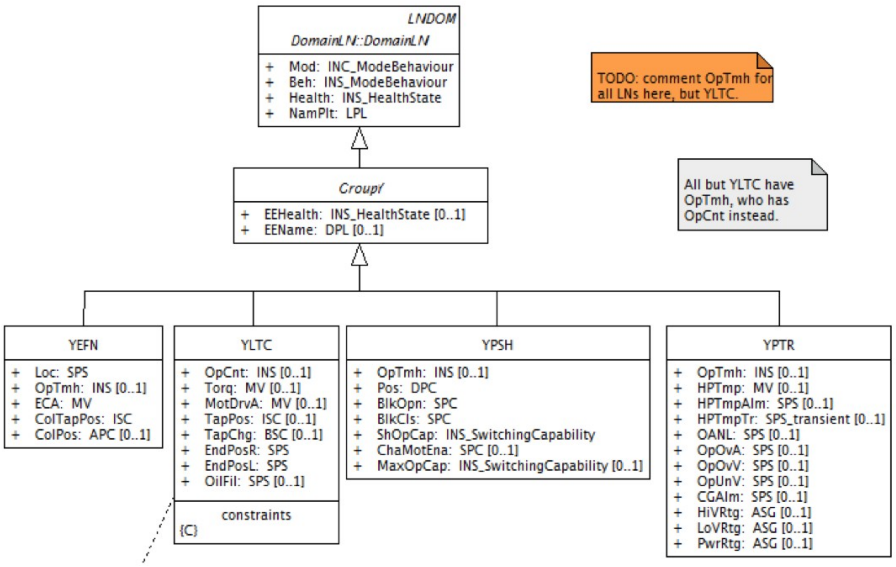
Lösungsbeispiel (siehe URL unter [3]):



Siehe Teil 7 mit den Vereinbarungen zu den Datenmodellen. Bei den logischen Knoten finden sich Abbilder der physikalischen Systeme (z.B. Laststufenschalter, siehe Abbildung). Außerdem Daten-klassen und Attribute nach dem in in der zweiten Abbildung in Abschnitt 5.6 dargestellten Schema.

Das UML Modell umfasst die Teile 5 und 7 der Spezifikation. Teil 5 mit Titel Communication Requirements beinhaltet die Beschreibung der Anwendungsdomäne, untergliedert nach Schutzgeräten (Protection Equipment), Steuerungsgeräten (Control Equipment), Messinstrumenten (Metering Equipment), Primärtechnik (Primary Equipment), und sonstigen Geräten. Die Klassendiagramme jeder Domäne finden sich unter der ersten Kategorie Detailed Domains. Für jede Domäne gibt es oben ein Klassendiagramm zur Übersicht.

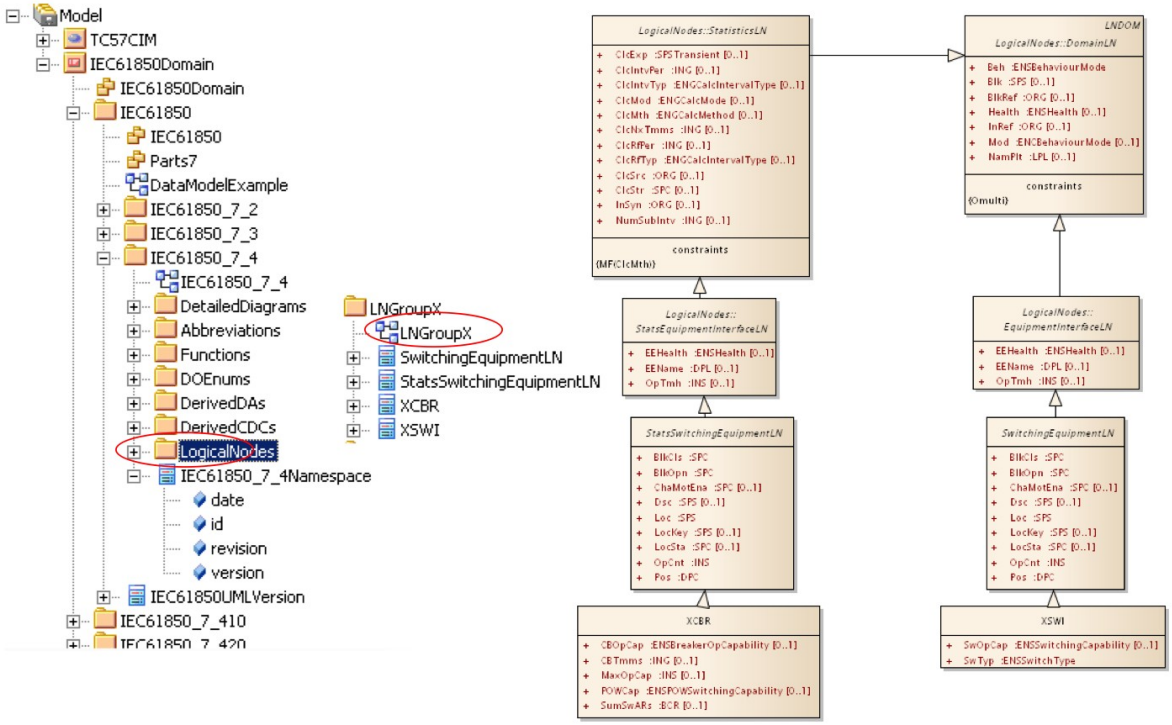
Teil 7 mit Titel Basic Communication Structure ist ähnlich aufgebaut. Auch hier finden sich zunächst Übersichtsdiagramme, dann Details zu den einzelnen Kategorien. Von speziellem Interesse sind hier das Meta-Modell, sowie die logischen Knoten (Logical Nodes) der Anwendungsgruppen P bis Z.



Die in der Gruppe Y befindlichen logischen Knoten sind dem Transformator zugeordnet.

Frage 5.6.2: Spezifikation als UML-Datei. Der Standard ist auch als UML-Datei verfügbar (der Bequemlichkeit halber findet sich eine Kopie hier). Untersuchen Sie den Standard mit Hilfe eines UML-Werkzeugs bzw. eines UML-Editors.

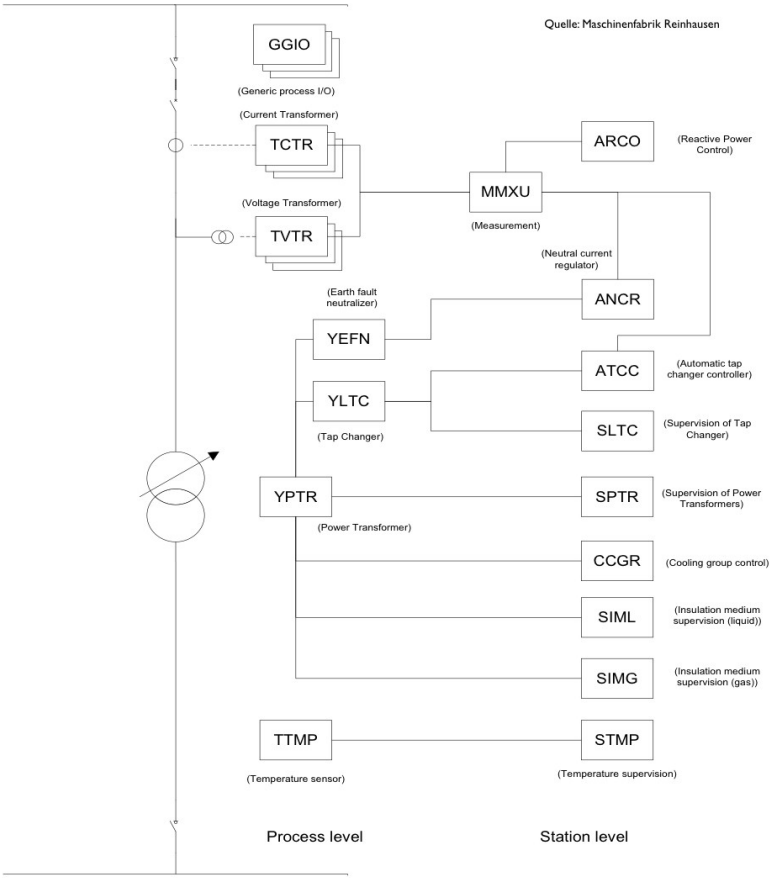
Lösungsbeispiel:



In der oben gezeigten Abbildung wurde Enterprise Architect verwendet (verfügbar mit einer kommerziellen Lizenz). Das Format ist jedoch auch mit Open-Source Werkzeugen lesbar bzw. konvertierbar (z.B. Violet UML). Hinweis: Die Modellstruktur findet sich Menüpunkt „View“ unter „Package Browser“.

Anwendungen

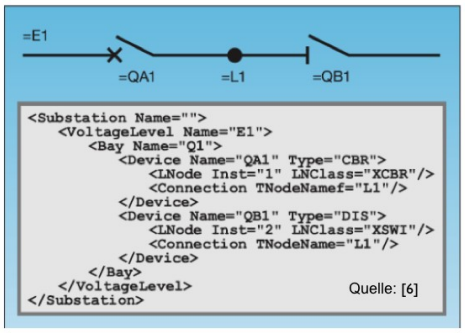
Frage 5.6.3: Anwendungsbeispiel. In der elektrischen Energieversorgung sind einphasige Ersatzschaltbilder der Anlagen gebräuchlich. Diese Beschreibung der Anwendungs-Domäne lässt sich unmittelbar in den Standard IEC 61850 übernehmen. Folgende Abbildung zeigt ein Beispiel hierfür.

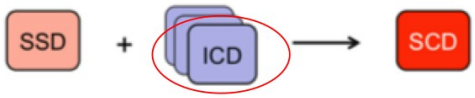


Links im Bild ist das Ersatzschaltbild bestehend aus Leistungsschalter, Trennschaltern, Stromwandler, Spannungswandler, sowie regelbarem Transformator zu sehen. Rechts daneben sind die Elemente und die Komponenten der Sekundärtechnik in der Terminologie nach IEC 61850 dargestellt. Identifizieren Sie die genannten Komponenten der Anwendungs-Domäne. Welche Funktion haben die Komponenten? Welche Daten werden übertragen?

Lösung: siehe UML-Browser bzw. UML-Editor.

Frage 5.6.4: Folgende Abbildung zeigt eine sogenannte ICD-Datei.





Dateien der System Configuration Language (SCL):

- ICD: IED Capability Description
- SSD: System Specification Dscription
- SCD: Substation Configuration Description

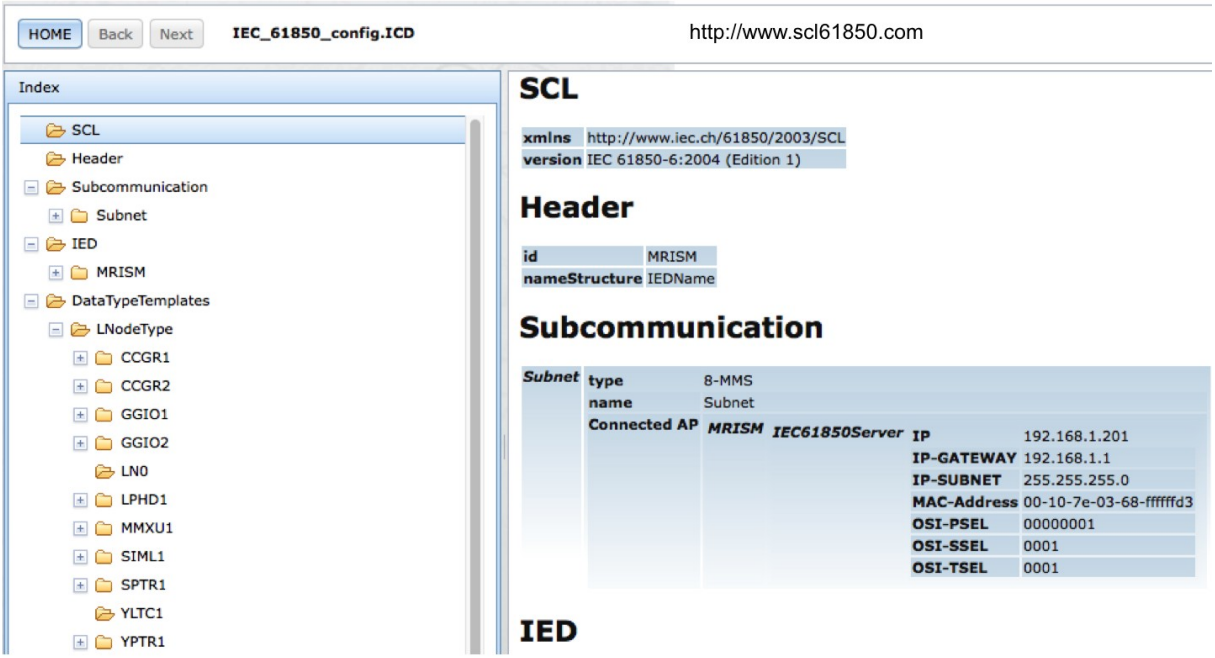
Welche Informationen enthält die ICD-Datei eines Gerätes? Wozu wird sie verwendet? Wie genau funktioniert der Austausch von Informationen zwischen zwei Geräten und welche Rolle spielt hier bei die ICD-Datei? Analysieren Sie die Informationen im gezeigten Beispiel.

Lösung: Die ICD-Datei enthält die Systemkonfiguration eines Gerätes (IED: Intelligent Electronic Device). Werden Daten ausgetauscht, lassen sich hiermit auch die Daten klassifizieren. Somit weiss ein mit dem IED verbundenes Gerät, welche Informationen kommuniziert werden. Bei einem Schalter wäre dies z.B. der Schaltzustand.

Frage 5.6.5: Eine gegebene ICD-Datei beschreibt ein Gerät, das als Server arbeitet, also z.B. Messwerte zur Verfügung stellt. Welche funktionen hat ein zugehöriger Client? Wie lässt sich aus dem gegebenen ICD-Datei ein passender Client realisieren?

Frage 5.6.6: Analysieren Sie die Struktur einer gegebenen IDC-Datei mit Hilfe des Browser-basierten Werkzeugs SCL-Explorer (http://www.scl61850.com).

Lösungsbeispiel:



6. Datenorganisation

6.1. Datenaustausch zwischen Verwaltungssystemen und Betreibern

Während der IEC61850 Standard Protokolle und Datenmodelle für die Sekundärtechnik beschreibt, geht der Standard IEC 61970 Common Information Model (CIM) weiter und beschreibt ein Datenmodell für die Primärtechnik. Beide Standards lassen sich wie folgt abgrenzen:

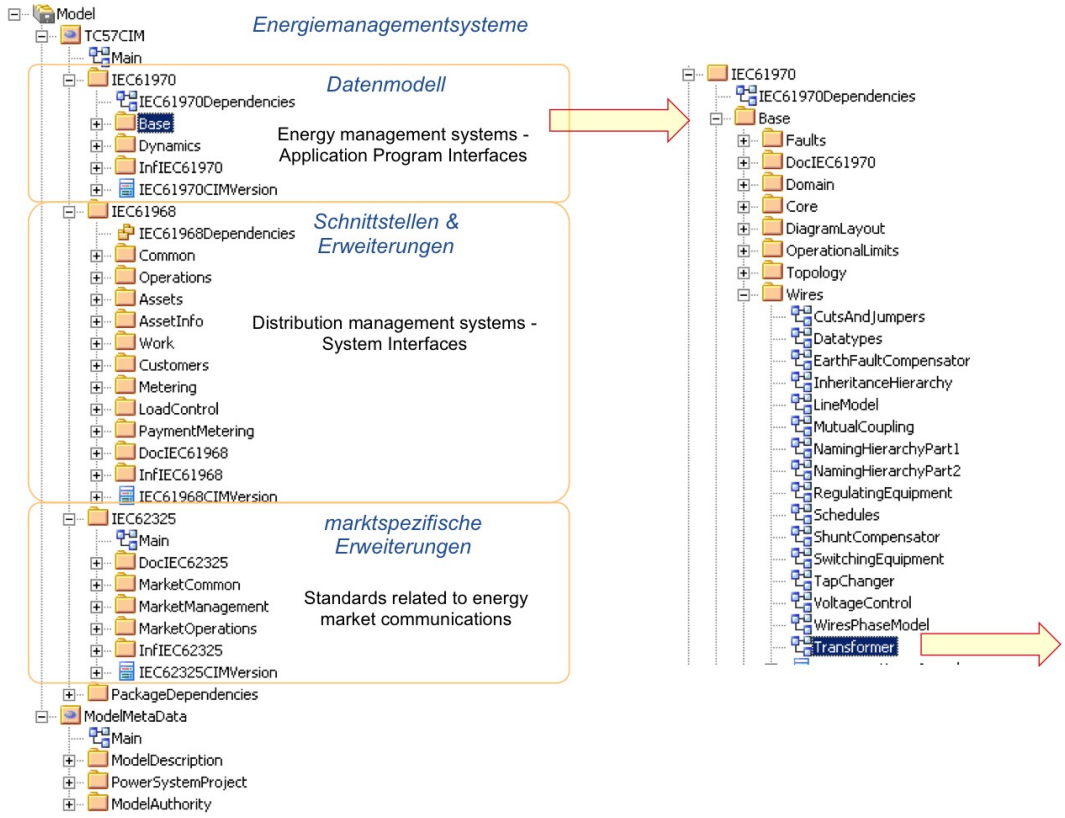
- IEC61850
  - Einheitliche Darstellung der Sekundärtechnik (Schutz, Regler, Überwachung)
  - Schwerpunkt: Schaltanlagen (Feldebene)
  - Datenmodell als Dokument verfügbar (IEC Standard)
- IEC61970 Common Information Model (CIM)
  - Einheitliche Darstellung der Primärtechnik (IEC 61970-301 definiert CIM)
  - Schwerpunkt: Leittechnik (Betrieb) und Wartung der Betriebsmittel
  - Datenmodell direkt im UML-Format verfügbar (IEC Standard)

Anwendungsbeispiele für das Common Information Model sind somit der Betrieb und die Überwachung der Betriebsmittel mit all ihren Schnittstellen zu den Verwaltungssystemen der Betreiber.

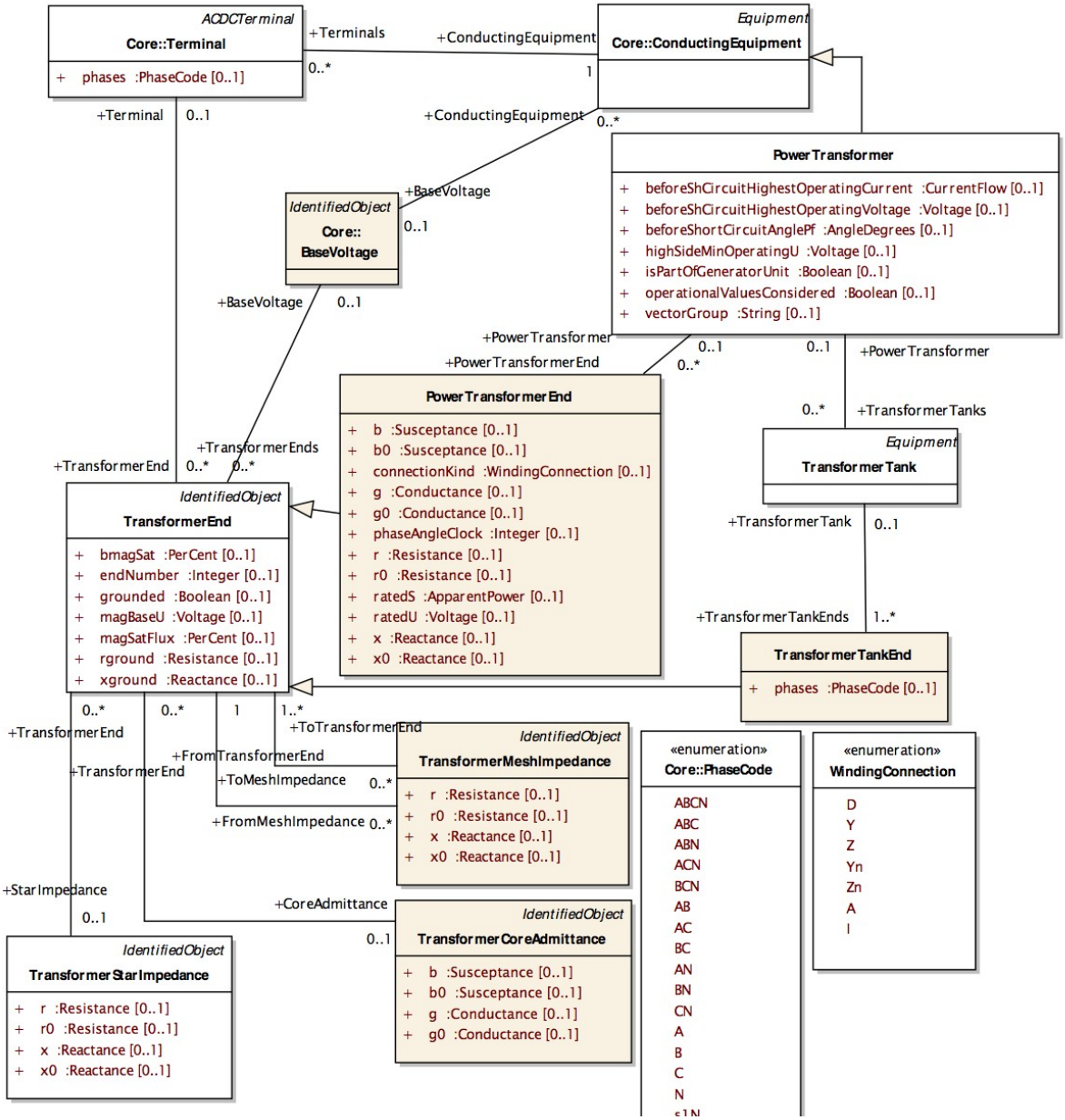
Inhalte des Standards

Frage 6.1.1: Der CIM-Standard liegt als UML-Datei vor (siehe [6]). Erkunden Sie die Inhalte.

Lösungsbeispiel:



Folgt man dem ausgewählte Pfad, so findet sich ein Domänen-Modell eines Transformators, das alle Betriebsmittel enthält, die der Wartung und Pflege bedürfen, darunter auch der Öltank.



Hinweis: Die Modellstruktur findet sich Menüpunkt „View“ unter „Package Browser“.

Frage 6.1.2: Wie grenzen sich folgende Bestandteile des CIM ab: (1) IEC 61970, (2) IEC 61968, (3) IEC 62325? Wie grenzt sich CIM zum IEC61850 ab?

Lösung: Alle Standards sind Ergebnisse der IEC Arbeitsgruppe TC 57. Schwerpunkte: (1) IEC 61970: Datenmodelle (= Kennzeichnungssystem) der primären Betriebsmittel; (2) IEC 61968: Schnittstellen zu Verwaltungssystemen, Erweiterungen des Datenmodells; (3) IEC 622325: marktspezifische Erweiterungen des Datenmodells (Stromhandel, Regelenergie).

Frage 6.1.3: Lassen sich die Datenmodelle des IEC 61850 in die des CIM einbinden?

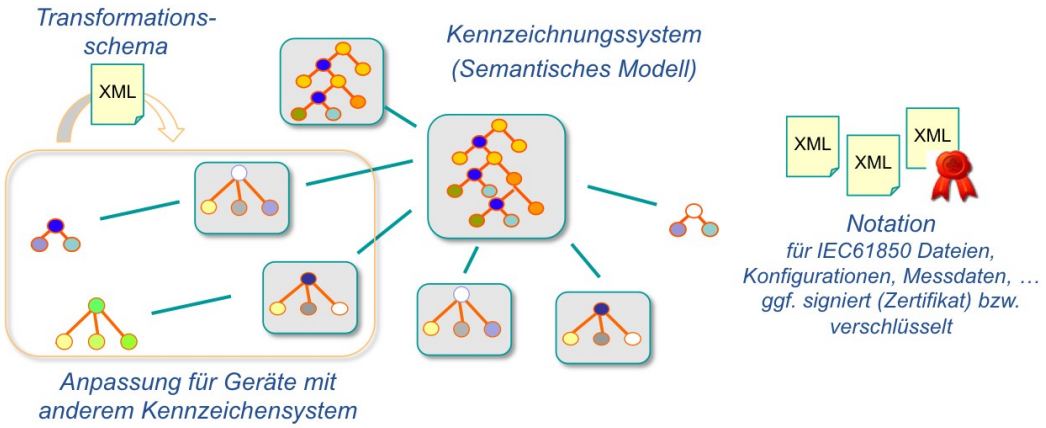
Lösung: Ja, die Modelle ergänzen sich. IEC 61850 beschreibt das Prozessabbild der Sekundärtechnik aus Sicht des operativen Betriebs (ohne Wartung, Erneuerung, Instandsetzung, Ausbau etc).

Frage 6.1.4: Wieso ist ein Datenmodell als Kennzeichnungssystem von Bedeutung? Wozu lässt es sich konkret verwenden?

Lösung: (1) Intern: Jede Software benötigt ein Domänenmodell zur Abbildung Ihrer Aussenwelt. Als Beispiele sind die Definition von Variablen bzw. Klassen zu nennen, die instanziert bzw. in einer Datenbank verwaltet werden. (2) Schnittstellen: Damit Systeme Informationen untereinander austauschen können, sind die Nachrichten und Datentypen zu definieren. (3) Ein generelles Datenmodell hierfür bietet eine Orientierung für die Anwendungsprogrammierer bzw. Hersteller der Geräte. (4) Liegt das Datenmodell in einer standardisierten Form und Notation vor, lässt sich die Entwicklung von Anwendungen und die Konfiguration von Anlagen hiermit automatisieren.

6.2. Verwendung von Datenmodellen

Das wissen um eine Domäne beschreibt der Anwendungsentwickler in Form von Klassen bzw. Klassendiagrammen. Diese lassen sich für die Software-Entwicklung und für die Gestaltung der Datenbank verwenden. Es entsteht ein Modell der Anwendungsdomäne: ein Datenmodell.



Wenn ein Datenmodell generisch angelegt ist, d.h. als allgemeine Beschreibung einer Anwendungsdomäne, lässt es sich als Kennzeichnungssystem bzw. als semantisches Modell verwen-den. Es stellt einen Bezugspunkt dar für die individuellen Datenmodelle der Systeme, bzw. kann direkt in diese Datenmodelle übernommen werden. Die Abbildung oben beschreibt eine Anordnung von Geräten, die sich auf ein gemeinsames Kennzeichnungssystem beziehen.

Frage 6.2.1: Nehmen Sie als Beispiel die Datenmodelle des IEC 61850 für das Gerät in der Mitte, das mit einem der anderen Geräte kommuniziert. Wie funktioniert die Kommunikation für IEC 61850 Geräte untereinander? Was genau ist als Datenmodell spezifiziert?

Lösung: siehe Abschnitt 5 und praktische Übungen in Teil 2.3.

Frage 6.2.2: Ein Gerät verwendet ein anderes Datenmodell als IEC 61850. Die Kommunikationsschnittstelle wird über einen Bus-Adapter an ein gemeinsames Protokoll angepasst. Die Geräte können also Nachrichten austauschen, jedoch ist die Bedeutung der Nachrichten nicht formal spezifiziert. Wie können sich die Geräte miteinander verständigen?

Lösung: Mit Hilfe eines Übersetzers (wie bei unterschiedlichen Sprachen im praktischen Leben auch). Hierbei werden Nachrichten in der Sprache des proprietären Datenmodells des Gerätes in die Sprache des generischen Datenmodells transformiert, und umgekehrt (d.h. man benötigt einen Übersetzer, der die proprietäre und generische Sprache spricht). IEC 61850 spielt hierbei die Rolle einer universellen Verkehrssprache (d.h. Englisch für die Stationsautomatisierung).

Frage 6.2.3: N Geräte mit proprietären Schnittstellen. Wenn jedes Gerät eine proprietäre Schnittstelle mit proprietärem Datenmodell besitzt, wie viele Adapter und Übersetzer sind für N Geräte erforderlich? Wenn zu N existierenden Geräten das N+1 Gerät dazukommt, wie viele Schnitt-stellen müssen dann angepasst werden. Wie ändern sich diese Verhältnisse, wenn zwar alle Geräte

proprietäre Datenmodell besitzen, jedoch ein generelles Datenmodell als Kennzeich-nungs-schema existiert?

Lösung: (1) Ohne generelles Datenmodell als Bezugspunkt: Jede Sprache muss in jede andere Sprache übersetzt werden. Für N Geräte gibt es N*(N-1)/2 Kommunikationsbeziehungen (= Kanten eines Graphen mit N Kanten bzw. Kanten und Diagonalen ei-nes N-Ecks). Der Aufwand steigt somit quadratisch mit der Anzahl der Geräte. Für das N+1 Gerät müssen N Schnittstellen angepasst werden.

(2) Mit generellem Datenmodell als Bezugspunkt: Jede der N Sprachen lässt sich in das Bezugssystem übersetzen, und von dort aus in eine andere Sprache. Für N Geräte sind somit N Schnittstellen und Übersetzer erforderlich, der Aufwand steigt linear. Für das N+1 Gerät muss eine Schnittstelle angepasst werden (nämlich die des Gerätes an das Bezugssystem).

Frage 6.2.4: Umfang der Datenmodelle. Welchen Umfang können die Datenmodelle haben, was lässt sich alles dort beschreiben?

Lösung: siehe IEC 61850 in Abschnitt 5. Der Umfang umfasst die ausgetauschten Nachrichten (z.B. Wert der Spannung auf der Oberspannungsseite von Trafo 2, Phase 3), die Konfiguration (SCL Dateien), die in CIM gegebenen Modelle, ggf. auch Transformationsschemata, sowie Meta-Informationen (z.B. Verzeichnisdienste mit Informationen, wo sich welche Information findet).

Frage 6.2.5: Notation. Welche Notation ist für Datenbankmodelle, Konfigurationen etc gängig? Welche Gründe sprechen hierfür?

Lösung: XML besitzt eine große Verbreitung. Ein Vorteil ist die Kodierung als Text.

Frage 6.2.6: Sicherheit. Wie lässt sich die Kommunikation zwischen zwei Geräten absichern? Wie lassen sich Datenmodelle und Konfigurationsdateien absichern?

Lösung: Mit Hilfe der Verschlüsslung und durch Signaturen, siehe Abschnitt 4.

Software und Systeme

Bei der Entwicklung von Software und Systemen lassen sich folgende Ebenen unterscheiden:

- Informationsebene: abstrakte bzw. semantische Modelle
  - Informationsmodell, z.B. in UML als Klassendiagramm beschrieben
  - Anwendungsprofil: z.B. im RDF-Format oder XML-Format zu verarbeiten
- Logische Ebene: implementierbare Modelle
  - Nachrichtenebene: Datenmodell, z.B. als ICD-Datei oder XML-Nachrichtendatei
  - Datenbankschema, z.B. relational in SQL oder objektorientiert implementierbar
- Systemebene: Verwendung spezieller Produkte, die die verwendeten Standards unterstützen, z.B. SPS, SCADA-Systeme mit Entwicklungsumgebung, Datenbanken, Entwicklungswerkzeuge.

Hierbei werden Datenmodelle entweder als Kennzeichnungssystem, zur Konfiguration oder als Meta-Information verwendet (Informationsebene), oder als Klassen oder Datenbank implementiert (logische Ebene). Diese Methoden sind unabhängig von den jeweils verwendeten Systemen oder Werkzeugen zur Entwicklung.

Frage 6.2.7: Nennen Sie Beispiele für die Anwendung semantischer Modelle bzw. für Kennzeichnungssysteme. Untersuchen Sie hierzu Standards wie z.B. CAN in Automation, Energie-management nach CiA 454, bzw. IEC 618560-7-420 für verteilte Energieerzeuger.

Lösung:

(1) Beispiele: ISBN-Nummern, Anlagenkennzeichnungssysteme nach DIN 6779 oder EN 61355, Gerätemodelle (z.B Fahrstuhl, Müllfahrzeug) von CANopen (siehe http://www.can-cia.org). Im einfachsten Fall werden nur Kennzei-chen (universal unique identifier) nach einem Nummernschema vergeben. Im medizinischen Bereich sind sind semantische Modelle (Ontolo-gien) im Aufbau, siehe z.B. zur Unterstützung der Diagnose von Krankheiten (http://disease-ontology.org).

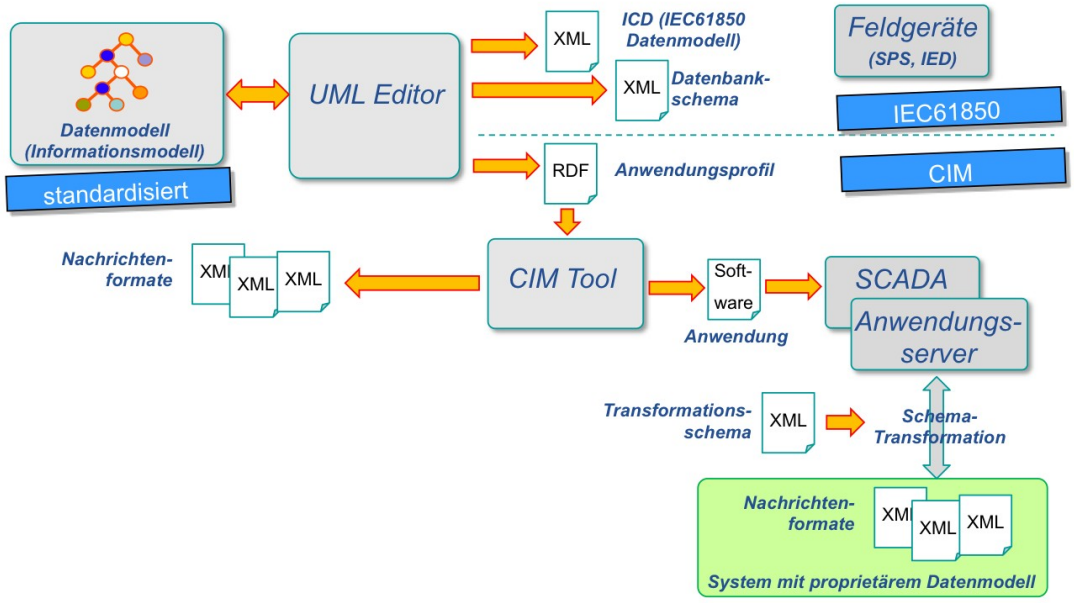
(2) Beide oben genannten Standards (CiA 454, bzw. IEC 618560-7-420) verfügen über Kennzeichnungssysteme für Systemkomponenten. Mit CIM und IEC 61850 ist die elektrische Energieversorgung im Vergleich zu anderen Disziplinen recht gut aufgestellt.

Frage 6.2.8: Welche Relevanz haben Kennzeichnungssysteme für Schlagworte wie Industrie 4.0 bzw. das Internet der Dinge? Wie schätzen Sie die weitere Entwicklung ein?

Lösung: zur Diskussion.

Werkzeuge und Methoden

Man kann das Domänenmodell bzw. Datenmodell in das Zentrum der Anwendungen stellen, wie in folgender Abbildung gezeigt. Nach dieser Sichtweise werden Anwendungen ausgehend von hier um die Daten herum entwickelt.



Hierzu werden gängige Methoden und Standards eingesetzt:

- UML: zur Definition von Datenmodellen und Software
- CIM: Common Information Model (für primäre Betriebsmittel)
- IEC 61850: Datenmodelle für die Stationsautomatisierung.

Frage 6.2.9: Vergleich mit funktionaler Sichtweise. Bei der traditionellen Sichtweise steht die Funktionalität im Vordergrund: Ein Gerät soll eine Funktion bereit stellen (z.B. einen Schalter stellen) und benötigt hierfür Informationen, die mit einem anderen System über eine Schnittstelle ausgetauscht werden müssen. Vergleichen Sie diese Sichtweise mit der oben dargestellten datenzentrischen Sicht? Welche Konsequenzen ergeben sich hieraus für die Entwicklung der Anwendungssoftware?

Frage 6.2.10: Beschreiben Sie die in der Abbildung gezeigten Entwicklungsschritte. Welche Werk-zeuge werden eingesetzt? Was ist jeweils das Ergebnis?

7. Seminararbeit

Die Seminararbeit dient der praktischen Vertiefung der in dieser Veranstaltung gewonnenen Erkenntnisse. Für den praktischen Teil werden Einplatinencomputer (Raspberry PIs) zur Verfügung gestellt, die mit Open Source Software zur Stationsautomatisierung ausgerüstet sind. Zur Ausstattung gehört speziell das Anwendungsprotokoll IEC61850.

Eine Anleitung zur Seminararbeit findet sich in Teil 2.3 dieser Veranstaltung. Dort werden die wichtigsten Eigenschaften der Protokolle zur Stationsautomatisierung zusammengefasst. Der letzte Abschnitt der Unterlagen unter der Überschrift „Anwendungsbeispiel: IEC61850 Server Implementierung“ enthält Anleitungen und die Aufgabenstellung zur Seminararbeit.

Die Seminararbeit ist in Heimarbeit zu leisten, idealerweise zwischen den beiden Vorlesungsblöcken Teil 1 und Teil 2 dieser Veranstaltung. Die Ergebnisse sind in Form eines Laborberichts zusammenzufassen und abzugeben. Je nach Vereinbarung mit dem Dozenten kann die Seminararbeit entweder als Testat oder als Teilnote bewertet werden.

7.1. Pflichtteil – IEC61850 Server Implementierung

Die Aufgaben zum Pflichtteil der Arbeit finden sich in Teil 2.3 der Vorlesungsunterlagen (siehe http://wwwlehre.dhbw-stuttgart.de/~srupp/DHBW_M/ENT/TM20602_2_3_Anwendungsprotokolle.pdf). Im letzten Kapitel „Anwendungsbeispiel“ ab Seite 35 findet sich eine Anleitung und die Aufgabenstellung. Server und Client kommunizieren über das IEC61850 MMS Protokoll. Für Server und Client existieren Anwendungsbeispiele, die Clients sind standardkonform formal mit Hilfe von ICD-Dateien beschrieben. Zum MMS Protokoll werden auf dem System Traces erstellt, die sich auf dem PC näher dekodieren und analysieren lassen.

Frage 7.1.1: Machen Sie sich mit dem System vertraut. Binden das System in Ihr lokales Netzwerk ein. Stellen Sie eine Verbindung mit dem System über ein Terminalfenster bzw. über einen Remote-Desktop her (Anleitung siehe S. 42). Analysieren Sie die Verzeichnisse auf dem System.

Frage 7.1.2: Aktivieren Sie den Protokollanalysator (Wireshark) auf dem System (Anleitung ab S. 42). Erstellen Sie Traces. Kopieren Sie die Traces auf Ihren PC und analysieren Sie diese dort mit Hilfe Ihre lokalen Installation des Protokoll-Analysators.

Frage 7.1.3: Beispiele für IEC 61850 Client – Server testen. Aktivieren Sie eine der auf dem System vorhandenen Beispiel-Anwendungen. Hierbei stellt das System den Server dar. Der Client wird ebenfalls auf dem System gestartet und kommuniziert lokal mit dem Server (über die IP-Adresse 127.0.0.1 localhost). Anleitung hierzu: ab S. 43.

Frage 7.1.4: ICD Struktur. Untersuchen Sie die Struktur der ICD-Datei zu dem von Ihnen gewählten Beispiel. Verwenden Sie hierzu die Online-Analyse von IPCom (siehe S. 44 ff), bzw. IEDScout oder einen geeigneten XML-Editor.

Frage 7.1.5: MMS Analyse. Analysieren Sie für die von Ihnen gewählte Beispiel-Anwendung die Kommunikation zwischen Client und Server über das MMS Protokoll. Gehen Sie hierzu vor, wie ab S. 46 beschrieben.

Frage 7.1.6: Dokumentieren Sie Ihre Ergebnisse in Form eines Laborberichts. Verwenden Sie hierzu Bildschirmkopien (screen dumps) Ihrer Analysewerkzeuge, wie in den Folien zu Teil 2.3.

7.2. Freie Aufgabe – Smart Grid

Als freies Thema stellen Sie sich bitte selbst eine weitergehende Aufgabe über den Pflichtteil hinaus. Als Themen kommen in Frage:

- Erweiterungen des Servers aus Ihrem Beispiel aus dem Pflichtteil. Die Erweiterungen werden mit Hilfe des Clients getestet und die Funktion dem Protokoll-Analysator untersucht. Es wird eine ICD Datei erzeugt und untersucht.

- Weiterentwicklung des Test-Szenarios. Untersuchungen der Konformität der Kommunikation und des ICD-Formates mit Bezug auf den Standard.
- Weiterentwicklung der Server. Bauen Sie die Server so aus, dass über Schnittstellen wirkliche Messwerte aufgenommen und kommuniziert werden können (z.B. Temperaturen, Zähler-stände, Ereignisse, Ströme, Spannungen).
- Datenmodelle. Zu IEC 61650 und CIM existieren Spezifikationen unmittelbar im UML-Format (als Klassendiagramme, siehe Literaturverzeichnis). Diese lassen sich mit einem UML-Werkzeug analysieren und mit den Datenmodellen im System vergleichen.
- Lokales Netz. Erweitern Sie Ihren Aufbau um Server und Clients im lokalen Netz, indem Sie den Client z.B. auf Ihrem PC realisieren, bzw. indem Sie weitere Systeme dazu nehmen. Führen Sie Untersuchungen im Netz durch.
- Weitverkehrsnetz mit anderen Teilnehmern. Verbinden Sie Ihr System mit Systemen anderer Teilnehmer über das Internet. Führen Sie Untersuchungen im Netz durch.
- Performance Messungen. Vermessen Sie Ihr Netz bzgl. Bandbreite, Laufzeiten, Laufzeitschwankungen und Paketverlusten mit Hilfe des Performance-Analysewerkzeugs Iperf. Stellen Sie hierzu Szenarien für die Kommunikation zwischen Servern und Clients ein und verfolgen Sie die Kommunikation mit dem Protokoll-Analysator.
- Smart Grid. In einem verteilten Netz verfügen Sie über die Kommunikationsinfrastruktur für ein Smart Grid. Erstellen Sie Anwendungsszenarien und führen Sie Tests durch. Analysieren Sie die Kommunikation mit dem Protokoll-Analysator.
- sonstige Themen.

Ihr Thema sprechen sie bitte mit Ihrem Dozenten ab. Die Ergebnisse ergänzen Sie dann bitte in Ihrem Bericht.

8. Klausuraufgaben

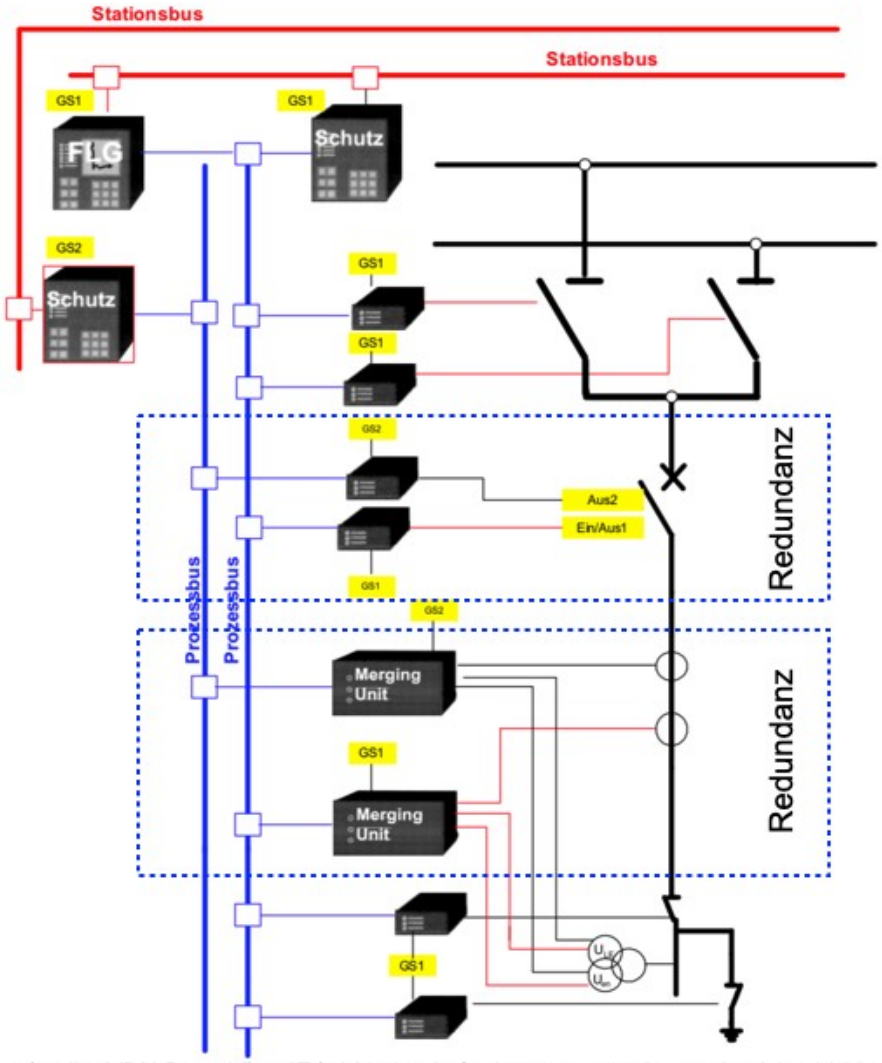
8.1. Stationsbus und Prozessbus

Für eine Umspannstation sollen Prozessbus und Stationsbus ausgelegt werden. Die Konfiguration soll pro Schaltfeld wie in der Abbildung gezeigt ausgeführt werden. Hierbei sind pro Schaltfeld vorgesehen:

- redundante Merging Units für Messungen (Abtastwerte von Strom und Spannung, 2 Geräte)
- redundante Schaltgeräte für den Leistungsschalter (2 Geräte)
- insgesamt vier Schaltgeräte für Trennschalter und Erdungsschalter (4 Geräte)
- redundante Schutzgeräte (2 Geräte, IED)
- ein Steuergerät (IED).

Folgende Abbildung zeigt die Anordnung. Es soll folgendes Verkehrsmodell verwendet werden:

- Schutznachrichten:
  - 256 Bytes pro Nachricht (Ethernet-Frame)
  - Wiederholung alle 100 ms für Schutznachrichten
  - bei Statusänderungen kurzzeitig 5-fache Wiederholrate
- Messwerte (Abtastwerte)
  - 256 Bytes pro Abtastwert (Ethernet-Frame mit insgesamt 8 Messwerten für Strom und Spannung)
  - 80 Abtastwerte pro Periode der Netzfrequenz von 50 Hz.



Quelle: VDN-Broschüre: IEC 61850 – Anforderungen aus Anwendersicht, 2004

Die Messwerte verbleiben hierbei auf dem Prozessbus.

Frage 8.3.1: Messwerte: Transaktionsrate und Datenrate. Wie viele Nachrichten pro Sekunde werden für Messwerte geschickt? Welche Datenrate ergibt sich insgesamt für die Messwerte? Wie verteilen sich diese Daten auf den Prozessbus und den Stationsbus?

Lösung: (1) 80 Abtastwerte pro Periode von 50 Hz: 4000 Nachrichten pro Sekunde; (2) mit 256 Bytes/Nachricht ergibt sich eine Datenrate von 8192 kbit/s pro Messgerät (Merging Unit), insgesamt somit ca 16 MBit/s. (3) Pro Prozessbus eine Merging Unit und somit 8192 kbit/s; die Daten verbleiben auf dem Prozessbus.

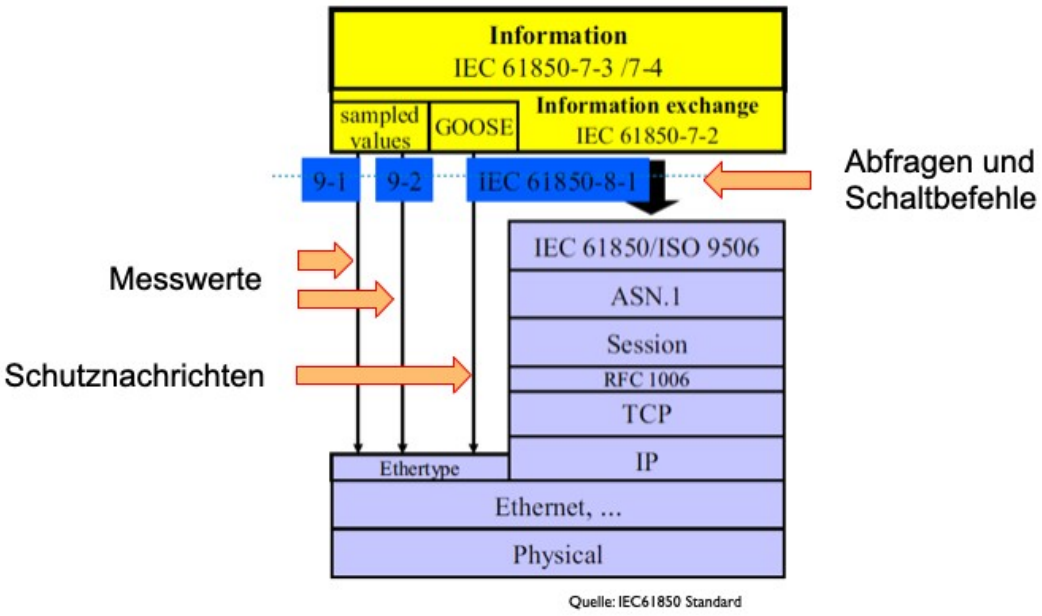
Frage 8.3.2: Datenverkehr Schutznachrichten. Welche Datenrate ergibt sich insgesamt für die Schutznachrichten? Wie verteilen sich diese Daten auf den Prozessbus und den Stationsbus?

Lösung: (1) Wiederholrate = Transaktionsrate der Schutznachrichten: 10 Nachrichten/s; kurzfristig bis zu 50 Nachrichten/s. (2) Datenrate somit ca. 20 kbit/s bis zu 100 kbit/s. (3) Diese Daten werden über den Stationsbus kommuniziert.

Frage 8.3.3: Die Schaltanlage hat insgesamt 10 Schaltfelder. Welche Datenrate ist auf dem Stationsbus zu erwarten? Welche Daten transportiert der Stationsbus außerdem?

Lösung: Die 10-fache Datenrate eines Schaltfeldes (zwischen 200 kbit/s und 1 Mbit/s). Außer Schutznachrichten werden relevante Zustandswerte, Abfragen und Schaltbefehle über den Stationsbus transportiert.

Frage 8.3.4: Die Abbildung zeigt den Aufbau der Protokollschicht für den Stationsbus und Prozessbus. Hierbei werden Messwerte und Schutznachrichten unmittelbar über Ethernet transportiert; Schaltbefehle und Zustandswerte hingegen über das Internet-Protokoll (TCP/IP). Erläutern Sie die Unterschiede und den Zweck dieser Wahl. Können Messwerte und Schutznachrichten aus der Station hinaus kommuniziert werden? Stellt die Verwendung von Internet-Adressen ein Sicherheitsrisiko dar?

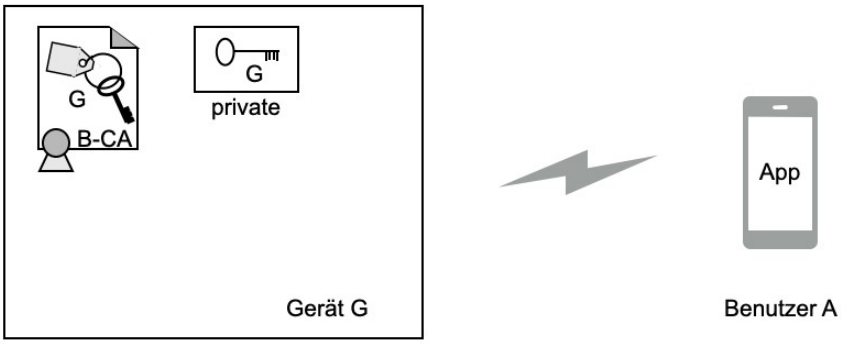


Quelle: IEC61850 Standard

Lösung: (1) Messwerte und Schutznachrichten sind zeitkritisch und werden daher unmittelbar über Ethernet kommuniziert. (2) Der Nachrichtenverkehr im Ethernet ist lokal, verbleibt also innerhalb der Station. (3) Schalbefehle und Zustandswerte sind über die Station hinaus relevant, z.B. bei Führung der Station von einer Netzleitwarte, und werden daher über Internet-Protokolle transportiert. Internet-Adressen ermöglichen Weitverkehrsnetze. (4) Das durch Internet-Adressen aufgespannte Netz kann ein privates Netz des Stromnetzbetreibers sein, ohne Verbindung zum öffentlichen Internet.

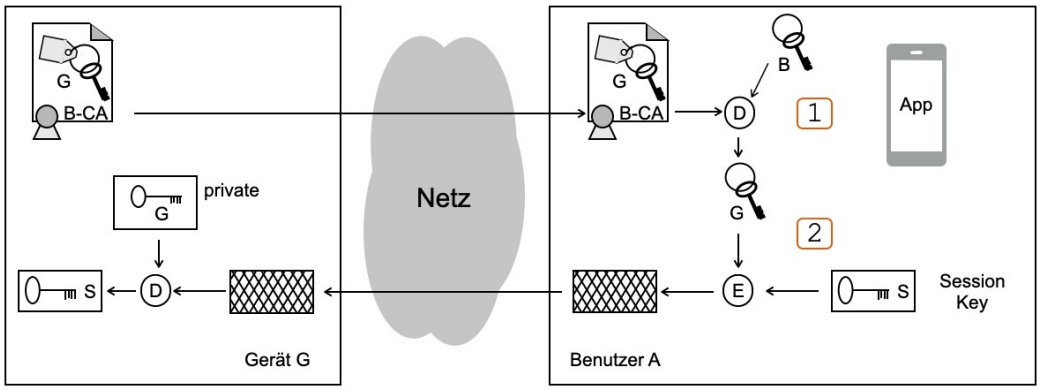
8.2. Sicherer Systemzugang mit App

Ein Gerät (z.B. Transformator, Schaltschrank, Maschine, Zugangstür) soll einen Zugriff nur für autorisierte Benutzer bieten. Die Benutzer sind mit einem mobilen Gerät ausgestattet, das den Zugriff per App gestattet. Als Kommunikationsschnittstelle soll ein Nahbereichs-Funk-Standard eingesetzt werden (z.B. Bluetooth, WLAN, NFC, …).



Hierzu wird das Gerät G mit einem privaten Schlüssel und einen Zertifikat ausgestattet, das der Betreiber B des Gerätes ausgestellt hat, wie in der Abbildung gezeigt.

Frage 8.4.1: Identitätsnachweis G. Wie kann die App (bzw. Benutzer A) sicher sein, mit dem korrekten Gerät zu kommunizieren? Wie kann Benutzer A eine verschlüsselte Nachricht an Gerät G schicken? Worauf beruht das Vertrauen des Benutzers A? Erläutern Sie den unten dargestellten Ablauf.



Lösung:

Ablauf: (1) Gerät G schickt bei Kontaktaufnahme durch A sein Zertifikat an A. A überprüft das Zertifikat. (2) Hierauf erzeugt A einen Session-Key, den es verschlüsselt an Gerät G schickt. Funktion siehe Skript (z.B. SSL, On-line Banking). Wenn Gerät G den Schlüssel korrekt auspacken kann, ist es im Besitz des privaten Schlüssels G.

Die Überprüfung des Zertifikates erfolgt mit Hilfe des in A gespeicherten Root-Zertifikates B, welches zuvor auf dem Gerät A installiert wurde. Das Zertifikat von G ist zuvor durch Signatur des Schlüssels G bei der Zertifizierungsinstanz B (B-CA) erstellt worden, wie in folgender zusätzlicher Abbildung dargestellt (sowie in zahlreichen Übungen im Skript).

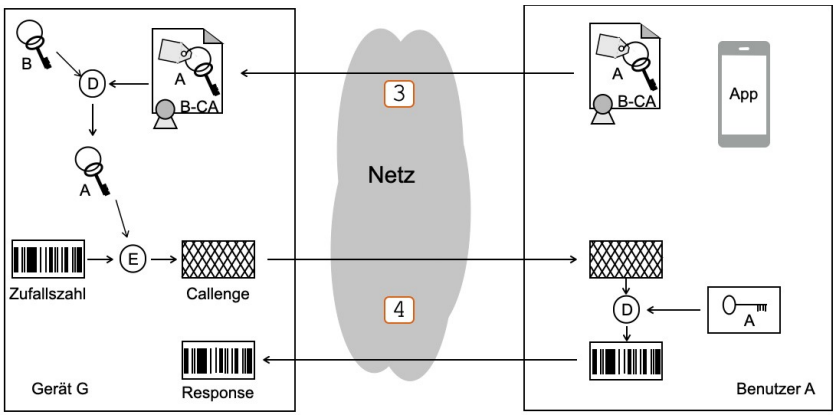
Frage 8.4.2: Worauf ist bei der Ausstattung des Gerätes G beim Hersteller bzw. beim Betreiber zu achten? Wie erfolgt die Ausstattung in der Praxis? Welche Rolle spielt das Betriebssystem des Gerätes? Hinweis: Welche Informationen sind geheim?

Lösung: Der geheime Schlüssel darf das Gerät niemals verlassen und muss sicher im Gerät abgelegt werden. Auf das Betriebssystem ist hierbei kein Verlass. In der Praxis bieten sich speziell geschützte Chips (TPM) bzw. Chipkarten an (siehe SIM-Karte).

Frage 8.4.3: Identitätsnachweis A. Bevor das Gerät G Zugriff für den Benutzer A auf Daten und Funktionen gewährt, muss es dessen Identität überprüfen. Beschreiben Sie hierzu eine Möglichkeit. Skizzieren Sie den Ablauf der Kommunikation. Bewerten Sie Ihre Wahl.

Lösungsbeispiele: (1) Passwort und Benutzerkennung (wie beim Home-Banking). Die sichere Übertragung ist mit Hilfe des Session-Keys möglich. Setzt jedoch die Einrichtung und Pflege dieser Daten auf dem Gerät voraus, daher wenig praktikabel. (2) Zertifikat A: gleicher Ablauf wie oben mit Zertifikat von A:

Gerät G muss hierbei prüfen, ob A tatsächlich im Besitz des passenden privaten Schlüssel ist. Dies kann z.B. durch Übermittlung einer verschlüsselten Zufallszahl geschehen (Challenge-Response-Verfahren, siehe Skript).



Frage 8.4.4: Zugriff für Werkspersonal. Der Zugriff ist nun abgesichert, was leider auch Abfragen zur Konfiguration im Werk des Herstellers bzw. Betreibers erschwert. Wie kann autorisiertes Werkspersonal auf das Gerät zugreifen?

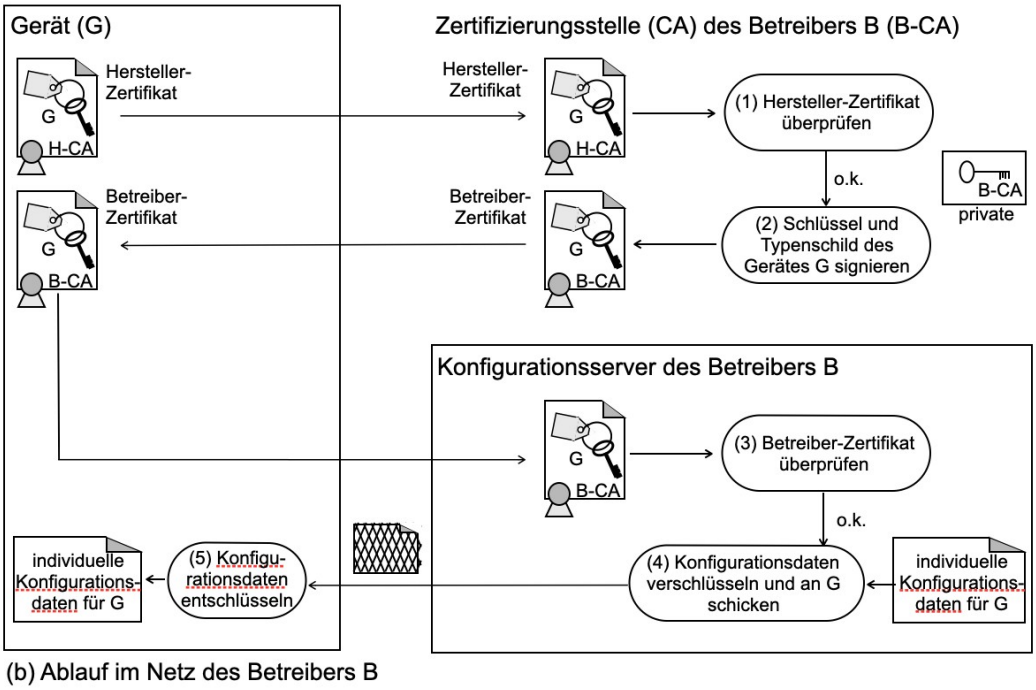
Lösung: Das Werkspersonal benötigt eine App mit Zertifikat des Herstellers bzw. Betreibers. Das Gerät kann das Zertifikat überprüfen. Wenn dem überprüften Zertifikat keine besondere Rolle zugewiesen ist (besondere Zugriffsrechte für hinterlegte Schlüssel), erhält das Personal Basisrechte für die Kommunikation mit den Gerät. Umgekehrt können in der App für das Werkspersonal die Schlüssel der Geräte hinterlegt sein, auf die sie Zugriff haben. So lassen sich Geräte automatisch identifizieren, um Fehler zu vermeiden.

Frage 8.4.5: Austausch der Zertifikate. Betreiber B hat Geräte vom Hersteller H gekauft, auf denen Zertifikate des Herstellers H hinterlegt sind. Diese Zertifikate von H sollen durch Betreiberzertifikate von B ausgetauscht werden. Skizzieren Sie einen Ablauf hierzu und erläutern Sie ihr den Ablauf.

Lösung: Der Betreiber liest die Herstellerzertifikate aus (siehe Frage 2.1), überprüft die Zertifikate (siehe Frage 2.1) und stellt dann neue Zertifikate aus, indem er den öffentlichen Schlüssel des Gerätes G in seiner Zertifizierungsstelle signieren lässt (siehe Frage 2.1). Hierbei lassen sich auch weitere Informationen in das Zertifikat einschließen, wie z.B. die Seriennummer des Gerätes, Kenngrößen, Baujahr etc, wie sie auf Typenschildern zu finden sind. Abbildung siehe Lösungen zu Frage 2.6.

Frage 8.4.6: Sichere Software-Updates. Mit Hilfe der Betreiberzertifikate soll das Gerät mit Software bzw. mit Daten bespielt und konfiguriert werden, Skizzieren Sie einen Ablauf hierzu und beschreiben Sie den Ablauf.

Lösung: siehe Abbildung unten. der Konfigurationsserver des Herstellers überprüft das Geräte-Zertifikat, verschlüsselt (und signiert) die Konfigurationsdaten bzw. Installationsdateien, und überträgt diese dann an das Gerät. Details siehe Skript.



(b) Ablauf im Netz des Betreibers B

Englisch - Deutsch

Energietechnik

Active power	Wirkleistung
Apparent power	Scheinleistung
Capacitor	Kapazität
Circuit breaker	Leistungsschalter
Line voltage	Leiter-zu-Leiter Spannung (Effektivwert)
Inductor	Induktivität
Nominal power	Nennleistung
Nominal voltage	Nennspannung
Peak value	Spitzenwert
Phase voltage	Leiter-zu-Nullleiter Spannung (Effektivwert)
Reactive power	Blindleistung
Resistor	Widerstand
Transformer	Transformator
Transmission	Übertragung
Voltage source	Spannungsquelle
Winding	Wicklung

...

Informations- und Kommunikationstechnik

Admission control	Zulassungskontrolle
Air Interface	Funkschnittstelle
Application layer	Anwendungsschicht, Verarbeitungsschicht
Basic Services (BS)	Basisdienste
Bearer Service	Trägerdienst
Block Error Rate	Blockfehlerrate
Broadcast	Rundsendung
Call Control	Rufsteuerung
Call Drop Rate	Verbindungsabbruchrate
Call Forwarding (CF)	Rufumleitung
Carrier	Verbindungsnetzbetreiber
Cell Identity (CID)	Zellkennung
Circuit switched domain	Leitungsvermittelte Domäne
Circuit switching	Leitungsvermittlung
Confidentiality	Vertraulichkeit
Content Provider	Inhalteanbieter

Control Plane	Steuerungsebene
Core Network	Kernnetz
Credentials	Beglaubigung, Zeugnis
Data Link Layer	Sicherungsschicht
Delay, Latency	Verzögerung, Laufzeit
Downlink	Abwärtsstrecke
Echo Canceller	Echokompensator
Expedited Forwarding	beschleunigtes Weiterleiten
Fading	Schwund
Firewall	Brandschutzmauer, Paketfilter
Frame Error Rate	Rahmenfehlerrate
Frequency Division Multiple Access	Frequenzvielfachzugriff
Handover, Handoff	(Verbindungs-)Übergabe, Weiterreichen
Integrity	Unversehrtheit (von Daten bzw. Systemen)
Jitter	Laufzeitschwankungen
Line of Sight	Sichtverbindung
Local Area Network	Lokales Rechnernetz
Location Area (LA)	Aufenthaltsbereich
Mobile Termination	Mobilfunk-Netzabschluss
Mobility Management	Mobilitätssteuerung
Multicast	Vielfachsendung
narrowband	schmalbandig
Network Layer	Vermittlungsschicht
Packet Loss	Paketverlust
Packet Switching	Paketvermittlung
Penetration Loss	Wanddämpfungsverlust
Physical Layer	Physikalische Schicht
Power Control	Leistungsregelung
Presence Service	Erreichbarkeitsdienst
Processing Gain	Prozessgewinn
Pseudo Noise Sequence	Pseudozufallsfolge
Push Service	Zustelldienst
Quality of Service	Dienstgüte
Release	Ausgabe (eines Normenpaketes oder Softwarepaketes)
Resource Management	Administration der Betriebsmittel
Resources	Betriebsmittel
Routing	Verkehrslenkung
Scrambling	Verwürfelung

Sensitivity	Empfindlichkeit
Service Provider	Dienstanbieter, Diensterbringer
Session	Sitzung
Session Layer	Sitzungsschicht
Session Management	Sitzungssteuerung
Short Message	Kurznachricht
State Event Diagram	Zustandsübergangsdiagramm
Subframe	Teilrahmen
Sublayer	Teilschicht
Subscription	Vertragsabschluss, Subskription, Diensteinschreibung
Supplementary Services (SS)	Zusatzdienste
Terminal Equipment	Endgerät
Time Division Multiple Access	Zeitvielfachzugriff
Traffic Model	Verkehrsmodell
Transcoding	Umcodierung
Transport Layer	Transportschicht
Uplink	Aufwärtsstrecke
User Equipment	Teilnehmerausrüstung
User Plane	Nutzerebene

...

Abkürzungen

Energietechnik

AC		Alternating Current, Wechselstrom
DC		Direct Current, Gleichstrom
$T = 1/f$		Schwingungsdauer, Periodendauer [s]
$f = 1/T$		Frequenz, Anzahl der Schwingungen pro Zeiteinheit [1/s]
$\omega = 2\pi f = 2\pi/T$		Kreisfrequenz, Winkelgeschwindigkeit der Kreisbewegung [1/s]
E		Energie [Joule, J, Nm, Ws, kg m^2/ s^2] potentielle Energie $E_p = 1/2\ k\ y^2$, kinetische Energie, Translation $E_k = 1/2\ m\ v^2$, kinetische Energie, Rotation $E_r = 1/2\ J\ \omega^2$, Energie elektrisches Feld $E_C = 1/2\ CU^2$, Energie magnetisches Feld $E_L = 1/2\ LI^2$
RMS		Root mean square (Effektivwert)
Z		komplexer Widerstand (Impedanz, impedance)
	R	Wirkwiderstand (resistance)
	X	Blindwiderstand (Reaktanz, reactance)
Y		komplexer Leitwert (Admittanz, admittance)
	G	Wirkleitwert (conductance)
	B	Blindleitwert (susceptance)
S		Scheinleistung (apparent power, in VA = Volt Ampere)
	P	Wirkleistung (power, in Watt)
	Q	Blindleistung (reactive power, in Var = Volt ampere reactive)
A		Ampere
deg		degrees (Phasenwinkel in Grad)
kV		Kilo Volt (1000V)
kVA		Kilo Volt Ampere (Scheinleistung S, zur Unterscheidung von kW = Wirkleistung))
kVar		Kilo Volt Ampere reactive (Blindleistung, Q)
MS		Mittelspannung
NS		Niederspannung
ONT		Ortsnetztransformator
p.u.		per unit (auf Nennwert und physikalische Einheit normierte Größe)
PV		Photovoltaik
W		Watt (Wirkleistung, P)

Informations- und Kommunikationstechnik

AAA	Authentication, Authorization, Accounting

AG	Access Gateway
AP	Access Point
API	Application Programming Interface
CDMA	Code Division Multiple Access
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LAN	Local Area Network
MAC	Medium Access Control
MSISDN	Mobile Subscriber ISDN Number
OSPF	Open Shortest Path First
RFC	Request For Comments (IETF)
RTP	Real Time Transport Protocol
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
UDP	User Datagram Protocol
UML	Unified Modeling Language
URL	Universal Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WWW	World Wide Web
XML	Extended Markup Language

Literatur

(1) R. Hoheisel, H. Jansen, R. Kochranke, G. Siegmund et al: Informationstechnik, Telekommnikation, Neue Netze, Europa-Lehrmittel; 7 Auflage, 2015, ISBN-13: 978-3808536278

(2) Gerd Siegmund, SDN - Software-defined Networking: Neue Anforderungen und Netzarchitekturen für performante Netze, VDE VERLAG GmbH, 2018, ISBN-13: 978-3800745111

(3) Andrew S. Tanenbaum, Computer Netzwerke, Pearson Studium; Auflage: 4., überarbeitete Auflage (2003); ISBN-13: 978-3827370464

(4) IEC 61850: UML Übersicht über den Standard für Web-Browser:

http://www.nettedautomation.com/download/std/61850/uml

(5) IEC 61870/61968, CIM (Common Information Model): UML Implementierung der CIM User Group (Dokument lässt sich nach Registrierung laden):

http://cimug.ucaiug.org/CIM Model Releases/Forms/AllItems.aspx

(6) Valentin Crastan, Dirk Westermann, Elektrische Energieversorgung 3: Dynamik, Regelung und Stabilität, Betriebsplanung und -führung, Leit- und Informationstechnik, FACTS. HGÜ, Springer-Verlag Berlin Heidelberg 2012, ISBN-13: 978-3-642-20100-4, Kapitel 10: Leit- und Informationstechnik

(7) Rudolf Baumann et al, Der Standard IEC 61850, Zeitschriftenartikel, Bulletin SEV/VSE 3/03:

http://www.nettedautomation.com/download/mannheim-2003-03/SEV-Bulletin_Baumann_2003-01.pdf

(8) M. Zillgith, Freie IEC61850 Implementierung (Open Source) und Dokumentation:

http://libiec61850.com/libiec61850/documentation/

Allgemein über die elektrischen Energieversorgungsnetze:

(9) Klaus Heuck, Klaus-Dieter Dettmann, Detlef Schulz: Elektrische Energieversorgung: Erzeugung, Übertragung und Verteilung elektrischer Energie für Studium und Praxis, Vieweg + Teubner Verlag, 8. Auflage, 2010, ISBN 978-3834807366